e-crime & cybersecurity DACH VR

14. Januar 2021
Online

@eCrime_Congress
#ecrimecongress

#ecrimecongress

Digitalisierung ist nicht optional.
Cloud ist unvermeidlich.
Geschäftstransformation bedeutet Überleben.
Können CISOs die Kontrolle behalten?

e-Crime & Cybersecurity DACH VR

“ Despite the difficulties that the current pandemic situation brings with it, I found the event yesterday in this new virtual format to be successful, very interesting and stimulating.

I took new insights and ideas with me, which I will share with colleagues to further develop information security management. ”
IT Security Officer
MLP

2020 sponsors included:

Strategic Sponsors

CROWDSTRIKE
paloalto NETWORKS
proofpoint.
RANGEFORCE
SentinelOne
SHAPE Part of F5
VERACODE

Education Seminar Sponsors

COFENSE
corelight
cybereason
onelogin
Synack
tripwire

For more information, please call Robert Walker on +44 (0)20 7404 4597
or email robert.walker@akjassociates.com

Das einzige Wort „Digitalisierung“ wird den tiefgreifenden Veränderungen, die wir sehen, kaum gerecht. Unternehmen vom kleinsten bis zum größten Unternehmen verlassen sich immer mehr auf mobile Apps und Websites, mit all den damit verbundenen Entwicklungs- und Sicherheitsproblemen. Kein Unternehmen kann die Cloud ignorieren, aber auch hier gibt es Betriebs- und Sicherheitsprobleme. Daten mögen das neue Öl sein, aber es ist genauso stark reguliert und Brexit, GDPR, Schrems II und der Rest verursachen überall mehr Kosten und Komplexität, vom Marketing bis zum Callcenter für den Kundensupport. und das IoT ist Realität, mit Sensoren, die in alles eingebettet sind, vom Auto bis zur Produktionslinie, die nicht nur Sicherheitsarchitekturen, sondern ganze Geschäftsmodelle auf den Kopf stellen.

Und natürlich gibt es Dritte (und vierte und fünfte und ……). Die Hacks Fireeye und Solar Winds, die Ende 2020 immer ein Problem in Bezug auf die konventionelle Lieferkette darstellten, erinnerten uns alle erstens daran, dass staatliche Akteure jeden hacken können, den sie wollen, und zweitens, wenn sie Ihre Sicherheitsanbieter, insbesondere ihre Update-Programme, hacken können sie jederzeit und überall auf so ziemlich alles zugreifen, was sie wollen.

2021 wird also das Jahr sein, in dem Unternehmen sich mit ihren neuen digitalen Infrastrukturen auseinandersetzen, Silos abbauen, die Sichtbarkeit erhöhen und Cloud, SaaS und eine Vielzahl anderer Sicherheitsherausforderungen in den Griff bekommen müssen. Wir hoffen, dass wir Ihnen mit unserer virtuellen E-Crime-Serie helfen können, den Angreifern immer einen Schritt voraus zu sein.

Wir freuen uns, Ihnen unseren 16. e-Crime & Cybersecurity DACH online stellen zu können. In Ermangelung physischer Besprechungen ist die Veranstaltung eine fantastische Gelegenheit, Fallstudien aus der Praxis und ausführliche technische Sitzungen von Kollegen zu hören, die auch per Fernsteuerung im Bereich Cybersicherheit navigieren. Eines der ständigen Ziele unserer Veranstaltungen ist es, die Konversation zu erleichtern. Nutzen Sie diese Gelegenheit, um sich mit Kollegen in der Networking-Lounge zu vernetzen, Fragen an die Redner im Auditorium zu stellen und die Ausstellungshalle zu besuchen, um sich mit Lösungsanbietern zu unterhalten. Wir hoffen, dass Ihnen die Veranstaltung gefällt. Bitte besuchen Sie unser Team am virtuellen Registrierungsschalter, wenn Sie Fragen haben!

Simon Brady | Chefredakteur

@eCrime_Congress **#ecrimecongress**

14. Januar 2021

Online

Editor:
Simon Brady
e: simon.brady@akjassociates.com

Design and Production:
Julie Foster
e: julie@fosterhough.co.uk

Forum organiser:
AKJ Associates Ltd
27 John Street
London WC1N 2BX
t: +44 (0) 20 7242 7820
e: simon.brady@akjassociates.com

© AKJ Associates Ltd 2021. All rights reserved. Reproduction in whole or part without written permission is strictly prohibited.

Articles published in this magazine are not necessarily the views of AKJ Associates Ltd. The publishers and authors of this magazine do not bear any responsibility for errors contained within this publication, or for any omissions. This magazine does not purport to offer investment, legal or any other type of advice, and should not be read as if it does.

Those organisations sponsoring or supporting e-Crime & Cybersecurity DACH VR bear no responsibility, either singularly or collectively, for the content of this magazine. Neither can those organisations sponsoring or supporting e-Crime & Cybersecurity DACH VR, either singularly or collectively, take responsibility for any use that may be made of the content contained inside the magazine.

Need for Speed: Das autonome SOC

Informationssicherheit hat sich in den letzten Jahren so dramatisch entwickelt wie die Security Operations Center (SOC).

Sergej Epp berichtet

Kaum eine Disziplin der Informationssicherheit hat sich in den letzten Jahren so dramatisch entwickelt wie die Security Operations Center (SOC). Die SOC's sind als letzte Meile der Verteidigung gegen Cyber Angriffe kaum mehr wegzudenken, weil durch die zunehmende Digitalisierung und Vernetzung die Anzahl der Gefahren und Risiken für Unternehmen rasant gestiegen ist. Viele Unternehmen setzen aber auch aus anderen Gründen auf schlagkräftige SOC's. Oft kann nämlich die in die Jahre gekommene IT-Infrastruktur nicht so einfach oder schnell modernisieren werden. Security Operations Center sollen dann durch zusätzliches Monitoring und schnelle Gegenmaßnahmen potenzielle Angreifer draußen halten.

Ursprünglich aus den Network Operations Center entwickelt, haben die SOC's viele Entwicklungen durchlebt wie zum Beispiel die Threat-Intelligence Ausrichtung oder die Zusammenführung mit den CERTs. Dabei sind die SOCs immer größer und größer geworden, um dem Spektrum der administrativen Tätigkeiten und der Anzahl der Stakeholder gerecht zu werden. Doch bei den neuen Cybersicherheits-Herausforderungen, stoßen auch große SOC's schnelle auf Ihr Grenzen.

Das „New Normal" für die SOC's

Ein SOC in einem Digitalunternehmen definiert sich in erster Linie über die enge Integration in die Produktentwicklung und als zweites über die Geschwindigkeit neue Umgebungen abzusichern. Historisch war der Fokus eher Governance und Infrastruktur Compliance.

Entwicklung der Security Operations Center

Die Beschleunigung der Digitalisierung durch COVID-19 hat teilweise über Nacht viele SOC Architekturen auf den Kopf gestellt. Kann das SOC von zu Hause aus operiert werden? Wie gehe ich mit BYOD oder Mitarbeitern aus der Incident Response oder Forensik Perspektive um? Wie überwache ich neue Technologien wie Public Cloud oder die diversen Remote Tools, die im Zuge von COVID eingeführt wurden? Wie komme ich mit der Geschwindigkeit der DevOps Prozesse mit? Viele dieser Frage müssen von den SOCs schnellstmöglich gelöst werden. Doch die Fachkräfte, die dafür bei Unternehmen zusätzlich aufgebaut werden müssen, fehlen bekanntlich auf dem Markt.

Zusätzlich dazu setzen die Angreifer zunehmend auf Automatisierung und erhöhen das Spieltempo für die Verteidiger. Bei Non-Petya Ransomware 2016, waren es zum Beispiel nur sieben (7) Minuten bis manche Organisation hundert Tausende von Geräten verloren haben. Nun, die KI-Basierte Malware ist zwar noch Science-Fiction, doch die Labors weltweit brühen schon dran diese bald Realität werden zu lassen.

Fragmentierung und Frankenstein

Zur effektiven Verteidigung haben wir uns historisch in Cybersecurity eine Reihe an Konzepten überlegt, die die Hürde für die Angreifer immer höher setzen. Defense in Depth, Kill Chain/MITRE ATT&CK, Pyramide of Pain, Zero Trust, DevSecOps sind wohl die wichtigsten Strategien auf, die jedes moderne Security Operations Center aufbauen sollte. Die meisten dieser Konzepte haben eins gemeinsam: den Gesamtblick auf die Cybersecurity.

Die Cybersecurity Technologien, die in den letzten Jahrzehnten entstanden sind, waren dagegen immer auf Teilbereiche unserer Organisationen oder auf einzelne Probleme ausgerichtet. Zwei Beispiele. Defense in Depth also das klassische Zwiebelmodel von Cybersecurity wird sehr oft von SOCs aus Produkten unterschiedlicher Hersteller aufgebaut. Falls ein Angriff vom Network Threat Analytics (NTA) entdeckt wird, ist dieses dann weder dem Endpoint Security System (EPP/EDR) bekannt, noch dem der Firewall. Die SOC Mitarbeiter müssen also manuell nachhelfen, um alle Technologien mit den neuen Indikatoren zu füttern. Ein weiteres Beispiel sind die Security Information Event Management (SIEM) Systeme und die damit verbundene Obsession mehr und mehr Daten zu sammeln, ohne sich ursprünglich Gedanken zu machen wie diese später in Analytiken oder Incident Response Aktivitäten verwertet werden. Weil man so viel Zeit in die Daten investiert hat, zwingt man sich dann irgendwelche Analytiken daraus zu machen. Das Resultat sind Alarme mit einer geringen Qualität und noch mehr manuelle Arbeit und Konsolen Burnout für die SOC's. Bei einem Unternehmen, können locker innerhalb von einem Monaten Zehntausende von Alarmen anfallen, die alle von Analysten abgearbeitet werden müssen. Bei einem

SOCs die Ihre Prozesse und Technologien konsequent rund um Automatisierung und Kollaboration aufbauen, können sich schnell auf die ständig wachsenden Business-Anforderungen und Bedrohungen anpassen und so zum Geschäftserfolg der Unternehmen beitragen.

DAX Unternehmen sind es noch mehr. Es gibt wohl aber nur wenige Angriffe die keine Spuren hinterlassen. Die Angreifer stolpern fast immer über ein Anti-Virus, welches eines ihrer Tools erkennt, einem zu offensivem Portscan oder einem User der auf bestimmten Systemen nichts verloren hat. Es gilt also die Alarme schnell in Kontext zu bringen und die Abarbeitung der Playbooks wie zum Beispiel die Implementierung der Gegenmaßnahmen schnell durchzuführen, anstatt noch mehr Alarme zu generieren.

Durch fragmentierte Technologien und viele manuelle Prozesse, erinnern die SOC's daher oft an einen Frankenstein der aus unterschiedlichen Teilen zusammengesetzt wurde und sich deshalb nur langsam bewegt und spricht. In einer zunehmend schnellen Welt, eine Spezies mit wenig Überlebenschancen.

Vom EDR zu XDR

Der Erfolg der Endpoint Detection & Response (EDR) Systeme seit 2013, basiert auf dem Misserfolg der SIEM Systeme qualitative Alarme zu generieren und dem Alarm mehr Kontext zu geben. EDR Systeme bauen dafür auf vordefinierten Analytiken auf und generieren so viel weniger False-Positives. Doch jeder Forensiker weiß, dass auch Endpoint-Daten nur ein Teil von dem Gesamtpuzzle sind. Einmal vom Angreifer übernommen, können die Logs auf jedem Gerät gelöscht oder manipuliert werden. Schließlich kann der EDR Agent auf einem Gerät ganz abgeschaltet werden. Wie soll man dann z.B. herausfinden ob und wieviele Daten abgeflossen sind? Gab es Seitwärtsbewegung im Unternehmen? Welches Gerät war der Patient Zero? All diese Fragen bleiben dann unbeantwortet. Zumal, mit Schatten IT und der steigenden Anzahl von IoT Geräten, können bei Unternehmen oft auf 50-80% der Geräte gar keine EDR Agenten installiert werden. Ein wachsendes Risiko.eXtended Detection & Response (XDR) ist die natürliche Weiterentwicklung von EDR. Dabei wird nicht nur die Telemetrie von den Endpoints ausgewertet, sondern auch die Telemetrie von weiteren Sicherheitstechnologien wie Firewalls (NGFW), Netzwerk Analytik (NTA), User Behaviour Analytics (UBA) oder Cloud Security einbezogen. Die Idee von XDR ist es ein unternehmensweites Cockpit für den SOC-Bereich bereitzustellen, der sich rund um die Analytiken dreht und nicht um die Daten - wie es bei einem klassischen SIEM der Fall ist. Durch die hohe Qualität der Alarme im XDR, ergeben sich zusätzlich bessere Perspektiven die nachfolgenden Response Aktivitäten zu automatisieren.

DevSecOps ist SOAR

XDR automatisiert aber nicht alles. Viele Playbooks im SOC benötigen unternehmens- oder sogar applikationsspezifische Schritte bevor die Gefahr mitigiert ist. Das kann zusätzliche maschinelle oder manuelle Analyse von Stakeholdern sein, Kommunikationsanforderungen oder spezielle Gegenmaßnahmen wie Konfigurationsanpassung oder User-Verwaltung. Diese Aufgaben sind zeitfressend und sind an Mangel von Programmierern in SOC's nur selten automatisiert. Security Orchestration, Automation and Response (SOAR) Tools fokussieren sich genau auf diese Problemstellung. Durch eine breite Unterstützung von API's zu diversen Technologien und Threat Intelligence Quellen können Workflows auch von nicht technischen Mitarbeitern abgebildet werden, um wiederkehrende Abläufe automatisiert auszuführen. Die Vorteile liegen auf der Hand. Lästige Aufgaben wie Tickets pflegen, Dedublication oder Enrichment von Tickets muss nicht mehr gemacht werden. Man bekommt mehr Zeit für Analyse Tätigkeiten und reduziert das Risiko, weil die Angriffe in Minuten oder Sekundenschnelle abgewehrt werden können. Viele Nebenprodukte wie effektive Metriken oder Audit Möglichkeiten ergeben sich dabei als das Sahnehäufchen auf dem Pudding dazu. Aber der entscheidende Erfolgsfaktor ist ein ganz anderer. Die Flexibilität beliebige Workflows zu Automatisieren ermöglicht es den Security Teams mit der Geschwindigkeit und Agilität der DevOps Teams mitzuhalten und somit Security von vorne rein in die Produkte zu integrieren. DevSecOps Ansatz für die SOC's wird damit kinderleicht.

Ein Autopilot für SOC

SOCs die Ihre Prozesse und Technologien konsequent rund um Automatisierung und Kollaboration aufbauen, können sich schnell auf die ständig wachsenden Business-Anforderungen und Bedrohungen anpassen und so zum Geschäftserfolg der Unternehmen beitragen. Automatisierte Playbooks die den ganzen Kreislauf zwischen Detection, Response und Prevention abbilden ermöglichen sogar eine ganz neue Klasse von SOCs'. Einen Autopiloten, der ähnlich wie im Flugzeug oder im modernen Auto, simple Aufgaben übernimmt oder dem SOC hilft Ihre Prozesse zu skalieren. Die SOC's bekommen damit mehr Ressourcen und Zeit sich auf das wesentliche zu fokussieren, wie Analyse, Threat Hunting oder Red Teaming. □

Sergej Epp, Chief Security Officer Central Europe, Palo Alto Networks.

Weitere Informationen unter
www.paloaltonetworks.com

paloalto NETWORKS

paloalto NETWORKS | CORTEX BY PALO ALTO NETWORKS

The Endpoints of Today, Secured Against the Threats of Tomorrow

Cortex XDR™ – The Future of Threat Detection & Response

Secure your future now

FREUND ODER FEIND?

Heutige Cyber-Angreifer sind Meister der Tarnung.

Hochentwickelte E-Mail-Angriffe, kompromittierte Cloud-Systeme, angreifbare Geräte - die Bedrohungen von morgen sind nur schwer vorherzusagen. KI kann zwischen legitimer Aktivität und einer sich entwickelnden Cyber-Bedrohung entscheiden und in Sekundenschnelle zurückschlagen.

Starten Sie eine 30-tägige Teststellung und seien Sie eins der tausenden Unternehmen, die sich mit Darktraces weltführender Cyber-KI schützen.

darktrace.com/de

DARKTRACE
World-Leading Cyber AI

Wie sich änderndes online-Verhalten die Tür für eine neue Welle von E-Mail-Angriffen öffnete

Hacker finden neue Wege, die volle Bandbreite menschlicher Emotionen durch hochentwickelte E-Mail-Angriffe auszunutzen.

Mariana Pereira berichtet

Wir haben in den letzten Monaten gesehen, wie Cyber-Kriminelle die globale Gesundheitskrise als "Fearware"-Thema nutzen, um ihre Angriffe zu starten und zu verbreiten. Da nun aber immer größere Teile der Bevölkerung von zu Hause aus arbeiten und der Konsum digitaler Inhalte dadurch zunimmt, finden Hacker neue Wege, die volle Bandbreite menschlicher Emotionen durch hochentwickelte E-Mail-Angriffe auszunutzen.

Von Angreifern, die "digital fake"-Kampagnen erstellen, die "Beratung" für Menschen in Quarantäne anbieten, zu Bedrohungsakteuren, die sich hinter vertrauten Websites verstecken, um Malware zu starten – die letzten Monate haben gezeigt, wie schnell Cyber-Kriminelle ihre Vorgehensweisen in der E-Mail-Umgebung anpassen können. Dieser Artikel stellt vier Beispiele vor, wie Hacker ihre Taktiken den momentanen Trends und sich ändernden Verhalten anpassen und wie Sicherheitsteams reagieren können, um gegen diese Entwicklungen zu schützen.

Mehr Abonnements

Mit der steigenden Anzahl digitaler Abbonements auf Entertainment-, und Nachrichten-Sites sollte es keine Überraschung sein, dass Spammer und Hacker mehr den je gefälschte Newsletter-Abonnements in ihren E-Mail-Angriffen nutzen.

Für Sicherheitstools wie Gateways und Posteingänge, die nur auf den historischen E-Mail-Verkehr schauen, kann ein neues Abonnement zu einem E-Mail Newsletter aussehen, wie jedes andere – besonders dann, wenn die E-Mail alle vorhandenen Sicherheitstests und Verifizierungen besteht. Eine brandneue Kampagne oder Domain wurde vielleicht noch nicht als bösartig erkannt und wird deshalb in den Posteingang des Empfängers gelassen.

E-Mails im breiteren Unternehmenskontext zu analysieren hilft, volles Verständnis für die Umstände zu entwickeln, in denen sie empfangen wurden. Dafür muss weiter als zum Posteingang geblickt und die normalen Verhaltensmuster – die sogenannten "Patterns of Life" – der Benutzer im gesamten digitalen Ökosystem in Betracht gezogen werden. Im Falle von gutartigen Abonnement-E-Mails wird der Benutzer vor kurzem die Domain des Absenders besucht und ein Abonnement angefragt haben. Da ist eine Aktion vor dem Erhalt der E-Mail – die Anfrage.

Mit Einblicken sowohl in den E-Mail-Verkehr, als auch in die normalen Verhaltensmuster, die sogenannten "Patterns of Life", der Benutzer im gesamten digitalen Unternehmen, kann die KI erkennen, ob ein E-Mail Newsletter angefragt wurde, oder nicht. Das alleine kann Sicherheitsteams helfen zu verstehen, ob ein Benutzer sich freiwillig für einen Newsletter angemeldet hat, oder ob er Ziel eines bösartigen Angriffs ist. So kann angemessen eingegriffen werden.

Erhöhte Nutzung von externen Präsentationswebsites

Da mehr und mehr Menschen von zu Hause aus arbeiten, gab es einen starken Anstieg in der Nutzung von Websites zur Erstellung von Präsentationen. Darktrace hat eine große Anzahl von Angriffen beobachtet, in welchen diese vertrauten Seiten ausgenutzt wurden, um bösartige Links zu hosten. Bösartige Payloads werden in Präsentationen eingefügt, welche dann in E-Mails verteilt werden, die unbemerkt an Gateway-Tools vorbeikommen.

Es gibt einige Hinweise, dass diese Aktivität von einer einzigen, gut organisierten Gruppe von Bedrohungsakteuren stammt: Zum Beispiel das abwechselnde Abzielen auf verschiedene Präsentationswebsites (Canva, Infogram, Axel, Piktochart und Sway), die stark fokussierte Art der Angriffe (sie geschehen innerhalb von zwei Wochen) und die einheitliche Art und Weise dieser E-Mails. Diese E-Mails wurden in einer großen Zahl von Deployments beobachtet, welche anscheinend ein sehr ähnliches gefälschtes eFax Mitteilungsformat nutzten.

Besorgniserregend ist, dass diese E-Mails keine der typischen "Trademark" Identifikatoren zeigen, die oft bei Phishing-E-Mails gesehen werden, wie zum Beispiel gespoofte oder nachgeahmte E-Mail Adressen oder ungewöhnliche Linkketten. Deshalb bleiben sie unbemerkt von Produkten wie Microsoft's Spam- und Phishing-Tools und erreichen den Posteingang der Empfänger ohne Eingriffe oder weitere Sicherheitsmaßnahmen.

Diese Aktivität scheint auf eine schwere und bis jetzt noch unerkannte externe Bedrohung hinzuweisen. Obwohl die Neuartigkeit dieser Aktivität es möglich machte, leicht herkömmliche Tools zu umgehen, erlaubte ein mehrschichtiges Verständnis des Menschen hinter der E-Mail Adresse es Darktraces KI, auf einzigartige

Anstatt E-Mails isoliert zu nur einem bestimmten Zeitpunkt zu analysieren, setzt Cyber-KI Einblicke über einen längeren Zeitraum hinweg in Verbindung und schätzt alte E-Mails fortlaufend neu ein, wenn neue Hinweise auftauchen.

Weise diese Reihen von E-Mails als höchst bedrohlich zu identifizieren. Die Technologie erkannte, dass die Links und Domains extrem unüblich waren, nicht nur im Kontext des normalen Verhaltens der Empfänger, sondern auch der normalen Verhaltensmuster – den sogenannten "Patterns of Life" ihrer Vergleichsgruppen und des gesamten Unternehmens.

Ein noch nie dagewesenes Zusammentreffen von Persönlichem und Beruf

Während IT- und Complianceteams Wege finden müssen, digitale Umgebungen auch mit Home Office weiterhin zu sichern, ändern Benutzer auch ihr eigenes Verhalten – nicht nur darin, welche Geräte und Tools genutzt werden, sondern auch darin, was für Inhalte und Dateien konsumiert werden, und mit welchen Inhalten interagiert wird. Dieses Zusammentreffen von Persönlichem und Beruf und die daraus resultierende Erweiterung der Angriffsfläche bringt neue Herausforderungen für Sicherheitsteams mit sich. Kompromittierte E-Mail-Zugangsdaten und übernommene Accounts sind noch schwieriger zu erkennen.

Um diese Umgebungen zu schützen, braucht es eine Technologie, die sich an die neuen Arbeitsweisen anpassen kann, ohne Regel neu schreiben oder konfigurieren zu müssen. Digitale Aktivität hat sich über Nacht verändert und wird sich auch weiterhin verändern – Sicherheitslösungen, die sich nicht anpassen und mitverändern können, werden schnell überflüssig. Da sie immer weiter lernt und ihr Verständnis von jedem Benutzer und Gerät immer weiterentwickelt, ist KI wichtig wie nie, um Mitarbeiter zu schützen – vor allem jetzt, wo wir unser Verhalten ändern und mehr Cloud-basierende Kommunikations- und Collaboration-Tools nutzen.

Sich anpassende KI-gestützte Angriffe

Ein Bericht von Forrester berichtete, dass mehr als die Hälfte von befragten Sicherheitsexperten erwarten, dass sich die Öffentlichkeit in den nächsten 12 Monaten KI-gestützter Cyber-Angriffen bewusst wird. Eine Möglichkeit, wie dies passieren könnte, ist durch die Automatisierung von maßgeschneiderten Spear-Phishing Kampagnen.

Da Angreifer KI nutzen, um die Inhalte, mit denen Nutzer interagieren, und die wichtigsten Emotionen, die jeden Nutzer antreiben, zu verstehen, können Malware oder bösartige Links nun als Inhalte getarnt werden, die auf spezifische Benutzer zugeschnitten sind. Nutzer, die aktiv Informationen zu bestimmten Themen suchen, oder öfter witzige, harmlose Inhalte teilen oder weiterleiten, können öfter oder aggressiver angezielt werden.

Indem sie ihre Zielpersonen mit KI untersuchen, können Hacker ihre Einblicke in einer noch nie dagewesenen Geschwindigkeit und Skalierbarkeit nutzen. Menschliche Analysten und herkömmliche Sicherheitstools haben bei hochentwickeltem Domain-Spoofing, ununterscheidbaren Schreibstilen und gekonnt versteckten bösartigen Links keine Chance mehr.

Um sich auf die nächste Angriffswelle vorzubereiten, verlassen sich die Sicherheitsteams selbst auf KI, die E-Mails im Kontext von Verhalten über die gesamte E-Mail Plattform und dem gesamten Unternehmen analysiert. Anstatt E-Mails isoliert zu nur einem bestimmten Zeitpunkt zu analysieren, setzt Cyber-KI Einblicke über einen längeren Zeitraum hinweg in Verbindung und schätzt alte E-Mails fortlaufend neu ein, wenn neue Hinweise auftauchen.

Traditionelle Sicherheitslösungen fragen ab, ob Teile einer E-Mail historisch schon in Angriffen beobachtet wurden; Antigena Email jedoch ist die einzige Lösung, die verlässlich feststellen kann, ob es für einen Empfänger im Kontext seiner normalen Verhaltensmuster, der sogenannten "Patterns of Life", und der seiner Vergleichsgruppen und des gesamten Unternehmens, unüblich ist, mit einer bestimmten E-Mail zu interagieren. Dank dieses kontextuellen Verständnisses kann KI extrem akkurate Entscheidungen treffen, um die volle Bandbreite an E-Mail Angriffen zu neutralisieren – von 'sauberen' Spoofing-E-Mails, die betrügerische Zahlungen veranlassen wollen, bis zu hochentwickelten Spear-Phishing Versuchen. □

Mariana Pereira, Director of Email Security Products, Darktrace.

Weitere Informationen unter
www.darktrace.com/de

Die Evolution der Endpunktsicherheit: XDR als neues Sicherheitsparadigma

Im Zuge der sich verändernden Bedrohungslandschaft sind auch Innovationen in Unternehmen notwendig.

Matthias Canisius reports

Die Welt der Cybersicherheit ist eine Welt der Akronyme. Von AV (Antivirus) über EPP (Endpoint Protection Plattform) bis hin zu EDR (Endpoint Detection and Response) – und jetzt auch XDR (Extended Detection and Response). Diese sich wandelnden Technologien und deren Bezeichnungen sind ein Beleg für eine sich wandelnde Cyberbedrohungslage. Sicherheitsverantwortliche müssen stets einen oder mehrere Schritte voraus sein, um ihre Netzwerke vor Angreifern zu schützen. Im Zuge der sich verändernden Bedrohungslandschaft sind auch Innovationen in Unternehmen notwendig, denn um den Geschäftsbetrieb aufrechtzuerhalten und weiterzuentwickeln, dürfen sich Organisationen in Sachen Digitalisierung keine Auszeit gönnen. Das alte „On-Premises"-Paradigma, das durch einen überschaubaren Netzwerkumfang begrenzt ist, gilt nicht mehr. Wir befinden uns nun in einer Welt, die zunehmend von einer dezentralen, Cloud-basierten Infrastruktur geprägt ist und in der die Remote-Arbeit die Komplexität der Geschäfts- und Betriebssicherheit noch weiter erhöht. Darüber hinaus nimmt, wie wahrscheinlich jeder CISO bestätigen wird, die Zahl der Cyberangriffe, Cyberangreifer und offensiven Toolsets täglich zu.

Die in der Vergangenheit konzipierten Sicherheitstechnologien wurden nicht entwickelt, um mit der komplexen, sich schnell verändernden Bedrohungslandschaft von heute fertig zu werden. Die Beweise dafür sind eindeutig: Zunehmende Ransomware-Angriffe in Verbindung mit Datenverlusten und IP-Diebstahl, strapazierte SOC (Security Operations Center)-Teams, die sich mit Alarmmüdigkeit und Personalmangel auseinandersetzen müssen, und die steigende Anzahl von Angriffen, die trotz des Einsatzes traditioneller Sicherheitstools erfolgreich sind – das sind nur einige der Beispiele für weit verbreitete Probleme in der heutigen IT-Sicherheit.

XDR wurde speziell als Lösung für eben diese (und viele weitere) Probleme konzipiert. In diesem Beitrag soll erörtert werden, was XDR ist und wie der Ansatz einen Wandel in der Cybersicherheit herbeiführt, um die Sicherheitsteams von Unternehmen zu stärken und Cyberkriminelle in Schach zu halten.

Was ist XDR?

XDR steht für Extended Detection und Response und repräsentiert die Weiterentwicklung von EDR, der Endpoint Detection und Response. EDR, insbesondere ActiveEDR, brachte Sichtbarkeit und automatische Reaktion auf Vorfälle auf Endpunkten wie Laptops und Workstations. Das typische Netzwerk von heute verfügt allerdings über eine enorme Vielzahl verschiedener Datenpunkte, die von Angreifern auf dem Weg zu einem erfolgreichen Kompromiss ausgenutzt werden können, von Mobiltelefonen und IoT-Geräten bis hin zu Containern und Cloud-Nativen Anwendungen. Um diese komplexen Netzwerkumgebungen adäquat zu schützen, bedarf es eines neuen und moderneren Ansatzes.

Was man heutzutage als XDR bezeichnet ist ein Sicherheitsverfahren, das das althergebrachte EDR ersetzt, indem es Transparenz über alle Daten bietet, die das Netzwerk durchqueren, und nicht nur über die Daten der Endpunktebene. XDR-Plattformen wie die Singularity-Plattform von SentinelOne sammeln Daten von allen Assets in der gesamten Unternehmensumgebung, führen sie in einem einzigen Data Lake zusammen und wenden Sicherheitsanalysen und künstliche Intelligenz über mehrere Sicherheitsebenen hinweg an, um eine verbesserte automatische Erkennung und Reaktion auf Bedrohungen zu ermöglichen.

Die Weiterentwicklung von EDR

XDR ermöglicht eine schnellere, umfassendere und effektivere Erkennung und Reaktion auf Bedrohungen als EDR, basierend auf einem einzigen Pool von Rohdaten, die Informationen aus dem gesamten Ökosystem umfassen. Dabei werden verglichen mit EDR die Daten aus einem breiteren Spektrum von Quellen gesammelt und zusammengestellt.

Cyberangriffe betreffen in der Regel viele verschiedene Bereiche einer Organisation. Die durch XDR ermöglichte Transparenz ist die einzige Möglichkeit, einen vollständigen Überblick darüber zu erhalten, was, wann, wo und wie passiert ist. Dieselben kontextualisierten Handlungsstränge, die ActiveEDR auf der Endpunktebene bietet, können dann auf mehreren Ebenen erstellt werden: Cloud, Container, virtuelle Maschinen, IoT, Endpunkte, Server usw.

Diese umfassende Sichtbarkeit bringt eine Reihe von Vorteilen mit sich, unter anderem:

- bessere Erkennung verborgener Angriffe
- reduzierte Verweildauer von Daten und Analysen
- erhöhte Geschwindigkeit bei der Reaktion auf Angriffe

Durch die Kombination von Endpunkt-, Netzwerk- und Anwendungs-Telemetrie liefert XDR die Sicherheitsanalysen, die erforderlich sind, um dieses Rennen als Organisation mithilfe von verbesserter Erkennung, Einstufung und Reaktion für sich zu entscheiden.

Darüber hinaus verringert die Lösung dank KI und Automatisierung die Belastung der Sicherheitsanalysten durch manuelle Arbeit. Eine XDR-Plattform wie SentinelOne Singularity kann proaktiv und schnell ausgefeilte Bedrohungen identifizieren, die Produktivität des Sicherheits- oder SOC-Teams steigern und dadurch den ROI des Unternehmens massiv erhöhen.

XDR vs. SIEM

Obwohl sowohl XDR- als auch SIEM-Tools Daten aus verschiedenen Quellen sammeln, haben sie ansonsten wenig gemeinsam. Im Gegensatz zu einer XDR-Plattform haben SIEMs (ebenso wie passive EDR-Tools) weder die Fähigkeit, aussagekräftige Entwicklungstrends zu erkennen, noch bieten sie automatische Erkennungs- oder Reaktionsmöglichkeiten. Außerdem erfordern SIEM-Systeme ein hohes Maß an manuellen Nachforschungen und Analysen, um ihren Nutzen zu entfalten.

Wenn ein Unternehmen in SIEM-Tools investiert hat, heißt das jedoch nicht, dass sie durch die XDR-Plattform überflüssig werden. Sie können nämlich direkt in den Datenspeicher der XDR-Plattform eingespeist werden, wodurch alle Rohdaten dem KI und Machine Learning der XDR-Lösung zugänglich gemacht werden.

Woran erkennt man ein leistungsfähiges XDR-Produkt?

Das erste Merkmal einer effektiven XDR-Lösung ist die Art und Weise, wie sie in das Netzwerk integriert. Sie muss nahtlos über den Sicherheits-Stack hinweg funktionieren und native Tools mit umfangreichen APIs bereitstellen. Hüten sollte man sich vor unausgereiften Lösungen, die sich oft als nicht mehr als eine Reihe alter und zusammengeschraubter Tools herausstellen. Die eigene XDR-Lösung sollte eine einzige Plattform bieten, die es dem Unternehmen ermöglicht, einfach und schnell einen umfassenden Überblick über sämtliche Assets und Vorgänge zu erhalten.

Zweitens ist eine Automatisierung, die durch fortschrittliche KI und bewährte Machine Learning-Algorithmen unterstützt wird, unerlässlich. Hat der Anbieter eine reiche Geschichte in der Entwicklung modernster KI-Modelle, oder ist er in erster Linie für althergebrachte Ansätze bekannt und versucht nun lediglich auf den Zug moderner Technologien aufzuspringen?

Drittens: Wie einfach ist es, das Produkt zu verstehen, es zu warten, zu konfigurieren und zu aktualisieren?

Einer der Hauptvorteile einer starken XDR-Lösung ist die erhöhte Produktivität der Mitarbeiter durch automatische Erkennung und Reaktion. Gleichzeitig möchte man natürlich auch sicherstellen, dass die Sicherheitsverantwortlichen nicht durch die Verwaltung oder Navigation einer komplizierten Lösung unverhältnismäßig gefordert werden.

Der Ansatz von SentinelOne: eine KI-gestützte XDR-Plattform für alle Zwecke

Die KI-getriebene XDR-Plattform von SentinelOne bietet alle Vorteile, die man von einer Komplettlösung erwartet: weitreichende Transparenz, automatische Erkennung und Reaktion, umfassende Integration und einfache Bedienung. Mit einer einzigen Codebasis und einem einzigen Bereitstellungsmodell ist Singularity das erste XDR-System, das den IoT (Internet of Things)- und CWPP (Cloud Workload Protection Plattform)-Ansatz in einer einheitlichen Plattform vereint.

Alle IoT-Daten sind nahtlos in Singularity integriert, um das Threat Hunting zu erleichtern und einen vollumfänglichen Kontext zu ermöglichen. Durch den Einsatz der KI zur Überwachung und Steuerung des Zugriffs auf jedes IoT-Gerät ermöglicht Singularity XDR den Maschinen die Lösung von Problemen, die zuvor nicht in großem Maßstab gelöst werden konnten.

Die Container-Workload-Protection wird auf allen wichtigen Linux-Plattformen unterstützt, sowohl physisch als auch virtuell, bei nativen Cloud-Workloads und Kubernetes-Containern. Sie bietet Prävention, Erkennung, Reaktion und Verfolgung von bekannten und unbekannten Cyberbedrohungen. Dazu gehört der Schutz vor Malware und Live-Angriffen in Cloud-nativen und containerisierten Umgebungen und erweiterte Reaktionsoptionen sowie autonome Gegenmaßnahmen in Echtzeit.

Fazit

Cybersicherheit wird oft mit einem Wettrüsten zwischen Angreifern und Verteidigern verglichen. Dieses Wettrüsten geht nun über die Ebene des Endpunkts hinaus. Da Unternehmen vermehrt auf Remote- und Cloud-Infrastrukturen setzen und damit eine immer größere Angriffsfläche schaffen, kann eine integrierte Plattform die erforderliche Transparenz und automatisierte Abwehr über alle Ebenen hinweg bieten. Durch die Kombination von Endpunkt-, Netzwerk- und Anwendungs-Telemetrie liefert XDR die Sicherheitsanalysen, die erforderlich sind, um dieses Rennen als Organisation mithilfe von verbesserter Erkennung, Einstufung und Reaktion für sich zu entscheiden. □

Matthias Canisius, Regional Sales Director Central Europe bei SentinelOne.

Weitere Informationen unter
www.sentinelone.com

SentinelOne

SentinelOne™

HUNT CYBERCRIME WITH SUPERHUMAN PRECISION.

PREVENTION | DETECTION | RESPONSE | HUNTING

Advanced Endpoint Security
Next Generation EPP
+ActiveEDR

To learn more, visit
sentinelone.com

CYBERSPRINT

RISIKEN FINDEN, PROBLEME LÖSEN.

Übernehmen Sie die Kontrolle über den digitalen Fußabdruck Ihres Unternehmens.

LERNEN SIE IHREN DIGITALEN FUSSABDRUCK KENNEN UND LÖSEN SIE SO DIE KOMPLEXESTEN SICHERHEITSHERAUSFORDERUNGEN.

VERHINDERN

// Markenmissbrauch
// Third-Party Risk
// Datenlecks

VERWALTEN

// Digitale Bestandsinventur
// Risikoübersicht
// External Threat Intelligence

www.cybersprint.de

Digitaler Fußabdruck

Wenn Cyber-Sicherheit zur Grundlage für ein erfolgreiches Fortbestehen der Geschäftsentwicklung wird…

Cybersprint berichtet

Der digitale Fußabdruck ist kein neues Konzept. Traditionell bezieht er sich auf die hinterlassenen Spuren und Informationen, die über eine Person oder Organisation im Internet gefunden werden können. Im Kontext der Cybersicherheit bezieht sich der digitale Fußabdruck auf die mit der Marke verbundenen Daten.

Diese Daten lassen sich in zwei Kategorien gliedern. Zum einen sind es die Online-Organisationsdaten wie die Art der Produkte, Kunden- und Mitarbeiterdaten und die physische Adresse, die bei der Vorbereitung und Durchführung eines potenziellen Angriffs verwendet werden können. Zum anderen die digitalen Assets, die sie selbst kontrollieren können, und solche, die außerhalb des eigenen Kontrollrahmens liegen, z.B. im Fall von Outsourcing oder der Zusammenarbeit mit Cloud-Diensten.

Assets sind digitale Teile der Organisation, wie z.B. Web-Domains, Social Media Accounts, OT und Netblocks, die für einen optimalen Schutz vor Bedrohungsakteuren und Angriffen abgebildet, überwacht und konfiguriert werden müssen. Darüber hinaus bietet der digitale Fußabdruck Einblicke in die gesamte digitale Infrastruktur und hilft so, unternehmensweite Entscheidungen zu treffen.

Im Folgenden werden die Anwendungen des digitalen Fußabdrucks ins Verhältnis zu anderen Lösungen und seiner Position in der Threat Intelligence-Landschaft gesetzt. Was treibt den Bedarf für eine digitale Fußabdrucks-Lösung an und welche Herausforderungen werden damit angegangen?

Was ist der digitale Fußabdruck?

Ist der digitale Fußabdruck dasselbe wie die Angriffsfläche?

Ein bekannter Begriff, der dem Digital Footprint nahe kommt, ist die Angriffsfläche. Beide beziehen sich auf die Verwaltung von digitalen Assets, um die Möglichkeiten für Bedrohungsakteure einzuschränken. Der Umfang und die Nutzung des digitalen Fußabdrucks sind jedoch vielfältiger als bei der Angriffsfläche.

Der digitale Fußabdruck bildet die auffindbaren Organisationsdaten und deren Risiken ab. Schwächen zu erkennen, ist der erste Schritt für die Stärkung der Cyber-Resilienz. Dennoch benötigen nicht alle Assets den selben Schutz. Die Visualisierung des digitalen Fußabdrucks ist nützlich, um Projekte zu priorisieren. Sollte beispielsweise ein Asset mit einem Server verbunden sein, der auch kritischere Systeme hostet, kann die Risiko-Behebung dieses Assets direkt umgesetzt werden. Eine gute digitale Fußabdrucks-Lösung bietet auch Möglichkeiten zur Risikominimierung. Denn je besser Ihre Cybersicherheit von außen aussieht, desto weniger wahrscheinlich ist es, dass Bedrohungsakteure versuchen werden, Sie anzugreifen.

Der digitale Fußabdruck verbindet das digitale Risiko mit dem Geschäftsrisiko. Nicht nur aus einer Sicherheitsperspektive, sondern durch die Abbildung der Risiken innerhalb des digitalen Fußabdrucks wird deutlich, welche Systeme mehr Aufmerksamkeit als andere benötigen. Welche Software und (Sicherheits-)Werkzeuge sind aktiv? Sind diese noch ausreichend für ihre Aufgabe? Diese Daten helfen dabei, fundierte Entscheidungen zu treffen, z.B. ob betriebliche Ausfallzeiten wegen Patches oder Updates sich lohnen.

Zusätzlich zeigt der digitale Fußabdruck auch die Assets, die außerhalb des Kontrollrahmens der Organisation liegen. Ein Datenleck bei einer angeschlossenen Drittpartei, eine Phishing-Webseite oder ein Social-Media-Konto eines Nachahmers kann z.B. nur begrenzte oder gar keine digitalen Verbindungen zu den ursprünglichen Domänen haben und dennoch ein Risiko darstellen. Wenn eine solche Domain mit dem Markennamen verbunden ist, wird eine digitale Fußabdrucks-Lösung dies erkennen und melden. Selbst wenn sie sich tatsächlich außerhalb der direkten Angriffsfläche der Organisation befindet.

Unsere Definition des digitalen Fußabdrucks

Die Grundlage des digitalen Fußabdrucks jeder Organisation ist Dynamik. Er entwickelt sich ständig weiter, wächst oder schrumpft. Er ist unterschiedlich interpretierbar und kontextabhängig - und fast immer ist er größer als geschätzt.

Aus diesem Grund funktioniert die digitale Fußabdruck-Plattform von Cybersprint ohne einen vordefinierten IT-Rahmen. Durch die vorherige Skizzierung der Domänenbereiche wäre der Scan bereits begrenzt, was zur Nicht-Identifizierung von Risiken führen kann. Stattdessen werden alle Assets anhand Ihrer Marke erkannt und bewertet. Cybersprint simuliert so die Reconnaissance-Phase von Bedrohungsakteuren und ermöglicht Ihnen einen Perspektivwechsel, um Ihre Organisation besser zu schützen. Wir nennen dies einen Zero-Scope-Ansatz.

Die automatisierte Identifizierung und Kartierung Ihrer digitalen Assets setzt Ressourcen frei – Zeit und

Investments. Idealerweise ermöglicht ein Programm zur Erfassung des digitalen Fußabdrucks außerdem eine Integration mit anderen bereits vorhandenen Sicherheitssystemen, SIEMs und TIPs. Diese Überzeugungen sind grundlegend für unsere KI-gestützte Plattform. Zusätzlich bauen wir auf Analyst Intelligence (KI²), um wertvolle Ergebnisse für unsere Kunden zu liefern. So gelingt uns eine verlässliche digitale Bestandsaufnahme und die Verwaltung von Ausnahmen. Dabei greift unsere cloudbasierte Lösung nicht in Ihre bestehenden Prozesse ein wie zu installierende Software. Wir nennen dies Zero-Touch.

Was steckt hinter dem Bedarf für digitales Fußabdruck-Management?

Organisationen digitalisieren und lagern mehr und mehr ihrer Dienstleistungen aus. Daraus ergibt sich eine grundlegendere Verantwortung für IT-Sicherheitsexperten: Sie müssen dafür sorgen, dass Daten, Mitarbeiter und Kunden geschützt sind und dadurch die allgemeine Produktivität und Kontinuität des Unternehmens erleichtern.

Sie können dies nur dann effektiv tun, wenn sie die Kontrolle über IT-Prozesse behalten und einen aktuellen Überblick über alle digitalen Assets, Dritte und Lieferketten haben. Folglich müssen sie ihre Fähigkeiten ständig erweitern, entweder durch den Aufbau neuer Workflows in bestehenden Tools, durch das Hinzufügen weiterer Tools oder durch beides. Dieser Bedarf wird von drei Hauptfaktoren angetrieben: der Bedrohungslage, der technologischen Entwicklung und den regulatorischen Trends.

Die Bedrohungslage

Der Kampf zwischen den Bedrohungsakteuren und den Sicherheitspraktikern ist ein ständiges Hin und Her. Wenn ein Weg zu den Daten einer Organisation versperrt ist, werden die Akteure versuchen, einen neuen zu finden. Im Gegenzug wehren sich die Sicherheitspraktiker und versuchen stets, den Bedrohungen einen Schritt voraus zu sein.

Gegenwärtig findet eine Veränderung von CEO-Betrug hin zu Lieferantenbetrug statt. Beide beruhen auf Phishing-Taktiken. Darüber hinaus werden Angriffe auf die Lieferkette, Malware und Spionage bei Dritten als Sprungbrett in die Systeme von Organisationen benutzt.

Neue Bedrohungen bedeuten, dass andere Teile des Fußabdrucks sorgfältiger überwacht werden müssen, und zwar mit einem sich ebenfalls weiterentwickelnden Instrumentarium.

Entwicklung der Technologie

Das Schlüsselwort für die technologische Entwicklung ist "Digitalisierung". Organisationen durchlaufen kontinuierliche digitale Transformationen und verlagern mehr Dienste und Infrastruktur in Cloud-Umgebungen und zu externen Anbietern. Die zunehmende Komplexität der Cloud macht auch die Verwaltung und Überwachung des digitalen Fußabdrucks schwieriger.

Eine digitale Fußabdruck-Lösung passt sich diesen Veränderungen an. Der Zero-Touch-Ansatz folgt dem Fußabdruck dynamisch und verändert das Risiko und die Priorisierung entsprechend. So werden auch Sicherheitsrisiken in Umgebungen Dritter überwacht. Dies ermöglicht konstruktive Sicherheitsverbesserungen und Einblicke in die Einhaltung von Vorschriften bei Zulieferern.

Regulatorische Trends

Ein dritter Treiber ist der externe Schub durch Vorschriften. Versicherungsgesellschaften verlangen einen bestimmten Reifegrad, und staatliche Stellen verlangen Sicherheitsberichte, die belegen, dass die Organisationen die Kontrolle über ihre eigene Infrastruktur und die von Dritten haben. Ein solches Beispiel sind die Richtlinien der European Banking Association.

Daraus ergibt sich der Bedarf an kontinuierlichen Einblicken in alle angeschlossenen Systeme. Regelmäßige Prüfungen und Momentaufnahmen reichen nicht aus, um allen Anforderungen gerecht zu werden. Eine digitale Fußabdrucks-Lösung mit kontinuierlicher Überwachung und benutzerdefinierter Datenexportfunktionalität wird die GRC-Prozesse drastisch verbessern.

Digitaler Fußabdruck: Das Schweizer Armeemesser der Cybersicherheit

Der digitale Fußabdruck von Cybersprint dient als direkter Weg zur Stärkung Ihrer Sicherheitsarchitekturlösungen. Es gibt keinen Kompromiss zwischen Gründlichkeit und Häufigkeit der Scans. Viele Organisationen führen jährlich Pentests und einfache Oberflächenscans durch. Daraus ergibt sich eine große Lücke, die durch eine ständige Überwachung des digitalen Fußabdrucks geschlossen wird.

Die erzeugten Daten können nicht nur für operative (Sicherheits-)Zwecke verwendet werden, sondern bilden auch den Input, der für die Erstellung und Anpassung unternehmensweiter Prozesse benötigt wird. Sie dienen sowohl den Sicherheitspraktikern als auch dem leitenden Management.

Seine große Vielfalt an Anwendungsfällen und seine unternehmensweite Nutzbarkeit machen den digitalen Fußabdruck zu einer der wichtigsten und vielseitigsten Lösungen für Sicherheitsexperten von heute.
Fragen Sie einen unserer Vertreter im Chat nach einem für Ihre Organisation spezifischen Anwendungsfall. □

Weitere Informationen unter
www.cybersprint.com

CYBERSPRINT
BREAKTHROUGH SECURITY

Why modern SOCs aren't keeping up

To understand why this is, and how to change that reality, we need to look closely at the toolkit and process being used by these SOCs, and the challenges those present to analysts trying their best to do their jobs.

Tracking individually named APTs and/or crimeware gangs is a commonly discussed function for SOCs around the globe. A myriad of threat intelligence vendors tag their data with attribution details, MITRE's popular ATT&CK framework lists actors observed to be using individual TTPs, and upper-level management often responds to non-technical news articles discussing specific threat actors by asking whether those actors are being tracked by the people doing the actual work of keeping their organisations safe.

The reality, however, is that the majority of SOCs today are still not even at a point where they are able to review and respond to every alert being generated by their security tooling – let alone do anything proactive like tracking specific actors. To understand why this is, and how to change that reality, we need to look closely at the toolkit and process being used by these SOCs, and the challenges those present to analysts trying their best to do their jobs.

Security tools are noisy things, and an average SOC can easily see 10,000 alerts in a given day – while often being staffed with a single-digit number of analysts. To keep up with that pace, analysts would need to be resolving each of those events in a matter of seconds. The reality that we see instead is typically tens of minutes to resolve any given alert, even in SOCs whose SIEM is full of what's supposedly all the data necessary to understand and validate security alerts.

The reason for this lag is that the data in those SIEMs suffers from two major problems: a lack of standardisation, and a lack of completeness. Both of these problems stem from the way that the data is gathered. Potentially dozens of production systems – ranging from security tools and infrastructure appliances to application servers and endpoint software — must be configured to send data into the SIEM as a central aggregation point. These systems are created by different vendors, and log details in different formats and levels of detail, any of which are subject to change at any given time.

The majority of SOCs today are still not even at a point where they are able to review and respond to every alert being generated by their security tooling – let alone do anything proactive like tracking specific actors.

As a result, linking these logs together into a coherent base of knowledge becomes an outsized chore. Minor details like millisecond-level timestamp skew, time zone conversion issues, or loss of visibility due to a NAT boundary can make it painfully difficult to get to the data that an analyst needs to validate a given alert.

Sometimes the data that security analysts need is simply not present, either. Systems sending in logs are often owned by teams outside the SOC, who might accidentally or intentionally disable security logging – while failing to notify the SOC in a timely manner. Even worse, some log sources don't provide the information a security analyst needs even when they're fully operational. Most DNS server logs, for example, fail to include the answer to a query that was asked of them – which renders them useless for a security analyst trying to see if a connection was actually made to a malicious site.

Corelight data enables immediate SOC improvements

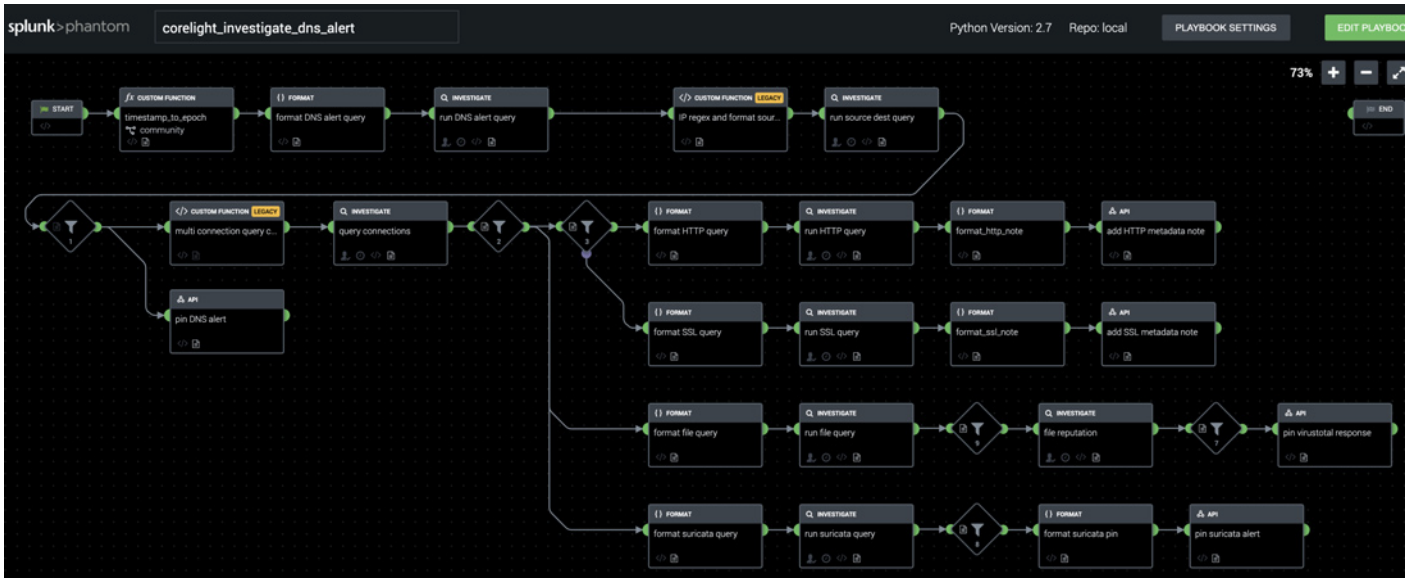
SOCs can resolve these operational pain points by shifting to a network traffic-centric logging model, enabled by open source Zeek (and its turnkey commercial implementation on Corelight appliances). Designed to parse live traffic streams and log relevant metadata across a wide variety of protocols, Zeek/Corelight is deployed out of band via packet broker/span/tap, and produces all of the network evidence a SOC could ever need to investigate a security event — in a single, standardised format that's designed for ease of access by incident responders and threat hunters alike.

That single source of data can be much more simply linked with detection tools for rapid investigation. In particular, Corelight has recently extended open source Suricata IDS by directly adding Zeek UIDs to alerts – which enables analysts to see all of the network telemetry related to those alerts in a single pivot.

This easy correlation of security events and data not only speeds up manual analyst tasks by simplifying processes – it drastically eases automation through SOAR. Powerful playbooks that speak to fundamental SOC processes can be written with fewer queries (for faster time to functionality and lower impact

Corelight reports

With simple plug and play integrations for most major firewall/NAC vendors included directly in Phantom, SOCs can easily extend this playbook to allow for remediation of confirmed-infected hosts.



on the SIEM), and without the constant worry of breaking because of a mundane change in data formats upstream.

Here again, Corelight is actively working to advance the state of the industry, by providing freely available Phantom playbooks that make use of our data for common workflows. These playbooks aim to be generically applicable across SOCs, while being easily customisable for a specific environment or workflow.

The example Corelight Phantom playbook shown here is designed to go after Suricata alerts on potentially malicious DNS queries – an extremely common yet surprisingly time-consuming type of event for most SOCs.

It begins by using the UID from the Corelight Suricata log to pivot directly into the linked DNS log, to determine whether any answer was received by the querying host; if not, processing is halted, since no connection is possible as a result, and thus the event is somewhere between irrelevant and very low priority. For each of the answered IP addresses, a query is made to the Connection log, to see if any sessions were established between the hosts in question. If any connections did occur, a set of indicators is pulled:

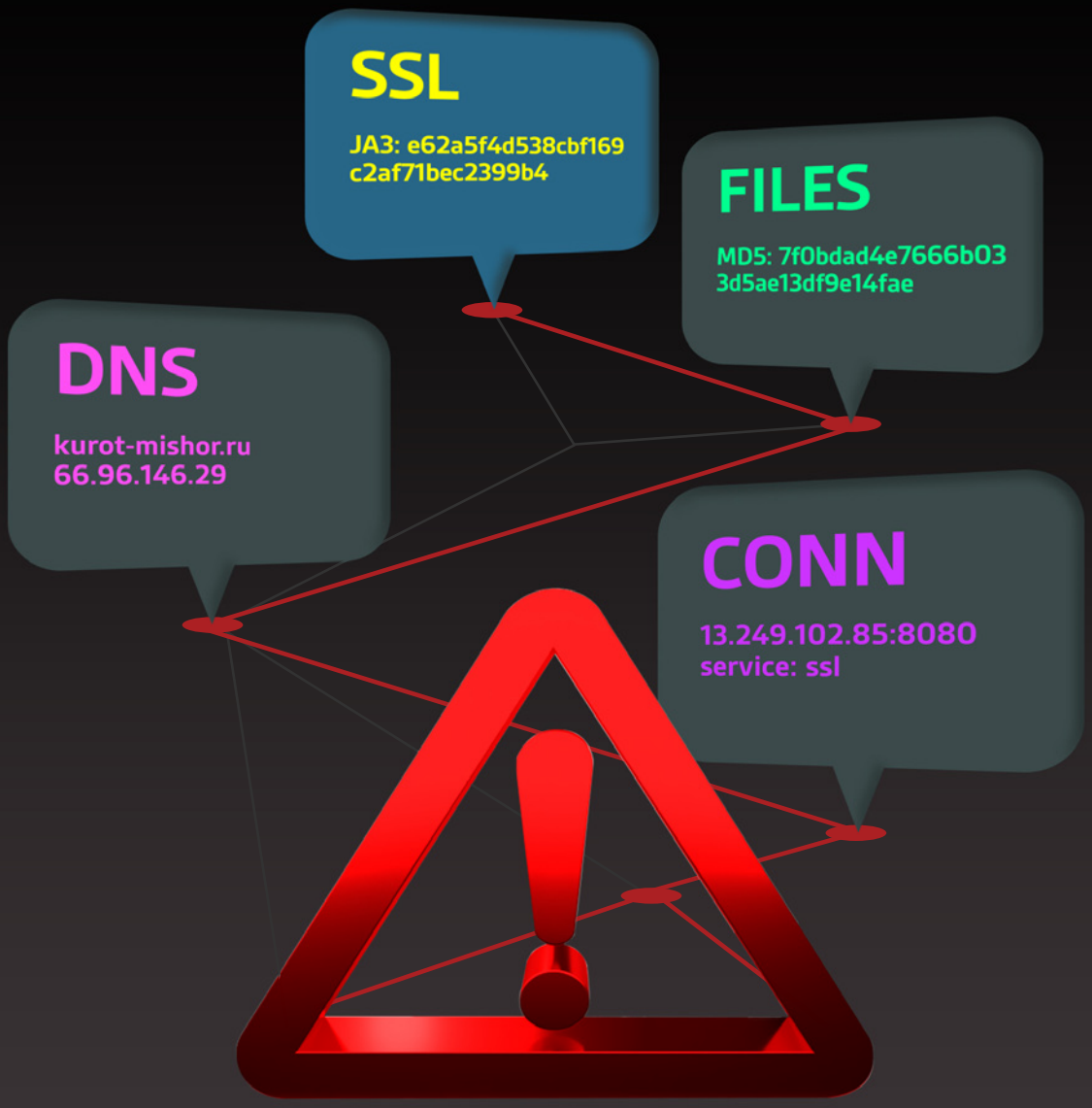
- HTTP details such as URI, Host, User-Agent, MIME type of files returned, etc.
- SSL details such as certificate validation status, JA3 hash, etc.
- If files were transferred, their SHA1 hashes – which have been pre-computed in the Corelight logs – are extracted and checked for reputation on VirusTotal
- All Suricata alerts between the two hosts are collected and displayed

All of this data is then presented to an analyst in a format that can be reviewed in a matter of seconds, with no need for a human to painstakingly construct searches or correlate results. Validation of potentially not just the original alert, but also others generated downstream, can take place quickly enough to match the pace at which alerts are being generated in the first place.

With simple plug and play integrations for most major firewall/NAC vendors included directly in Phantom, SOCs can easily extend this playbook to allow for remediation of confirmed-infected hosts. Corelight's second playbook, which prepares a full host history report for a suspect IP address, could also be kicked off to help determine the scope of the compromise. The playbook can even be adapted to work with other sources of DNS-based alerts with a simple re-working of the query into Corelight's DNS logs. □

For more information, please visit
corelight.com

corelight



THE END OF DEAD ENDS

SURICATA + zeek | No more alerts that go nowhere, no more investigations starved of data. Corelight merges the best open source Suricata alerts and Zeek evidence to propel your SOC team forward. **LEARN MORE** ›

corelight

The only universal security intelligence solution

Recorded Future – delivering relevant cyber-threat insights in real time.

Recorded Future reports

Who we are

Using a sophisticated combination of machine and human analysis, Recorded Future fuses the broadest set of open source, dark web, technical sources, and original research together to deliver relevant cyber-threat insights in real time. The Recorded Future Security Intelligence Platform aggregates this rich intelligence with any other threat data sources, which empowers security teams to collaborate on analysis and deliver intelligence wherever they need it most – including rapid integration with existing security solutions.

Security intelligence solutions

Security intelligence accelerates detection, decision-making, and response times by positioning comprehensive intelligence at the centre of your security workflows.

- *Threat intelligence:* Gain context on who is attacking you, their motivations and capabilities, and indicators of compromise to look for in your systems. This information is searchable in real time and presented in a single-pane-of-glass view and via customised alerts.
- *SecOps and response:* Discover previously unidentified threats and triage internal alerts in your SIEM based on rich external context and threat indicators correlated with internal threat data – so you can make faster, more confident decisions
- *Brand protection:* With real-time alerting, you can find things like leaked credentials, typosquat domains, social media accounts meant to impersonate an employee or brand, fake applications, threats to executives, and more. Takedown services go the last mile to simplify and expedite the removal of malicious content from the internet.
- *Vulnerability management:* Real-time risk scores based on real-life exploitability make it easy to prioritise where you should focus efforts and what you need to patch to prevent attacks. Real-time alerting on vulnerabilities affecting your tech stack provides new insights for effective risk reduction.
- *Third-party risk:* Make informed decisions to reduce your overall risk based on insights from real-time intelligence about the vendors and partner companies that form your business ecosystem – including vulnerable technologies, domain abuse, threats targeting the organisation, and more.

Intelligence-led security

Lead with intelligence across your security teams, processes, and workflows with security intelligence solutions from Recorded Future.

- Threat intelligence
- SecOps and response
- Brand protection
- Vulnerability management
- Third-party risk
- Geopolitical risk

- *Geopolitical risk:* Accelerate critical decision making with contextual data on threats, trends, sentiments, and evolving security situations – so you can protect your assets and understand shifting geopolitical dynamics in the geographic areas that matter to your organisation.

Innovative security intelligence technologies

Security Intelligence Graph

Recorded Future's unique ability to model all relevant security information available on the internet is what has set us apart since the beginning. With billions of indexed facts, and more added every day, the Recorded Future Security Intelligence Graph leverages a unique combination of patented machine learning and human analysis to provide you with unmatched insight into emerging threats that are relevant to your organisation.

Recorded Future Intelligence Cards™

Security teams gain instant context around suspicious observables and indicators with Recorded Future Intelligence Cards – with just one click. This innovation enables security teams to rapidly prioritise threats or dismiss false-positives using Recorded Future's dynamic risk scores. All of the evidence gathered by our Security Intelligence Graph is visible on these cards, allowing you to pivot quickly between indicators and attack methods, or vulnerabilities and exploits. □

For more information, please visit
www.recordedfuture.com

Recorded Future®

Recorded Future®

Elite Intelligence to Disrupt Adversaries

The World's Most Advanced Security Intelligence Platform

Powered by patented machine learning, the Recorded Future platform automatically collects and analyzes information from an unrivaled breadth of open, dark, and technical sources. Access context-rich, actionable intelligence in real time across your entire security ecosystem.

recordedfuture.com

Sponsoren und Aussteller

Corelight | Strategischer Sponsor

Corelight delivers powerful network traffic analysis (NTA) solutions that help organisations defend themselves more effectively by transforming network traffic into rich logs, extracted files, and security insights. Corelight Sensors are built on Zeek (formerly called 'Bro'), the open-source network security monitoring framework that generates actionable, real-time data for thousands of security teams worldwide. Zeek has become the 'gold standard' for incident response, threat hunting, and forensics in large enterprises and government agencies worldwide. Corelight makes a family of virtual and physical network sensors that take the pain out of deploying open-source Zeek and expand its performance and capabilities. Corelight is based in San Francisco, California and its global customers include Fortune 500 companies, large government agencies, and major research universities.

For more information, please visit www.corelight.com

Cybersprint | Strategischer Sponsor

Cybersprint befähigt Cybersecurity-Experten, von CISOs bis hin zu Analysten, relevante Risiken zu priorisieren. Wir bieten vollständige Transparenz - vom Risiko bis zur Sanierung - durch kontinuierliche Überwachung und Erkennung des digitalen Fußabdrucks in Echtzeit. Wir beziehen Ihre Marke, Organisation, Infrastruktur, VIPs, Dritte und mehr in unsere Analyse ein. Unsere KI-Tools korrelieren Dutzende von Datenquellen und verwenden eine Vielzahl von Scannern, wodurch Risiken relevant werden.

Mit der Plattform von Cybersprint können Sie Bedrohungen wie das Risiko von Dritten, Internetkriminalität, Markenmissbrauch, Datendiebstahl und mehr erkennen. Unsere Zero-Touch-Plattform lässt sich in wenigen Minuten installieren und kann mit Standard- oder maßgeschneiderten Services ergänzt werden, um Ihr Sicherheitsprogramm abzurunden.

Weitere Informationen unter www.cybersprint.de

Darktrace | Strategischer Sponsor

Darktraces selbstlernende Cyber-KI Platform basiert auf dem menschlichen Immunsystem und wird von über 4,000 Kunden weltweit genutzt, um sich gegen Bedrohungen für die Cloud, E-Mail, IoT, SaaS, Netzwerke und Industriesysteme zu schützen. Wir schützen unter anderem vor Insider Bedrohungen, Industiespionage, IoT-Kompromittierungen, Zero-Day Malware, Datenverlust, Lieferkettenrisiken und langzeitigen Infrastruktur-Schwachpunkten.

Das Unternehmen hat über 1,300 Mitarbeiter, 44 Niederlassungen und Hauptsitze in San Francisco und Cambridge, UK. All 3 Sekunden bekämpft Darktrace KI eine Cyber-Bedrohung, bevor sie Schaden anrichten kann.

Weitere Informationen unter www.darktrace.com/de

ExtraHop | Strategischer Sponsor

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Our breakthrough approach analyses all network interactions and applies cloud-scale machine learning for complete visibility, real-time detection, and guided investigation. With this approach, we help the world's leading enterprises including Home Depot, Credit Suisse, Caesars Entertainment, and Liberty Global to rise above the noise of alerts, organisational silos, and runaway technology. Whether you're investigating threats, ensuring the availability of critical applications, or securing your investment in cloud, ExtraHop helps you protect and accelerate your business.

Learn more at www.extrahop.com

Fidelis Cybersecurity | Strategischer Sponsor

Fidelis Cybersecurity ist ein führender Anbieter von Lösungen für Bedrohungserkennung, -bekämpfung und -abwehr. Fidelis bekämpft das gesamte Spektrum der Cyberkriminalität, des Datendiebstahls und der Spionage, indem es vollständige Transparenz in hybriden Cloud-/On-Prem-Umgebungen bietet, die Erkennung von Bedrohungen und Datendiebstahl automatisiert, die Bedrohungsjagd ermöglicht und die Reaktion auf Vorfälle mit Kontext, Geschwindigkeit und Genauigkeit optimiert.

Durch die Integration einer bidirektionalen Analyse des Netzwerkverkehrs in Ihrer Cloud und in internen Netzwerken mit E-Mail-, Web-, Endpunkt-Erkennung und -Reaktion sowie automatisierter Deception-Technologie erfasst die Fidelis Elevate™-Plattform umfangreiche Metadaten und Inhalte, die eine Echtzeit- und retrospektive Analyse ermöglichen und Sicherheitsteams die Plattform für eine effektive Erkennung von Bedrohungen in ihrer Umgebung bieten. Die Lösungen von Fidelis werden als eigenständige Produkte, als integrierte Plattform oder als 24×7 Managed Detection and Response Service angeboten, der die bestehenden Sicherheitsabläufe und Incident-Response-Funktionen ergänzt. Fidelis wird von Global 1000s sowie nationalen, regionalen Behörden als letzte Verteidigungslinie eingesetzt.

Unsere Herausforderung ist es, Ihnen zu helfen, Cyber-Angreifer bei jedem Schritt zu überwinden, auszumanövrieren und zu bekämpfen, um Ihre Geschäftsabläufe und Daten zu schützen. Unternehmen sind gegenüber ihren Cyber-Gegnern im Nachteil. Bedrohungen kommen aus allen Richtungen, und viele Unternehmen haben keinen vollständigen Überblick über ihr Cyber-Terrain, so dass Cyber-Angreifer sich unbemerkt auf die Lauer legen können, wenn sie es auf sensible Daten abgesehen haben oder versuchen, den Geschäftsbetrieb zu stören. Um den entscheidenden Vorteil zu erlangen, müssen Sicherheitsteams wie ihr Gegner denken. Das bedeutet, dass sie einen besseren Überblick über die verschiedenen Ebenen ihrer Umgebung haben und die Erkennungs- und Reaktionsfähigkeiten automatisiert skalieren können.

Weitere Informationen unter www.fidelissecurity.com

Palo Alto Networks | Strategischer Sponsor

Palo Alto Networks ist ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, das mit seinen bahnbrechenden Technologien die Weichen für die Cloud-orientierte Zukunft stellt und die Arbeitsweise von Unternehmen und ihren Mitarbeitern von Grund auf modernisiert. Das erklärte Ziel von Palo Alto Networks ist, zum bevorzugten Cybersicherheitspartner für Unternehmen zu werden und gemeinsam mit ihnen unseren digitalen Lebensstil zu schützen. Dazu geht das Unternehmen durch kontinuierliche Innovation die größten Herausforderungen rund um die Cybersicherheit an, mit denen Unternehmen derzeit konfrontiert sind. Dabei kommen die neuesten Forschungsergebnisse aus den Bereichen der künstlichen Intelligenz, Analysen, Automatisierung und Orchestrierung zum Einsatz. Mit einer integrierten Plattform und einem wachsenden Partnernetzwerk schützt Palo Alto Networks die Clouds, Netzwerke und Mobilgeräte von Zehntausenden von Unternehmen und arbeitet unermüdlich für eine Welt, in der jeder Tag ein bisschen sicherer ist als der Tag zuvor.

Weitere Informationen unter www.paloaltonetworks.com

Recorded Future | Strategischer Sponsor

Recorded Future delivers the world's most advanced security intelligence to disrupt adversaries, empower defenders, and protect organisations. With proactive and predictive intelligence, Recorded Future's platform provides elite, context-rich, actionable intelligence in real time that's ready for integration across the security ecosystem.

Learn more at recordedfuture.com

SentinelOne | Strategischer Sponsor

SentinelOne is the only cybersecurity solution encompassing AI-powered prevention, detection, response, remediation and hunting across endpoints, containers, cloud workloads, and IoT devices in a single lightweight autonomous and fully automated platform. With SentinelOne, organisations gain realtime full transparency into every activity happening across the network at machine speed – to defeat every attack, at every stage of the threat lifecycle.

To learn more visit www.sentinelone.com or follow us at @SentinelOne, on LinkedIn or Facebook

BeyondTrust | Bildung Seminar Sponsor

BeyondTrust ist der weltweit führende Anbieter für Privileged Access Management und bietet einen nahtlosen Ansatz, um Datenverstöße im Zusammenhang mit gestohlenen Daten, missbrauchten Privilegien und kompromittierten Fernzugriffen zu verhindern.

Unsere erweiterbare Plattform ermöglicht Unternehmen eine einfache Skalierung zur Absicherung von Privilegien, da sich Bedrohungen über Endpunkt-, Server-, Cloud-, DevOps- und Netzwerkumgebungen hinweg ebenfalls weiterentwickeln. Mit zentralisierten Management-, Reporting- und Analysefunktionen vereint BeyondTrust die branchenweit umfassendste Funktionalität für den Schutz privilegierter Zugangsdaten und ermöglicht IT-Verantwortlichen so, zielgerichtete und fundierte Maßnahmen zur Abwehr von Angreifern zu ergreifen. Unsere ganzheitliche Plattform zeichnet sich durch ihr flexibles Design aus, das technische Integrationen vereinfacht, die Produktivität der Nutzer steigert und IT- und Sicherheitsinvestitionen maximiert.

BeyondTrust gibt Unternehmen die erforderliche Sichtbarkeit und Kontrolle, um Risiken zu reduzieren, Compliance-Ziele zu erreichen und die operative Leistung zu steigern. Deshalb vertrauen uns 20.000 Kunden — einschließlich der Hälfte der Fortune-100-Unternehmen — und ein globales Partnernetzwerk.

Mehr erfahren Sie unter www.beyondtrust.com

IntSights | Bildung Seminar Sponsor

IntSights definiert Cyber-Sicherheit mit der ersten und einzigen Enterprise Threat Management Plattform der Branche, die relevante Bedrohungsinformationen in automatisierte Sicherheitsprozesse umwandelt.

Unsere einzigartigen Data-Mining Algorithmen sowie einzigartigen Cyber-Aufklärungsfunktionen überwachen kontinuierlich das digitale Unternehmensprofil unter der Oberfläche, im Deep und Dark Web, kategorisieren und analysieren zehntausende Bedrohungen, um durch Automatisierung den Bedrohungszeitraum zu verkleinern, Arbeitsabläufe zu optimieren und eine maximale Sicherung der Ressourcen und Geschäftsabläufe zu erreichen.

Das hat IntSights zu einem der am schnellsten wachsenden Cybersecurity-Unternehmen der Welt gemacht.

IntSights hat Niederlassungen in Amsterdam, Boston, Dallas, New York, Singapur, Tel Aviv und Tokio.

Weitere Informationen unter intsights.com

Kenna Security | Bildung Seminar Sponsor

Kenna.VM, eine Software-as-a-Service-Plattform (SaaS), sammelt sämtliche Schwachstellendaten über Infrastrukturen, Anwendungen, Container und das Internet der Dinge (Internet of Things, IoT) hinweg. Die speziell auf die einzigartige IT-Umgebung des Kunden abgestimmte Lösung von Kenna führt kontinuierlich Updates durch und identifiziert somit diejenigen 2 % der Schwachstellen, die zuerst eliminiert werden sollten.

Kenna kombiniert dazu mehr als 15 Feeds mit Informationen über Angriffe, mehr als sieben Milliarden gemanagte Schwachstellen, globale Angriffstelemetrie und Informationen über die Beseitigung, um reale Aktivitäten in Verbindung mit Attacken über die weltweite Angriffsfläche des Unternehmens hinweg präzise nachzuverfolgen und zu messen. Anhand prädiktiver Modellierungstechnologie ermöglicht Kenna.VM zudem die genaue Vorhersage des zukünftigen Risikos von Schwachstellen, sobald diese festgestellt werden. Dies erlaubt es Unternehmen, Risiken proaktiv zu managen und Berichte über diese zu erstellen.

Mit mehr als 55 vorgefertigten Konnektoren für mehr als 30 Anbieter bietet Kenna Kunden den umfassendsten Überblick über Risiken über den gesamten Stack hinweg, von Schwachstellen-Scannern bis zu SAST-, DAST- und SCA-Sicherheitstest-Tools, Bug-Bounty-Programmen und Konfigurationsmanagement-Datenbanken (CMDBs).

Weitere Informationen unter www.kennasecurity.com

Onapsis | Bildung Seminar Sponsor

Onapsis schützt die Applikationen der weltweiten Wirtschaft. Um Risiken frühzeitig zu erkennen, bietet die Onapsis Plattform umsetzbare Einblicke, sicheres Veränderungsmanagement, automatisierte Verwaltung und kontinuierliche Überwachung. Arbeitsabläufe werden optimiert, Änderungen kontrolliert und die Berichterstattung automatisiert. Onapsis ermöglicht es seinen Kunden, die Modernisierung von SAP-Systemen und der Oracle E-Business Suite, sowie Cloud-Initiativen zu übernehmen und voranzutreiben. ERP, CRM, PLM, HCM, SCM, BI und Cloud-basierte Anwendungen sind geschützt und compliant.

Mit Hauptsitz in Boston und Regionalbüros in Heidelberg und Buenos Aires, betreut Onapsis mehr als 300 der weltweit führenden Firmen und Organisationen, darunter viele der Global 2000. Durch einzigartige strategische Allianzen mit führenden Beratungs- und Wirtschaftsprüfungsunternehmen wie Accenture, Deloitte, IBM, Infosys, PwC und Verizon sind die Lösungen von Onapsis zum de-facto-Standard geworden, um Unternehmen beim Schutz dessen zu unterstützen, was am wichtigsten ist.

Weitere Informationen erhalten Sie über Twitter oder LinkedIn oder besuchen Sie uns unter www.onapsis.com

Snyk | Bildung Seminar Sponsor

Snyk is a developer-first security company that helps software-driven businesses develop fast and stay secure. Snyk seamlessly and proactively finds and fixes vulnerabilities and license violations in open source dependencies and container images.

Get started with Snyk for free, visit snyk.io

Synack | Bildung Seminar Sponsor

Synack bietet eine neue und revolutionäre Plattform für Sicherheitstests, konzipiert, um schwerwiegende Sicherheitslücken in geschäftskritischen Anwendungen und Infrastrukturen ausfindig zu machen und zu beheben, die ansonsten unerkannt bleiben. Synack gibt Kunden große Teams aus internationalen, hochkarätigen Sicherheitsexperten an die Hand, die die IT-Assets auf Kundenseite prüfen – unter Berücksichtigung eines mehrschichtigen und kontraindikatorischen Ansatzes – und Schwachstellen oft innerhalb von Stunden aufdecken.

Das, in Verbindung mit der Entwicklung einer selbstlernenden, auf Datenanalyse beruhenden Aufklärungstechnologie und einer transparenten, KI-basierten Plattform mit einem Echtzeit-Kundenportal, macht Synack zum Anbieter einer innovativen und effektiven Methode für Sicherheitstests. Diese Testplattform der nächsten Generation überwindet die Defizite herkömmlicher Penetrationstests und der Überprüfung auf Sicherheitsrisiken. Darüber hinaus bietet sie den Vorteil beispielloser Simulationen von immer komplexeren Cyberangriffen und TTPs, sprich Taktik, Technik und Prozeduren.

Synack hält seinen Kundenstamm vertraulich. Darunter befinden sich einige der größten F500-/G500-Konzerne, darunter Banken und Finanzdienstleister, Handelsunternehmen, Vertreter der Gesundheitsbranche, Konsumgüterkonzerne, Fertigungs- und Technologieunternehmen sowie die US-Regierung (das Verteidigungsministerium/das Projekt „Hack the Pentagon", die Steuerbehörde IRS). Gegründet wurde das Unternehmen Synack im Jahr 2013 von den ehemaligen NSA-Sicherheitsexperten Jay Kaplan, CEO im Unternehmen, und Dr. Mark Kuhr, in der Rolle des CTO.

Synack bietet seine Lösung in Form eines Abonnements für fortlaufende Sicherheitstests an – um den Schutz geschäftskritischer Assets zu gewährleisten. Für Assets, die zeitpunktgenaue Tests erfordern, gibt es die Möglichkeit eines 14-Tages-Sicherheitstests.

Wenn Sie mehr erfahren möchten, besuchen Sie unsere Website unter www.synack.com

AGENDA

08:00 Login und Networking

08:50 Begrüßung

09:00 **Unsere Herausforderungen in der IT: Angriffs-Szenarien**

Ernestine Schikore, Informationssicherheitsbeauftragte CISO, Universität Basel

- Schwachstellen: Fallbeispiel «WannaCry»
- Herausforderung der Verwendung von AD: Ausnutzen von Account-Rechten
- Bedeutung der zentralen Log-Infrastruktur

09:20 **CORTEX secures the future**

Stefan Schinkel, Director Cortex Central Europe, Palo Alto Networks

Security Operations Centres (SOCs) are characterised by chaos, struggling with siloed tools, manual processes, and reliant on the old premise of high-volume, low-fidelity rule-based correlation for everything from detection to investigation. This session details the building blocks of simpler, and more effective security operations and how SOCs transform to an automated proactive model by spending less time on manual reactive processes and more on hunting for unknown threats and transferring knowledge gained into future improvement.

- Simplify operations across networks, clouds and endpoints
- Trusted intelligence with automation
- Rapidly respond to threats with deep visibility, flexibility and contextual insight
- Arm your security team with integrated best-in class detection, investigation and threat intelligence

09:40 **Current pricing models for cyber-attacks**

Abdelkader Cornelius, Threat Intelligence Analyst, Recorded Future

- Why ransomware attacks are so lucrative and easy
- How volatile the price structure is, and also the supply and demand dynamics
- How the prices commanded by threat actors has developed over the last two years

10:00 **Internationale Datenübertragung**

Andreas Lober, Partner, BEITEN BURKHARDT

- Wie Schrems II die internationale Datenübertragung zunichte gemacht hat
- Warum die Übertragung von Daten in die USA so schwierig geworden ist
- Warum Sie China und andere nicht vergessen sollten
- Wie Cloud Services und SaaS beeinflusst werden
- Warum die Behörden sagen, dass sogar Videokonferenzen illegal sind

10:20 **Bildungsseminare | Block 1** **Siehe Seite 26–27 für weitere Details**

BeyondTrust

Effektive Sicherheit: Least Privilege als wichtiger Bestandteil Ihrer PAM-Strategie

Mohamed Ibbich, Senior Technology Consultant, BeyondTrust

Snyk

Enterprise security – securing cloud-native applications at scale

Mathias Conradt, Sr. Solutions Engineer (DACH), Snyk

10:50 Kaffeepause und Networking

11:20 **PODIUMSDISKUSSION** **Das Blatt für den Überwachungskapitalismus wenden**

Maximilian Schrems ist noch nicht fertig. Tatsächlich hat er vielleicht gerade erst angefangen. Und der Ball, den er den Hügel hinuntergeschoben hat, gewinnt an Geschwindigkeit. Von ihren Steuerangelegenheiten über ihre aufsichtsrechtliche Arbitrage bis hin zur Nutzung von urheberrechtlich geschütztem Material und personenbezogenen Daten sowie den Problemen im Zusammenhang mit gefälschten Nachrichten und politischen Störungen werden Social-Media-Modelle angegriffen. Für CISOs, DPOs und andere Sicherheits- und Datenschutzfachleute bedeutet dies einen fortgesetzten (globalen) regulatorischen Fokus auf den Datenschutz sowie eine zunehmende Sensibilität von Kunden und anderen Stakeholdern für die Sicherheit ihrer Daten. Es kann auch ein Strafvollstreckungs Regime Vorboten. In diesem Panel untersuchen wir, wie sich Schrems II heute auf Sie auswirkt, und werfen einen Blick auf die Zukunft von Daten aus Sicherheits- und Datenschutzsicht.

Steffen Siguda, Corporate InfoSec Officer, OSRAM Licht AG
Hermann Huber, CISO, Hubert Burda Media KG

11:40 **Die Evolution der Endpunktsicherheit – Von EPP über EDR zu XDR**

Matthias Canisius, Regional Director Central Europe, SentinelOne

- Warum AV tot ist und wie sich Endpunktsicherheit in den letzten Jahren weiterentwickelt hat
- Was eine Endpoint Protection Platform (EPP) von Endpoint Detection and Response (EDR) unterscheidet
- Die Vorteile einer komplett integrierten XDR-Plattform gegenüber herkömmlichen EPP und EDR Lösungen

12:00 **Talking to the Board: the new realities of IT security**

Jamie Moles, Senior Security Engineer, ExtraHop

- The large-scale adoption of work-from-home technologies, heightened activity on customer-facing networks, and greater use of online services has greatly increased the risk of misconfigurations and cyber-threats
- Hackers have taken advantage of these new vulnerabilities and in recent weeks, ransomware attacks have affected several major organisations
- When attacks like these make headlines, board members have one question for CISOs: how can we be sure that won't happen to us?
- Join to hear top strategies for CISOs to lead board-level conversations about risk management amidst the stark new realities of IT

12:20 **Schützen der dynamischen Belegschaft mit Cyber-KI**

Mariana Pereira, Director of Email Security Products, Darktrace

- Trends & Herausforderungen der digitalin Zusammernarbeit
- Wie KI Ihre dynamische Belegschaft schützen kann
- Automatisierte Untersuchung und Reaktion mit Cyber-KI

12:40 **Bildungsseminare | Block 2** **Siehe Seite 26–27 für weitere Details**

IntSights	**Onapsis**
Working from home is not safe for work	**Bedrohungen für Ihre SAP-Systemlandschaft 2021 (EN)**
Etay Maor, Chief Security Officer, IntSights	**Frederik Weidemann,** Chief Technical Evangelist, Onapsis Inc

13:10 Mittagspause und Networking

14:10 **PODIUMSDISKUSSION** **Das Unerwartete zu erwarten, zeigt einen durch und durch modernen Intellekt**

Oscar Wilde hätte wahrscheinlich nicht das Leben eines CISO gewählt, aber er hatte Recht damit, wie sie die Welt sehen sollten. Der Solar Winds-Hack macht die Sicherheit zu dem Problem, das es immer hätte sein sollen. Erzwungene Digitalisierung von allem von der Kundenschnittstelle zu Supply Chain Management macht jedes Element der meisten Unternehmen eine Cyber-Angriffsfläche. Das IoT, besser gedacht als ein unendliches Ökosystem von Sensoren, tut dasselbe, während es Geschäftsmodelle wie Versicherungen auf den neuesten Stand bringt. Und es scheint, als ob WFH, COVID und eine Fortsetzung der On/Off-Fern- und Hybridarbeit noch viele Monate bei uns sind. Was denken Ihre CISO-Kollegen, was 2021 bringen wird? Und wie wollen sie diesen Herausforderungen begegnen?

Ernestine Schikore, Informationssicherheitsbeauftragte CISO, University of Basel
Klaus Nötzel, CISO, EUMETSAT
Marcel Zumbühl, CISO, Swiss Post

14:30 **Gegenwärtige und zukünftige Angriffsfaktoren: Die Risiken für die Internet-Hubs in Deutschland und deren Schutz**

Eward Driehuis, Senior Vice President Strategy, Cybersprint

- Deutschlands Rolle im „internationalen Internet"
- Die 3 größten Risiken, die damit verbunden sind
- Wie Kriminelle diese Risiken missbrauchen
- Was Sie tun können, um Ihre Organisation zu schützen

14:50 **The SOC that cried wolf**

Achim Kraus, Solutions Engineering CEEUR, Corelight Inc.

- How and what causes the signs of fatigue and consequences in the SOC?
- What can you do in order to keep pace instead of exchanging technologies?
- How do I achieve the required decision-making quality with my resources?
- The normalisation and completion of necessary data for the larger whole
- See – Decide – Act: Out-of-the-box, but yet open, flexible, integrable?

15:10 **Bildungsseminare | Block 3** **Siehe Seite 26–27 für weitere Details**

Kenna Security	**Synack**
Ein neuer Ansatz zur Lösung des Patch-Problems	**Next generation offensive security testing**
Stephen Roostan, VP EMEA, Kenna Security	**Thomas Hornung,** Solutions Architect EMEA, Synack

15:40 Kaffeepause und Networking

16:00 **Die Verteidigung von Unternehmen gegen das umfassende Spektrum von Cyber-Bedrohungen**

Chris Kubic, Chief Information Security Officer, Fidelis Cybersecurity

Die Bedrohungslandschaft entwickelt sich unentwegt weiter und unsere Umgebungen werden immer komplexer und schwieriger zu verteidigen. Angesichts des Ausmaßes und der Raffinesse der jüngsten Angriffe, die unsere Sicherheitswelt erschüttern, stellt sich die Frage, was CISO's und Security Operation Teams tun können, um das Spielfeld zu ebnen und Ihre Unternehmensumgebungen gegen Bedrohungen zu verteidigen, die von Cyberkriminellen, raffinierten und heimlichen staatlich organisierten Angreifern, Insidern, Drittanbietern und Wertschöpfungsketten ausgehen. In seinem Vortrag wird Chris aufzeigen, was wir tun können, um uns besser gegen das gesamte Spektrum dieser Bedrohungen zu schützen.

- Sorgfältiges Patchen von geschäftskritischen und angreifbaren Systemen
- Frühzeitige Erkennung und Bestätigung von untypischen Aktivitäten
- Ein gut durchdachter Plan für den Fall, dass Sie das nächste Opfer einer Datenpanne werden

16:20 **Ransomware im Rampenlicht: die polizeiliche Perspektive**

Peter Vahrenhorst, Kriminalhauptkommissar, Landeskriminalamt Nordrhein-Westfalen

- Ransomware ist immer noch die Geißel von IT-Systemen, auch oder gerade in Zeiten der Pandemie. Warum?
- Schritte zur wirksamen Prävention und Schadensreduzierung: Vorbereitung auf das Worst-Case-Szenario
- Ein Einblick aus der Perspektive der Polizeiarbeit

16:40 **Cybersecurity in the age of disorder**

Simon Brady, Managing Editor, AKJ Associates Ltd

Pandemic, digitalisation, climate change, the collapse of Chimerica, Brexit – the list goes on. In all this chaos, cybersecurity, like everything else, has to change. But how? In this session, AKJ's Managing Editor, Simon Brady, gives his take on where CISOs should be looking in 2021.

- Stop talking about 'the business' and start understanding it
- From facilities management to strategic advisory, or….?
- Cyber ROI is dead, good riddance to bad rubbish?
- Making use of enforced transparency: a new solution paradigm

17:00 Schlußbemerkungen

17:05 Networking

17:30 Konferenz Ende

Bildungsseminare

Im Laufe des gesamten Tages werden, als Teil der Agenda, eine Reihe von Bildungsseminaren stattfinden. Die Konferenzteilnehmer haben die Möglichkeit selbst zu bestimmen welche Seminare sie besuchen möchten. Die Bildungsseminare bieten gleichermaßen herstellerneutrale und praktische Empfehlungen. Die Seminare innerhalb eines Blockes finden zeitgleich statt.

Block 1: 10:20–10:50

BeyondTrust

BLOCK 1
10:20–10:50

Effektive Sicherheit: Least Privilege als wichtiger Bestandteil Ihrer PAM-Strategie

Mohamed Ibbich, Senior Technology Consultant, BeyondTrust

Es wird immer schwieriger ein gutes Gleichgewicht der Rechteverteilung für Mitarbeiter und Administratoren zu finden. Benutzer sowie auch IT-Administratoren sollten ausreichend Berechtigungen erhalten, um ihre Arbeit produktiv ausführen zu können, wobei gleichzeitig das IT-Sicherheitsrisiko miniert und sensible Daten sowie Systeme geschützt werden müssen. Angreifer sind Organisationen oft einen Schritt voraus. Selbst diejenigen mit den umfassendsten IT-Sicherheitssystemen und Kontrollmechanismen befürchten, dass ein Angreifer eine Schwachstelle entdecken und ausnutzen könnte. Dieser Vortrag erläutert praktische Hilfestellungen, mit denen Unternehmen branchenweit anerkannte Best Practices rund um das Thema Endpoint Privilege Management und grundlegende Sicherheitskontrollen implementieren können, um IT-Systeme und -Daten vor den meistverbreiteten Angriffen zu schützen.

Es enthält Empfehlungen zur erfolgreichen Implementierung einer Least-Privilege-Strategie, mit der Sie überflüssige Berechtigungen beseitigen können. Ebenso kann eine Erhöhung der Rechte auf mehreren Plattformen und vernetzten Geräten erfolgen, ohne die Produktivität der Endbenutzer zu beeinträchtigen.

Der Vortrag informiert über:

- Empfehlungen zur Implementierung grundlegender Sicherheitskontrollen
- Best-Practice-Beispiele rund um das Thema Endpoint Privilege Management
- Tipps zur erfolgreichen Umsetzung einer Least-Privilege-Strategie (Prinzip der geringsten Berechtigungen)

Snyk

BLOCK 1
10:20–10:50

Enterprise security – securing cloud-native applications at scale

Mathias Conradt, Sr. Solutions Engineer (DACH), Snyk

Join this session to learn:

- How DevSecOps is being used to secure cloud-native applications
- Cloud-native architecture is improving time to capability at a reduced cost for the enterprise
- Unify your dev team around a secure deployment approach with cloud-native architecture such as containers

Block 2: 12:40–13:10

IntSights

BLOCK 2
12:40–13:10

Working from home is not safe for work

Etay Maor, Chief Security Officer, IntSights

- How threat actors leverage threat intelligence
- New emerging threats for the remote work force
- What security professionals need to ask themselves to better understand their security posture

Onapsis

BLOCK 2
12:40–13:10

Bedrohungen für Ihre SAP-Systemlandschaft 2021 (EN)

Frederik Weidemann, Chief Technical Evangelist, Onapsis Inc

In den letzten Jahren wurden laut einer IDC Forschungsstudie 64% der ERP-Systeme von Unternehmen angegriffen.

Ist Ihnen bewusst, wie Angreifer in ungeschützte SAP-Landschaften eingedrungen sind und in diese einbrechen könnten?

Nehmen Sie an dieser Session teil, um Einblicke zu gewinnen:

- Wie Angriffe auf Ihre SAP-Systeme aussehen können
- Welche Sicherheitsherausforderungen in SAP-Umgebungen bestehen (z. B. S/4HANA)
- Zuversichtlich in die Cloud – wie man Sicherheit in hybriden Landschaften schafft
- Wege zum Schutz Ihres Unternehmens

Block 3: 15:10–15:40

Kenna Security

BLOCK 3
15:10–15:40

Ein neuer Ansatz zur Lösung des Patch-Problems

Stephen Roostan, VP EMEA, Kenna Security

In dieser Sitzung wird erklärt, warum der Bereich des Schwachstellenmanagements bislang nicht genutzte Möglichkeiten bietet, das Risiko messbar zu senken und Betriebskosten zu sparen.

- Strategische und taktische Vorteile der Entwicklung eines neuen Ansatzes
- Veränderung der Einstellung aller Interessengruppen hinsichtlich Patches
- Nutzung bestehender Investitionen mit zukunftssicheren, flexiblen Tools
- Festlegung – und Erreichung – der geeigneten Erfolgsmetriken für Ihr Unternehmen

Synack

BLOCK 3
15:10–15:40

Next generation offensive security testing

Thomas Hornung, Solutions Architect EMEA, Synack

Die Informationsflut in der Cyber Security ist dramatisch angestiegen und macht es extrem schwierig sich auf die wirklich kritischen Punkte zu konzentrieren. Herkömmliche Pen Testing Ansätze reichen sehr oft nicht mehr aus, daher beschäftigen sich Unternehmen zunehmend mit den Möglichkeiten des crowdsourced Security Testing. Die Zielsetzung ist es proaktiv Risikoquellen schneller zu identifizieren, zu priorisieren und zu beheben. Und dies Remote aber basierend auf einer vertraulichen Zusammenarbeit und sicheren Plattform.

In dieser Session erfahren Sie mehr über:

- Einen revolutionären Ansatz Security Testing durch ein internationales, geprüftes Team von Top Security Researchern durchführen zu lassen – um die wirklich kritischen Schwachstellen in kürzester Zeit zu finden und zu beheben
- Wie Sie die Synack remote Security Testing Plattform für sich nutzen, um Ihre Security Resourcen erheblich zu steigern
- Eine Reihe von Use Cases und PoC's von anderen europäischen Synack Kunden □

Sprecher

Die e-Crime & Cybersecurity DACH freut sich die Konferenzteilnehmer und -sprecher Willkommen zu heißen. Die Verstaltung versammelt regelmäßig Entscheidungsträger und Schlüsselpersonen verschiendener Industrien.

Matthias Canisius

Regional Director Central Europe, SentinelOne

Seit 2018 ist Matthias Canisius Regionaldirektor Mitteleuropa bei SentinelOne und verantwortlich für das strategische und operative Geschäft in Deutschland, Österreich und der Schweiz. Matthias verfügt über mehr als 20 Jahre Erfahrung in verschiedenen Geschäftsentwicklungs- und Vertriebsfunktionen in führenden IT-Sicherheitsunternehmen wie Palo Alto Networks, F5, Juniper oder Check Point.

Mathias Conradt, Sr.

Solutions Engineer (DACH), Snyk

Als Senior Solutions Engineer (DACH) arbeitet mit Snyk-Interessenten zusammen, um ihre technischen Anforderungen zu verstehen und diese bestmöglich in einer Software Security-Lösung abzubilden. Er verfügt über mehr als 20 Jahre Berufserfahrung im Bereich Software-Engineering und IT-Projektmanagement und besitzt diverse Zertifizierungen (AWS, CSM, CSP, CIPT, PRINCE2, ITIL, u.a.). Sein derzeitiger Schwerpunkt liegt auf Cybersecurity im Allgemeinen, wobei er sich auf Open Source Security, SCA, SAST sowie Open Source Lizenz-Compliance spezialisiert hat. Mathias ist regelmäßiger Speaker bei diversen Security-bezogenen Branchenveranstaltungen. Durch seine fast zehnjährige Tätigkeit im Ausland (Hongkong, China, Macau, Schweiz) und in verschiedenen Rollen hat er ein sehr breites Spektrum an interkulturellem Wissen und Erfahrung erworben. In seiner Freizeit treibt er gerne Sport, fährt Motorrad, und hält sich über die neuesten Technologien auf dem Laufenden.

Abdelkader Cornelius

Threat Intelligence Analyst, Recorded Future

Abdelkader is an industry leading Threat Intelligence and Cybercrime Researcher. Over the last 15 years, he has collaborated with numerous enterprise organisations, investigative authorities and law enforcement agencies to identify and eliminate cyber-threats across Europe. He has real-world experience of working on blue, red, and purple teams to test the effectiveness of security programs to defend against attackers.

Eward Driehuis

Senior Vice President Strategy, Cybersprint

Eward Driehuis ist mit mehr als 24 Jahren Erfahrung ein Veteran in der IT-Sicherheit. Er selbst beschreibt sich als Mann "mit technischem Herzen, Design-Mentalität und Geschäftssinn". Als SVP Strategy bei Cybersprint analysiert Eward Driehuis verschiedenen Aspekte und Entwicklungen innerhalb der Cybersicherheits-Branche. Er ist ein begeisternder Redner in den Medien und Präsentator bei internationalen Veranstaltungen wie der RSA und dem FS-ISAC. Dabei kann er auf seine langjährige Erfahrung im Kampf gegen Cyber-Bedrohungen zusammen mit Strafverfolgungsbehörden, Finanzorganisationen und Unternehmen zurückgreifen. Eward verfügt über eine nachgewiesene Erfolgsbilanz bei der innovativen Führung von Start-ups und Großunternehmen. Als CTO und Business Director bei mehreren IT- und Softwareunternehmen leitete er bereits Threat Intelligence- und Advanced Analytics-Produktabteilungen und war als CMO und Forschungsleiter bei einem der größten Anbieter von Cybersicherheit in Europa tätig.

Thomas Hornung

Solution Architect EMEA, Synack

Thomas Hornung ist ein IT-Experte mit über 20 Jahren Erfahrung in den Bereichen IT-Sicherheit, Infrastruktur und Service-Management. Er hat zahlreiche Unternehmen in ganz Europa dabei unterstützt, ihre Anforderungen zu verstehen, abzubilden und zu adressieren, insbesondere in den Bereichen Vulnerability Management, Endpoint Security, Critical Communications und Privileged Account Management. Heute konzentriert er sich als Solution Architect bei Synack darauf, Organisationen bei der Definition und Vorbereitung von Pentests zu unterstützen.

Hermann Huber

CISO, Hubert Burda Media KG

Hermann Huber Jahrgang 1961 begann seine berufliche Karriere mit einer Ausbildung zum Elektroniker bei der

Firma SEL/Alcatel in Stuttgart und bekam hierbei früh Kontakt mit dem internationalen Geschäft im Bereich der Nachrichtentechnik. Später studierte er nach einer mehrjährigen internationalen Bundeswehrzeit (schnelle Eingreiftruppe) Elektrotechnik und Informatik. Als ausgewiesener Spezialist im Bereich IT-Security und Datenschutz führte er von 1996-2011 das Systemhaus Intastic GmbH und wurde 2007 -2011 von deren Muttergesellschaft der Ecounion AG zum CTO später CEO berufen.

Nach einem Sabbatical Jahr (Geburt des Sohnes) folgte Hermann Huber dem Ruf zum IT Security Officer und Data Privacy Officer International, bei der J.Schmalz GmbH in Glatten.

Der erfolgreiche Aufbau der internationalen IT Security und Data Privacy Struktur innerhalb einer internationalen Mittelstandsgesellschaft konnte im Jahr 2015 mit dem 1. Preis „Sicherheitspreis Baden Württemberg" nachgewiesen werden.

Im September 2019 berief die Firma Burda Herrn Huber zum CISO. In seiner Freizeit beschäftigt sich Hermann Huber sehr stark mit dem Thema Psychologie, welches er nebenberuflich studiert und geschickt mit Technologiefragen „Mensch-Maschine-Schnittstelle" verknüpfen kann.

IT-Security und Industrie 4.0 ist zu einem großen Prozentsatz mit Organisation und dem Menschen verbunden. Herr Huber prägt daher den Begriff „Human Sensor" sehr stark.

Herr Huber spricht mehrere Sprachen, darunter Deutsch, Englisch, Niederländisch, Französisch und etwas Italienisch. Verschiedene Zusatzausbildungen im Bereich von Betriebssystemen, ITIL Servicemanagement, ISO 27001 Lead Auditor, CISM oder Lean Management runden das Gesamtwissen ab. Herr Huber doziert an verschiedenen Hochschule Technologiefolgenabschätzung und Business Continuity Management. Herr Huber ist Mitglied des Fachbeirats Cybersicherheit des Landes Baden-Württemberg.

Mohamed Ibbich

Senior Technology Consultant, BeyondTrust

Mohamed Ibbich ist als Senior Technology Consultant bei BeyondTrust in Frankfurt am Main tätig und hat sich als zuverlässiger Berater für Kunden und Partner erwiesen. Er bringt über 18 Jahre Erfahrung als Vertriebspartner in Großbritannien, DACH und im Mittleren Osten mit umfangreichen Know-how beim Verkauf von Sicherheits- und Verschlüsselungslösungen an Unternehmenskunden sowohl im öffentlichen als auch im privaten Sektor mit. Er hat sich auf die Beratung vor und nach dem Verkauf in den Bereichen IT-Sicherheit und Verschlüsselung spezialisiert. Vor seiner Tätigkeit bei Avecto, ein Unternehmen der BeyondTrust, war er Senior Pre-Sales Consultant bei WinMagic und Sales Engineer bei Sophos.

Achim Kraus

Solutions Engineering CEEUR, Corelight Inc.

Achim ist seit mehr als 30 Jahren im Bereich Cybersicherheit tätig und konzentriert sich auf Branchengründer, die neue Technologien auf den Markt bringen. Er war an der Anwendung von Technologie in der E-Mail-Sicherheit und in Firewall-Bereichen der nächsten Generation beteiligt und hat maßgeblich dazu beigetragen, die heutige Anwendung von Sicherheitstechnologie zu ändern. Zuletzt hat er in SOC-Umgebungen mit NBA-, EDR- und Sicherheitsanalysetechnologien gearbeitet. Derzeit arbeitet er bei Corelight, das Netzwerkverkehrsanalysen bereitstellt und Sicherheitsüberwachungsdaten in hochmodernen SOC-Umgebungen erstellt. Er arbeitet lieber direkt mit Kunden und Dienstleistern zusammen, um sie bei der Lösung ihrer Cybersicherheitsprobleme zu unterstützen.

Chris Kubic

Chief Information Security Officer, Fidelis Cybersecurity

Herr Chris Kubic ist der Chief Information Security Officer (CISO) bei Fidelis Cybersecurity, verfügt über mehr als 30 Jahre Erfahrung in der Entwicklung von Informationssicherungs- und Cybersicherheitsinitiativen im US-Verteidigungsministerium (DoD), der Intelligence Community (IC) und der Bundesregierung. Herr Kubic hat eine herausragende Karriere bei der National Security Agency (NSA) hinter sich, wo er leitende technische Funktionen innehatte, u.a. als NSA Chief Information Security Officer, als Senior Security Architect für die Intelligence Community Information Environment, als Chief Architect der IA Architecture and Systems Security Engineering Group und als zahlreicher Technical Director.

Dr. Andrea Lober

Partner, BEITEN BURKHARDT

Andreas ist Partner und Leiter der TMT Praxis in der internationalen Anwaltskanzlei BEITEN BURKHARDT. Er verfügt über rund 20 Jahre Erfahrung im IT-Recht. Ein Schwerpunkt seiner Arbeit sind das Recht der Daten und Innovationen. Er interessiert sich immer für neue technische Entwicklungen, aktuell beispielsweise für Künstliche Intelligenz.

Etay Maor

Chief Security Officer,
IntSights

Etay is Intsight's Chief Security Officer, an industry recognised cybersecurity researcher and key note speaker. Previously, Etay was an Executive Security Advisor at IBM where he created and led breach response training and security research. Prior to that, Etay was the Head of RSA Security's Cyber Threats Research Labs where he managed malware research and intelligence teams and was part of cutting edge security research. Etay is an adjunct professor at Boston College and holds a BA in Computer Science and an MA in Counter Terrorism and Cyber Terrorism. Etay contributed to the ICT (International Institute for Counterterrorism) in cybersecurity, fraud and dark web topics and is a frequent featured speaker at major industry conferences. He is often tapped by major news outlets for his astute commentary on and insights into the cybersecurity news of the day.

Jamie Moles

Senior Security Engineer,
ExtraHop

Jamie has worked in the computer industry for over 30 years, focused primarily on security and infrastructure technologies. In the early 1990s, Jamie was one of the UK's leading experts on computer viruses – authoring his own Virus Scanner for MSDOS before joining Symantec as technical support lead for the new Peter Norton range of products, including the new Norton AntiVirus product. Nowadays, Jamie is helping customers understand and mitigate the risk contemporary threats pose to their business.

Klaus Nötzel

CISO,
EUMETSAT

Klaus Nötzel wurde mit dem Security Leader Award für den Mittelstand ausgezeichnet. Er hat in Darmstadt Elektrotechnik studiert und war verantwortlich für das Satellitenkontrollzentrum der Deutschen Telekom. Seit 2007 ist er verantwortlich für Informationssicherheit bei EUMETSAT. Er hält Vorträge auf internationalen Sicherheitskongressen und Forschungseinrichtungen. Ergänzend zu Zertifizierungen wie ISO 27001 Lead Implementer, CISSP und CISM hat er einen Master Abschluss als Organisationsentwickler der Hochschule Frankfurt. Eine wirkungsvolle Sicherheitskultur kann und muss gestaltet werden. In der Informationssicherheit vertritt er einen humanistischen Ansatz. Sicherheit wird durch Menschen gemacht und hier liegt der heutige Fokus seiner Arbeit.

Mariana Pereira

Director of Email Security Products,
Darktrace

???????

Stephen Roostan

VP EMEA,
Kenna Security

Roostan verfügt über mehr als zehn Jahre Erfahrung mit Cyber-Sicherheits- und Transformationsprojekten, und seine Aufgabe bei Kenna besteht darin, das Wachstum des Unternehmens in der Region Europa, Nahost und Afrika voranzutreiben, um der Kundennachfrage nach risikobasiertem Schwachstellenmanagement Rechnung zu tragen. Bevor Roostan zu Kenna kam, hatte er leitende Vertriebsfunktionen bei Forcepoint, Citrix und Imperva mit dem Schwerpunkt auf IT-Lösungen für komplexe Unternehmensanforderungen inne. Als Verfechter einer modernen Lebensweise engagiert sich Roostan unermüdlich für Gleichberechtigung und Flexibilität am Arbeitsplatz. In verschiedenen Unternehmen bekleidete er Positionen in Lenkungsausschüssen, in denen er sich für die Verringerung geschlechtsspezifischer Gehaltsunterschiede und die Entwicklung von Karrieremöglichkeiten für berufstätige Eltern einsetzte. Darüber hinaus ist er stets auf der Suche nach Initiativen zur Unterstützung von Gleichberechtigung in der Arbeitsumgebung und der Branche. Roostan ist überzeugt, dass die Schaffung einer kollaborativen Arbeitskultur sowohl Unternehmen als auch deren Mitarbeitern wesentliche Vorteile bietet.

Ernestine Schikore

Informationssicherheitsbeauftragte
CISO, Universität Basel

Ernestine ist Chief Information Security Officer an der Universität Basel, wo sie seit zehn Jahren im Bereich Cybersicherheit tätig ist. Seit 2000 konzentriert sie sich auf IT-Sicherheit und vermittelt zwischen IT-Benutzern und Technikern. Vor ihrem Eintritt an die Universität Basel arbeitete sie als Sicherheitsberaterin und bei der Schweizerischen Nationalbank.

Stefan Schinkel

Director Cortex Central Europe,
Palo Alto Networks

Stefan Schinkel ist seit Februar 2020 als Director Cortex DACH, einem Geschäftsbereich von Palo Alto Networks, beschäftigt. Mit über 25 Jahren Vertriebserfahrung in verschiedenen Positionen sind er und sein Team für einen der großen Wachstumsmärkte von Palo Alto

Networks verantwortlich. Zuvor hatte Stefan Schinkel bei Docker die gleiche Managementverantwortung. Zuvor hatte er viele Jahre verschiedene Managementpositionen bei Veritas und Symantec inne.

Steffen Siguda

Corporate InfoSec Officer, OSRAM Licht AG

Herr Siguda ist seit des Spin-Offs der OSRAM GmbH vom Siemens Konzern im Juli 2013 als Corporate InfoSec Officer für die Informationssicherheit weltweit verantwortlich. In dieser Funktion führt er eine globale Organisation mit InfoSec-Kontaktpersonen an allen OSRAM Standorten, seine Gruppe entwirft und überwacht aber auch alle technischen Sicherheitsfunktionen des Unternehmens (Firewall, Virenschutz, Applikationssicherheit). OSRAM sieht Bedrohungen der Informationssicherheit nicht nur im technischen Bereich, deshalb wird seit Jahren großer Wert auf Schulungen und Awareness gelegt. Insbesondere mit globalen Awarenesstests wurden signifikante Erfolge erzielt, die sich in der regelmäßigen Abwehr von teilweise hochkomplexen Social-Engineering-Angriffen auszahlen. Da OSRAM eine „Cloud first" Strategie verfolgt, sind die aktuellen Schwerpunktthemen Cloud Sicherheit (insbesondere der Bereich Identität), Zero-Trust Konzepte und Daten-orientierter Schutz (z.B. Digital Rights Management bei Dokumenten). Zur optimalen Integration der Informationssicherheit in die Applikationslandschaft des Unternehmens ist Herr Siguda auch als Datenschutzbeauftragter der OSRAM GmbH tätig. Vor dem Engagement im Bereich Informationssicherheit/Datenschutz war Herr Siguda nach dem Informatik-Studium an der TU München am Aufbau eines unternehmensweiten Netzwerks und dem Einstieg in die SAP CRM Welt beteiligt.

Peter Vahrenhorst

Kriminalhauptkommissar, Landeskriminalamt Nordrhein-Westfalen

Peter Vahrenhorst ist Kriminalhauptkommissar beim Landeskriminalamt Nordrhein-Westfalen. Er ist für die Prävention von Cybercrime mit der Zielrichtung „Wirtschaft" zuständig. Die Aufgabenfelder des Cybercrime-Kompetenzzentrums liegen unter anderem in der Computer Forensik, der Mobile Forensik, Ermittlungen, TKÜ, Open Source Recherche, Kriminalistische luK-Lageunterstützung, Prävention/Medien und der Auswertestelle Kinderpornografie. Nach dem Studium an der Fachhochschule für öffentliche Verwaltung NRW war Peter Vahrenhorst zunächst 10 Jahre als IT-Ermittler tätig. Danach war er im Bereich der polizeilichen Prävention zum Thema Internet unterwegs. Drei Jahre war er zusätzlich Lehrbeauftragter an der Universität Bielefeld. Peter Vahrenhorst wurde 2009 mit dem Preis „Kooperation Konkret" vom Schulministerium NRW und 2010 mit dem Landespreis Innere Sicherheit vom Ministerium für Inneres und Kommunales NRW ausgezeichnet

Frederik Weidemann

Chief Technical Evangelist, Onapsis Inc

Frederik Weidemann ist Experte für Computer- und Netzsicherheit und Chief Technical Evangelist bei Onapsis. Er hat über 50 Mal bei SAP- und sicherheitsbezogenen Konferenzen wie RSA, Troopers, SAPPHIRE, TechEd, SAP Insider, ASUG, DSAG und OWASP Vorträge gehalten. In den letzten vierzehn Jahren hat er sich auf die SAP-Sicherheit konzentriert und ist Mitautor des ersten Buchs über sichere ABAP-Programmierung. Außerdem schreibt er häufig Artikel über SAP-Sicherheit und hat zahlreiche Zero-Day-Schwachstellen in geschäftskritischen Anwendungen gefunden.

Marcel Zumbühl

CISO, Swiss Post

Marcel Zumbühl arbeitet seit August 2018 als Chief Information Security Officer (CISO) und Mitglied des IT-Vorstands für die Schweizerische Post und ist für die Informationssicherheit im Konzern verantwortlich. Der 50-Jährige hat einen Master-Abschluss in Informatik mit einem Nebenfach in Betriebswirtschaft. Nach seinem Studium an der Universität Bern arbeitete er im In- und Ausland für verschiedene Unternehmen wie Accenture, Swisscom und Credit Suisse. Seit 2009 ist Marcel Gastdozent für Risikomanagement und Risikokommunikation an der ETH Zürich und seit Sommer 2020 Co-Präsident der Information Security Society Switzerland (ISSS), dem größten unabhängigen Verband von Cybersecurity-Experten in der Schweiz. □

WHEREVER YOUR BIG IDEA LIVES, EXTRAHOP SECURES IT.

Stop Breaches 70% Faster with SaaS-Delivered
Network Detection & Response.

extrahop.com/freetrial

ExtraHop

Rise Above the Noise.

Remote working for the long haul and IT crisis planning for the long term

How to take the rapid, large-scale digital transformation that has taken place in the last few months, and make it work long term.

John Matthews reports

Enterprise IT has radically changed almost overnight. The events of the last few months have pushed organisations into a position many had considered but for which few had prepared: mass remote working, or 'teleworking'.

As lockdown orders went into effect, many organisations, from enterprises to government agencies, shifted their workforces to remote work in an effort to ensure business continuity and minimise disruption.

Remote working tools, like video conferencing software, instantly became central to business continuity. VPNs, which allow for a secure connection between the home network and the enterprise, have seen a huge resurgence and Remote Desktop Protocol (RDP) use has soared by 41%, according to Shodan data.

Months later, offices have started to reopen but it looks like remote working will continue to be a part of daily life. Now IT and security organisations are faced with a new task: How to take the rapid, large-scale digital transformation that has taken place in the last few months, and make it work long term.

A question of access – and security

First, there's the matter of access. When employees work remotely, many of them will be accessing corporate resources over insecure connections and personal devices. This means that the proper measures need to be implemented in order to provide access without compromising security.

VPNs and VDI play a key role here, but they need to be used effectively to mitigate performance problems. Enabling visibility across the VPN delivery chain is critical – not only to deal with performance bottlenecks at the gateway, but to document how well IT can deliver that performance and, if needed, demonstrate resource requirements to management. Many organisations are also accelerating adoption of cloud infrastructure and services, which substantially lessen or altogether eliminate the need for employees to connect to the corporate network.

Security and IT teams need to be vigilant to spot the locations from which users are remoting in, which remote access apps they are using, and the behaviour of their user accounts.

Then there's the matter of security. When configuring VPN access or migrating workloads to the cloud, there are many security best practices that can and should be used, particularly when managing a large remote workforce.

Watch for abnormal behaviour patterns. Security and IT teams need to be vigilant to spot the locations from which users are remoting in, which remote access apps they are using, and the behaviour of their user accounts. Of particular interest should be Active Directory account behaviour. IT teams should watch for failed logins and repeated lockouts. – which could be a sign that an attacker is trying to get in from a compromised user device.

Shore up your weakest link: People. Your remote workers are especially vulnerable now and their personal security habits may leave an organisation exposed to attack. They might use weak passwords as their single factor of authentication for their home devices. Those devices may be irregularly updated, potentially leaving old vulnerabilities present. Adversaries are trying to exploit their fears around COVID-19 too and Google reports that phishing has skyrocketed by 350%.

Organisations too recognise that precarious position and build defences around that fact. Primarily, users need to know how to defend themselves and the enterprise. Enterprises must communicate quickly and clearly to employees about the necessity of patching and updating their machines, choosing strong passwords and resetting them regularly, enabling multi-factor authentication where possible and providing ongoing education about the kinds of threats arrayed against remote workers.

This is an opportunity to think about people and processes. Consider escalation paths, for example. Senior IT engineers need to focus on larger issues within the enterprise – such as hunting sophisticated threats or designing more secure remote connectivity – and not spend their time fixing minor problems on

Enterprises need to shift away from prevention and protection and towards detection and response, a model which accepts the porous nature of modern networks.

the IT help desk. To make the most of your senior staff, you may have to re-organise those escalation paths and equip your frontline personnel to do more on their own.

These kinds of short-term measures are critical, but traditional perimeter-based networks weren't built to be stretched like this and have often not kept up with new threats or new ways of working or technological advancements like the cloud. Enterprises need to see the pandemic as a stress test; an opportunity to reexamine how they carry out remote access. There are a number of longer-term options that enterprises can consider.

Migrate toward the cloud

The current situation should prompt enterprises to migrate further towards the cloud, as a way to simplify access. By pushing more workloads to the cloud and relying more heavily on SaaS, enterprises can more manageably enable remote working and secure access for the long term. But they should do so carefully, and with security in mind.

Visibility into your environment will still be a prime concern. Until relatively recently, cloud providers either did not provide visibility tools, or provided ones that did not integrate easily with enterprise visibility tools. Without the ability to unify visibility across data centre and cloud environments, enterprises risk data leakage and exposing themselves to attackers.

Accept that the perimeter is dead

Previous generations of security thought about the protection and prevention at the perimeter. They assumed that data and employees stayed in the office and one could draw a neat line around a network and set up defensible walls where its borders lay. That is demonstrably not the case anymore but many enterprises still use the infrastructure that that mindset built. It's with that infrastructure that many enterprises are currently struggling to manage mass remote working.

In an age of mobile workers and even more mobile data, concepts like Zero Trust Network Access have arisen to transcend perimeters. Enterprises need to shift away from prevention and protection and towards detection and response, a model which accepts the porous nature of modern networks.

Reduce security and access friction in the long term

Going forward, employees must be able to remotely access enterprise resources securely and seamlessly. Desktop as a Service and virtualisation are ways to deliver employee workstations into their home. The cloud can also help enterprises ensure business continuity and maintain access to critical applications in the event of a crisis.

Again visibility here is critical. That means enabling rapid visibility across the network, which can tackle performance bottlenecks and see oncoming threats. In cases like the current one, it must be able to do so without the benefit of agent-based endpoint visibility, due to the prevalence of employee-owned devices. □

John Matthews is CIO at ExtraHop.

For more information, please visit **www.extrahop.com**

Dealing with the full spectrum of cyber-threats

Threats continue to evolve, and our environments are getting more complex and harder to defend.

It's hard dealing with the full spectrum of cyber-threats. The threat landscape is constantly evolving and, to further compound the challenge of defending our enterprises, we continue to roll out new technologies and extend security boundaries into the cloud and 'work from home' environments. The bottom line here is that threats continue to evolve, and our environments are getting more complex and harder to defend.

The keys to defending against these threats are:

1. *Effective cyber-hygiene:* The attackers 'go to' attack techniques continue to be phishing and social engineering attacks, exploitation of unpatched vulnerabilities, and exploitation of weak logon credentials. Minimising these threats requires:

    - *Knowing the terrain you are defending* – your critical data sets, business critical workflows, avenues of attack, and the high-risk assets associated with those
    - *Diligent patching* – particularly for those high-risk assets and for systems that support work at home users
    - *Good account and password management* – ensuring employees are using complex, hard to guess passwords backed with two factor authentication
    - *Robust endpoint protection* – using a combination of automated patch management software, anti-virus software to catch signature-based threats, and Endpoint Detection and Response (EDR) to catch the stealthier attacks. EDR adds additional benefits for remote employees by enabling your security team to quarantine a device that is misbehaving, remotely diagnose the device to determine if and how it was compromised, return the device to a secure state, and apply global policy updates to all your remote devices to ensure other devices are not compromised in a similar way.
    - *Continually reinforcing security best practices* with your employees to include best practices for detecting and reporting phishing and social engineering attacks

2. *Early detection and validation of anomalous activity:* Stopping a ransomware attack as systems are being encrypted is too late in the game. At this point, the adversary likely owns your environment and has exfiltrated sensitive data from the environment. Detecting and blocking sophisticated and stealthy attacks early in the attack kill chain requires threat focused analytics that can detect anomalous activities occurring throughout your enterprise and correlate that activity with other events to produce high confidence and actionable alerts. This proactive approach to detecting and responding to threats requires:

    - Full visibility of the terrain you are defending through an integrated security stack that cuts across endpoints, networks, and cloud workloads
    - Threat focused analytics to identify and correlate interesting and anomalous events and provide context surrounding the events
    - Sophisticated tools backed by automation to enable security analysts and threat hunters to:
        - Perform deep inspection and analysis of anomalous activities
        - Track an attacker's movements and anticipate their next moves
        - Block their advance
    - Integrated deception tools to improve confidence in and correlation of attacks
    - Security analysts knowledgeable in the attack techniques used by cybercriminals and nation-state threat actors

It is through these proactive security capabilities that you can move your organisation beyond a preventative and reactive defence posture and truly address the full spectrum of cyber-threats targeting your organisation. As an added bonus, it can help address other challenges including alert fatigue, analyst overload, and the impacts of limited cyber-personnel.

Leverage an attack framework

Using an attack framework helps to identify gaps, redundancies, and inefficiencies in your enterprise security architecture and helps your analysts better understand and anticipate attacker tactics, techniques and procedures (TTPs).

Securing the enterprise has traditionally focused on the acquisition of multiple security tools to meet differing needs and respond to new and evolving threats. This approach leads to a complex security stack that is managed in silos without any integration, automation, or correlation amongst the tools and data within the security stack. Use of a cooperative cybersecurity framework such as the MITRE ATT&CK Framework to drive security stack consolidation ensures that complementary tools are selected that can cover the full

Fidelis Security reports

Security teams need to shift focus from manual alert triage to reducing dwell time; stopping attacks before sensitive data is stolen or mission operations are disrupted.

range of TTPs employed by adversaries. The framework can be used to essentially measure the effectiveness of your existing security stack and help you identify gaps and redundancies.

Mapping anomalous activity against an attack framework is also a good way to piece together seemingly unrelated events and demonstrate that they are part of a broader attack.

Increase alert accuracy and actionability

Traditional threat detection based on attack signatures and flagging anomalous events contained in logs, lack the visibility and contextual understanding of the processes, behaviours, network actions, and content needed to detect sophisticated attacks and to weed out false positives.

When an alert fires, the primary things that security teams want to know are:

- Is this a real incident?
- What data and systems have been potentially exposed or compromised?
- How should I respond?
- Was I successful in mitigating the attack?

Answering effectively, and (most importantly) in cyber-relevant time, requires the ability to correlate anomalous events and activity across multiple points in your enterprise using analytics, automation, and machine learning. As you look across multiple data sets, patterns begin to emerge that help to fuel new threat hunting hypotheses and uncover hidden threats – both internal and external. Automation and analytics also allows for increasing the accuracy, integration, prioritisation, and actionability of alerts.

Deception technology can also play an important role in increasing the accuracy of alerts. Activity detected by deception decoys provides a high confidence indication of an ongoing attack and are used to not only identify that an adversary has breached your defences, but enables you to capture their tools, track their actions (reconnaissance, initial infiltration, lateral movement, …), understand their attack objectives, and block further exploitation.

The correlation of activity across multiple points in your enterprise enables you to increase the confidence and enrichment of alerts with value added information to produce more actionable alerts. The Fidelis Elevate™ eXtended Detection and Response (XDR) platform takes this approach by collecting rich metadata from across the enterprise and correlating anomalous activity through detection rules and analytics to enable your security operations team to identify potential threats early in the attack kill chain and remediate those threats before significant damage can be done.

Enhance the efficiency of security analysts with automation

Investigation of security alerts has traditionally been performed manually by analysts using data sourced across multiple security tools, leading to extremely labour-intensive and time-consuming analysis of anomalous events – many of which turn out to be false positives and leads to significant delays in identifying, verifying, and responding to security incidents. Security teams need to shift focus from manual alert triage to reducing dwell time; stopping attacks before sensitive data is stolen or mission operations are disrupted.

Introducing automation helps ease the analyst workload and frees up their time from manually responding to alerts (a reactive security posture) to active hunting (proactive defence). This allows security analysts to detect adversary TTPs much earlier in the attack kill chain by automating the verification of alerts to produce a prioritised list of high confidence alerts – what Fidelis calls 'attack conclusions'.

Threat intelligence comes into play here as it gives your security analysts insights into the changing TTPs used by attackers, provides analysts with a head start in where to hunt for adversary TTPs, and generates updated detection rules to ensure defences can detect new and evolving threats with high confidence. □

For more information, please visit
www.fidelissecurity.com

Fidelis™ Cybersecurity

Fidelis®
Cybersecurity

Detect. Hunt. Respond.

UNLOCK THE POWER OF YOUR RAW DATA.

- **Gain the visibility** you need to detect and respond
- **Protect data** across cloud, mail, and web traffic
- **Detect lateral movement** within your enterprise
- **Hunt** via metadata, threat intel and analytics

Learn how you can move beyond preventive defenses by automating threat detection, threat hunting, and response.

Fidelis Cybersecurity @FidelisCyber FidelisCyber fidelissecurity.com

Vertrauensbericht 2020

2020 hat sich eines erwiesen: Vertrauen ist wertvoller denn je. Wir alle sehnen uns danach, die vertraute Stabilität in der Welt um uns herum zurückzubekommen. Vertrauen ist elementar.

Synack reports

Der Vertrauensbericht 2020[1] ist der unentbehrliche Leitfaden für CISOs, CIOs, Sicherheitsexperten, das C-Level-Management und Vorstandsmitglieder, denn er bietet einen Überblick, wie Branchen und Wirtschaftszweige Messungen durchführen, um ihre Hausaufgaben in puncto Sicherheit zu machen. Grundlage für den Bericht bilden Daten aus der patentierten Synack-Kennzahl Attacker Resistance Score (ARS)™[2]. Für die Berechnung der ARS werden Informationen direkt aus der Plattform für Crowdsourcing-basierte Sicherheitstests von Synack abgerufen, die in Tausenden Sicherheitstests zwischen 2019 bis Juli 2020 durchgeführt wurden. 28 % der Schwachstellen, die die Community aus ethischen Hackern, das Synack Red Team[3], bei ihrer Arbeit auf der Synack-Plattform ermittelt haben, wurden als schwerwiegend oder kritisch eingestuft. Synack ist branchenweit führend in der Ermittlung der kritischsten und gefährlichsten Schwachstellen in den digitalen Assets und Apps der Kunden und bietet damit die fundierten Informationen, die erforderlich sind, um Angriffe zu verhindern.

Während der globalen Pandemie hat sich der Druck auf CISOs und andere Sicherheitsexperten verstärkt – eine Personengruppe, die vor dem Hintergrund der digitalen Transformation und der damit verbundenen Auswirkungen auf die Sicherheit ohnehin schon stark beansprucht war. Verbraucher setzten unverzüglich auf Homeoffice-Plattformen und Videokonferenz-Apps und erwarteten – oder forderten, dass Unternehmen ihre Sicherheit und Privatsphäre schützen sollten. Marken, die nicht in der Lage waren, dieses Vertrauen aufrechtzuerhalten, waren mit realen und messbaren Konsequenzen konfrontiert.

Der Vertrauensbericht 2020 von Synack ist eine Pflichtlektüre für alle Sicherheitsexperten, die ihrem C-Level-Management, dem CEO oder dem Vorstand bei folgender Fragestellung Rede und Antwort stehen müssen: „Kann ich unseren digitalen Systemen vertrauen?"

Michael Coden, Global Leader Cybersecurity Practice, BCG Platinion, Boston Consulting Group, zufolge sei die Cybersicherheit der digitalen Assets Ihres Unternehmens genau so wichtig, wie Ihre körperliche Gesundheit. Coden legt Erkenntnissen zufolge nahe, dass 98 % der US-Bürger sich bisher nicht mit COVID-19 infiziert hätten. Wenn Sie jedoch zu den 2 % der Betroffenen gehören, dann haben Sie gelitten. 97 % der US-Bürger mit einer COVID-19-Infektion sind vollständig genesen, für 3 % der Infizierten gilt das leider nicht. Die Wahrscheinlichkeit, mit der Ihr Unternehmen schwere Schäden aufgrund eines Cyberangriffs erleidet, ist gering. Trifft es Sie aber doch, dann können die Auswirkungen verheerend sein.

Synacks Vertrauensbericht 2020 ist Ihr Leitfaden, um den Wert von Sicherheit inmitten einer unsicheren Umgebung zu bestimmen. Die geschützte Kennzahl „Attacker Resistance Score" (ARS) von Synack ist eine Bewertung, wie gehärtet Ihre Assets gegen einen Angriff sind. Die Kennzahl ARS bietet insgesamt einen umfassenden Überblick über die Anfälligkeit von Anwendungen für einen Angriff, basierend auf einem patentierten Algorithmus, der von Synacks Data Science Team entwickelt und bewertet wurde.

Synack berechnet eine eindeutige ARS im Bereich von 0 bis 100 für jedes Asset, jede Bewertung und Organisation, die das Unternehmen testet. Bei der Berechnung werden die Angriffskosten, die Schwere der Feststellungen und die Effizienz bei der Behebung mit berücksichtigt. Je höher der Wert der ARS ist, um so gehärteter ist ein Asset gegenüber einem Angriff. Grundsätzlich gibt ein höherer ARS-Wert an, dass wesentlich mehr Zeit investiert werden muss und hohes Expertenwissen vonnöten ist, um ein Asset zu kompromittieren. Zu viel Zeit und Expertenwissen für die meisten böswilligen Angreifer – ein solches Asset ist kein attraktives Angriffsziel. Die guten Nachrichten aus dem Bericht für 2020: Regierungsstellen, der Finanzdienstleistungs- und Technologiesektor haben alle überdurchschnittliche Bewertungen erzielt.

Vertrauen ist verletzlich. Schutz ist entscheidend

Verbraucher wünschen sich Vertrauen in die Marken, die sie in ihrem Alltag begleiten. Ironischerweise ist in Zeiten wie dieser, wenn das Gesundheitswesen, die Regierung und alle Branchen unter immensem Druck stehen, das Vertrauen gering und Menschen müssen mehr denn je Vertrauen aufbringen. Ohne Vertrauen werden auch die besten Marken am Markt Schwierigkeiten haben, und Institutionen sind nicht in der Lage, wichtige und entscheidende Funktionen bereitzustellen, wie beispielsweise das Angebot von Gesundheitsdienstleistungen oder kürzlich die Durchführung der US-Wahlen. Vertrauen ist praktisch das Tragwerk für alle gesellschaftlichen Aspekte – und Vertrauen vor dem Hintergrund der zunehmend schweren digitalen Bedrohungen aufrechtzuerhalten, ist eine gewaltige Aufgabe.

Das ist die Aufgabe eines CISO. Mit der ARS steht ihnen eine Kennzahl zur Verfügung, die die Erkenntnisse bietet, die sie benötigen. Damit können sie gewährleisten, dass Unternehmen sicher sind, kostspielige Verstöße und Schwachstellen vermeiden, ihre Kunden und Partner schützen und langfristig Vertrauen und Loyalität aufbauen. Hier können Sie den vollständigen Bericht herunterladen. □

[1] https://www.synack.com/trust-report/
[2] https://www.synack.com/products/
[3] https://www.synack.com/red-team/

Mehr erfahren auf
www.synack.com
Synack

Synack

DIE ULTIMATIVE LÖSUNG FÜR CYBERSICHERHEIT

UMFANGREICHE PENETRATIONSTESTS MIT UMSETZBAREN ERGEBNISSEN

Unterbrechungslose Sicherheit — dafür sorgen die weltweit talentiertesten ethischen Hacker und KI-Technologie

DAS VERSPRECHEN VON SYNACK

Vertrauen muss man sich verdienen — und wir spielen mit offenen Karten:

das Versprechen, unsere Kunden und ihre Kunden zu schützen.

Absolute Vertraulichkeit. Optimale Anonymität.

Vollständige Kontrolle über den Prozess.

Absolut zuverlässig, wenn Sie sich auf Ihr Geschäft konzentrieren müssen.

Wir sind Synack: die vertrauenswürdigste Crowdsourcing-basierte Sicherheitsplattform.

BESUCHEN SIE UNS AUF WWW.SYNACK.COM

Cyberattacken auf die Medizin

Seit einigen Monaten laufen APT-Angriffe auf Entwickler von COVID19-Impfstoffen. Die betroffenen Pharmaunternehmen arbeiten an COVID-19-Tests oder an Impfstoffen, die sich in verschiedenen Phasen der klinischen Erprobung befinden.

BeyondTrust berichtet

Die Abhängigkeit von Technologie im Gesundheitswesen nimmt zu und Schaden durch Computerviren, Ransomware oder Hacker-Attacken wie im obigen Fall kann lebensbedrohlich sein. Cyberattacken können Forschungsprozesse torpedieren oder im Krankenhausbetrieb die medizinische Versorgung unterbrechen. Schwache Passwörter, unsichere (IoT)-Endgeräte und unerkannte Netzwerkzugriffe von außen zählen zu den häufigen Angriffsszenarien. Ohnehin müssen alle Kommunikationsprozesse im Healthcare-Umfeld strenge Sicherheitsvorgaben erfüllen, was vor allem personenbezogene Daten und den Umgang damit betrifft.

Datenschutz und Gesundheitsschutz

Wie wichtig Datensicherheit ist, zeigt der BeyondTrust Privileged Access Threat Report. Das schriftliche Notieren von Passwörtern wird demnach von 60 Prozent der befragten Organisationen als Problem benannt. Auch die Weitergabe von Kennwörtern an Kollegen ist bei 58 Prozent ein häufig notierter Missstand. In jedem Fall zeigen die ermittelten Zahlen, dass die Absicherung von Zugangsdaten und Passwörtern weit oben auf der Aufgabenliste von Sicherheits- und IT-Experten steht.

Im Internet der Dinge treten solche Gefahren noch schneller zutage. Zwar sorgen Innovationen bei medizinischen Geräten, Medikamenten und der Patientenüberwachung für produktive Arbeitsabläufe, Kosten- und Effizienzgewinne. Allerdings mangelt es häufig an der Visibilität auf Logins von IoT-Geräten. Ein Viertel der von BeyondTrust befragten Organisationen war unsicher, wieviele IoT-Geräte mit den eigenen IT-Systemen vernetzt sind. Jede fünfte Einrichtung konnte nicht detailliert nachvollziehen, welche Einwahlvorgänge durchgeführt werden. Sechs von zehn Verantwortlichen konzedierten, dass im Internet of Things gespeicherte Standardpasswörter eine mittlere oder erhebliche Bedrohung darstellen. Die gleiche Anzahl von Befragten befürchtet, dass Passwörter von IoT-Geräten im Klartext gespeichert werden.

Versteckte Risiken im Internet der Dinge

Wichtige Medizingeräte, auf denen sensible Daten lagern, werden häufig von Drittanbietern gewartet. Der BeyondTrust-Umfrage zufolge sind bei jedem zweiten Unternehmen mehr als 100 Service-Dienstleister, die sich auf unterschiedliche IT-Systeme wöchentlich aus der Ferne einloggen. Je größer die Zahl der Techniker mit Zugriffsrechten, desto schwieriger wird deren Kontrolle und umso größer ist auch die Gefahr, dass personenbezogene Daten abfließen.

Hinzu kommt, dass viele Wartungsarbeiten mit Administrationsrechten durchgeführt werden (müssen). Bei einer unkontrollierten Ver- und Weitergabe privilegierter Zugangsdaten geraten Anmeldedaten schnell aus dem Blickfeld. Geraten sie in die falschen Hände, haben Hacker leichtes Spiel, um sich Zugang zu weiteren Netzwerkbereichen zu verschaffen. Unter Sicherheitsgesichtspunkten ist es daher sinnvoll, dass alle Nutzer nur über diejenigen Lese-, Schreib- und Zugriffsrechte verfügen, die sie auch wirklich in ihrem jeweiligen Aufgabenbereich benötigen.

Entscheidend ist, dass alle Admin-Aktivitäten protokolliert und die Sitzungsdaten durch Verschlüsselung geschützt werden. Mit den Informationen über Bildschirmfreigaben, Dateiübermittlungen und Shell-Vorgänge lassen sich auch zu einem späteren Zeitpunkt verdächtige Aktivitäten im Netzwerk zielgerichtet nachverfolgen und auswerten. Automatisch generierte Meldungen sowie Echtzeitinformationen über laufende Sitzungen erlauben dabei jederzeit ein situationsbezogenes Eingreifen des IT-Admin-Teams.

Mehrere Sicherheitsstufen

Wirksame Sicherheitsvorkehrungen hängen aber auch von ihrer Benutzerfreundlichkeit ab. Security-Tools müssen so alltagstauglich sein, dass sie unkompliziert in der Handhabung sind. Ansonsten werden sie nicht eingesetzt und die Gefahr ist groß, dass sensible Daten der Einfachheit halber auf mobile Speichermedien kopiert werden, um sie später zu bearbeiten. Aus diesem Grund haben sich PAM-Lösungen (PAM, Privileged Access Management) für die Durchsetzung mehrstufiger Sicherheitsvorkehrungen durchgesetzt.

Privileged-Access-Management-Lösungen weisen Zugriffsberechtigungen nur für autorisierte Aufgaben zu, protokollieren und überwachen ihren Einsatz. Sie helfen Organisationen bei der Absicherung von privilegierten Benutzerkonten und Zugangsdaten, indem sie eine granulare Kontrolle und Überwachung der Systemzugriffe und Benutzeraktivitäten ermöglichen. So lassen sich höchste Sicherheits- und Produktivitätskriterien für Zugangsdaten durchsetzen, Schwachstellen aufspüren und Cyberbedrohungen bis auf Desktop-Ebene abwehren. □

Weitere Informationen unter
www.beyondtrust.com

BeyondTrust

BeyondTrust

UNIVERSAL PRIVILEGE MANAGEMENT

Secure and protect privileges across passwords, access, and endpoints to stop data breaches and achieve compliance.

Privileged Password Management

Endpoint Privilege Management

Secure Remote Access

beyondtrust.com

Eine Flutwelle von Sicherheitslücken

Der Preis des herkömmlichen Ansatzes.

Stephen Roostan berichtet

Nie standen IT-Sicherheitsabteilungen unter größerem Druck, ihr Budget optimal zu nutzen, als in den vergangenen sechs Monaten. Der Grund: Der bisherige Ansatz des pauschalen Schwachstellenmanagements funktioniert nicht mehr, da aufgrund des immer raffinierteren Vorgehens von Hackern die Bedrohungslandschaft ständig wächst und Sicherheitslücken rasant zunehmen.

Auch die am besten ausgestatteten Unternehmen können lediglich 10 % der Schwachstellen angehen. Der Anteil der Sicherheitslücken, die überhaupt zu einer echten Bedrohung für eine Unternehmensumgebung werden, beträgt zwar lediglich 2-5 %. Doch die herkömmlichen Methoden für den Umgang mit Schwachstellen sind wahrscheinlich nicht sehr hilfreich, wenn es darum geht, herauszufinden, für welche von ihnen das höchste Risiko besteht, ausgenutzt zu werden.

Legacy-Schwachstellen-Scanner geben IT- und Sicherheitsteams kaum Einblick in das konkrete Risiko, das eine Schwachstelle für das Unternehmen darstellt. Daher verlassen sich viele Unternehmen weiterhin auf den veralteten Ansatz, bei dem Patches auf alle Sicherheitslücken angewendet werden, die gemäß dem Common Vulnerability Scoring System (CVSS) einen Schweregrad von 7 oder mehr aufweisen. In Ermangelung einer besseren Herangehensweise kommen Sicherheitsteams oft mit Listen Tausender sogenannter „kritischer" Sicherheitslücken zur IT-Abteilung. IT-Teams verschwenden dann wertvolle Zeit damit, Schwachstellen zu beseitigen, die kein großes Risiko für das Unternehmen darstellen, während echte Lücken ignoriert werden. Dies hält sie davon ab, andere, strategisch sinnvollere Projekte zur Erreichung der sich ständig wandelnden aktuellen Geschäftsziele umzusetzen. Gleichzeitig kann das wahllose Patchen geschäftskritischer Anwendungen unnötige, kostenaufwändige Ausfallzeiten verursachen.

Der Druck, alle Schwachstellen zu eliminieren, treibt die Kosten in die Höhe, hat negative Auswirkungen auf die Zusammenarbeit zwischen den IT-, Sicherheits-, Entwicklungs- und Betriebsteams und führt zu einer enormen und anhaltenden Verschwendung von Ressourcen, die für die Erreichung anderer Ziele eingesetzt werden könnten.

Fokus auf Risiko

Sicherheitsteams müssen daher ihren Fokus weg von der rudimentären oder manuellen Priorisierung auf diejenigen Sicherheitslücken richten, die für ihre jeweilige IT-Umgebung die größte Rolle spielen. Die Umstellung auf einen wirklich risikobasierten Ansatz beim Schwachstellenmanagement erlaubt es Teams, sich auf die Erkennung und Beseitigung von Sicherheitslücken zu konzentrieren, für die die größte Gefahr besteht, dass sie ausgenutzt werden. Eine solche Herangehensweise bietet dringend benötigte Transparenz für Unternehmen, die ihre Sicherheits-, IT-, Entwicklungs- und Betriebsressourcen optimal nutzen wollen.

Wenn diese Risikoorientierung in alle Aspekte der Unternehmenstätigkeit integriert wird, profitieren alle Beteiligten.

Tatsächliches Risiko messen

Sicherheitsteams können damit beginnen, das tatsächliche Risiko zu messen, und herausfinden, wie sie dieses am besten verringern können. Indem Unternehmen das Risiko ins Blickfeld rücken, haben sie die Möglichkeit, eine neue Self-Service-Umgebung zu schaffen, sodass Sicherheits- und IT-Teams automatisch auf dasselbe Ziel hinarbeiten. Durch die Automatisierung und Priorisierung des Fokus aller Beteiligten auf die Schwachstellen, die das größte Risiko für das Unternehmen darstellen, steht Teams mehr Zeit für die Berichterstellung, Überwachung und Ausnahmebehandlung zur Verfügung.

Sicherheitsniveau verstehen und nachverfolgen

Führungsteams können sich nicht nur ein genaues Bild von dem Sicherheitsniveau des Unternehmens machen, sondern auch davon, wie sich dieses verändert und welche Maßnahmen und Investitionen für laufende Verbesserungen erforderlich sind.

Zusammenarbeit von Sicherheits-, Entwicklungs- und Betriebsteams

IT-, Entwicklungs- und Betriebsteams können weiter mit vorhandenen Tools, Prozessen und Plattformen arbeiten und gewinnen immer mehr Einblicke in die Unternehmensrisiken. Mit einem risikobasierten Ansatz können die für die Beseitigung von Sicherheitslücken zuständigen Teams ihre Anstrengungen auf die strategisch sinnvollsten Maßnahmen konzentrieren. Darüber hinaus können diese Teams ihre Zeit effektiver nutzen, da sie nicht mehr riesige Tabellen durchgehen und nach Patches suchen müssen.

Und ganz wichtig: Die Verbesserung der Zusammenarbeit zwischen den Sicherheits- und IT-Teams fördert auch die risikobasierte Entscheidungsfindung im Unternehmen. □

Stephen Roostan,
Vice President EMEA,
Kenna Security.

KENNA Security

Lesen Sie weiter unter:
www.kennasecurity.com/resources

KENNA Security

Modern Vulnerability Management

Focus on the vulnerabilities that matter most.

Remediate faster and more efficiently with data-driven risk prioritization.

www.kennasecurity.com

Kenna and Kenna Security are trademarks and/or registered trademarks of Kenna Security, Inc. and/or its subsidiaries in the United States and/or other countries. © 2020 Kenna Security, Inc. All rights reserved.

Unterstützung für Sicherheit und Compliance von geschäftskritischen SaaS-Anwendungen

Onapsis erweitert die Unterstützung für Sicherheit und Compliance von geschäftskritischen SaaS-Anwendungen wie Salesforce, Workday, Oracle, SAP und anderen Cloud-Anwendungen.

Onapsis berichtet

Als führendes Unternehmen auf dem Gebiet der Cybersicherheit und Compliance für unternehmenskritische Anwendungen gab Onapsis kürzlich bekannt, dass es 55 Millionen Dollar in der Serie D-Finanzierung gesammelt hat. Führend in der Unterstützung waren Caisse de dépôt et placement du Québec (CDPQ) und NightDragon, weiter waren die bestehenden Investoren .406 Ventures, LLR Partners und Arsenal Venture Partners beteiligt. Durch diese Investitionen wird Onapsis schnell in den Markt für geschäftskritische SaaS-Anwendungen expandieren. Hierbei stehen zunächst Salesforce- und SuccessFactors-Anwendungen und deren Sicherheit und Compliance im Fokus.

Diese neue Unterstützung für geschäftskritische SaaS-Anwendungen ermöglicht es Onapsis, seine Vision des Schutzes des intelligenten Unternehmens und der Beschleunigung digitaler Transformationsinitiativen umzusetzen. Zukünftig sollen Cybersicherheits- und Compliance-Lösungen für alle geschäftskritischen Anwendungen bereitstellt werden – sowohl für on-premise Systeme als auch für Cloud-basierte Infrastructure-as-a-Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS), sowie für deren API-basierten Integrationen.

Unternehmensdynamik und -leistung

Mehr als 300 der größten globalen Unternehmen, darunter mehr als 20 % der Fortune-100-Unternehmen, vertrauen beim Schutz ihrer Cloud-, Hybrid- und unternehmenskritischen on-premise Anwendungen auf Onapsis. Diese jüngste Finanzierungsrunde verleiht Onapsis nach einer starken Leistung im bisherigen Jahresverlauf 2020 eine solide Dynamik. Zu den Höhepunkten gehören:

- Über 145% Wachstum bei den jährlichen wiederkehrenden Netto-Neueinnahmen (ARR)
- Vier Jahre in Folge von der Deloitte Technology Fast-500-Publikation als eines der am schnellsten wachsenden Technologieunternehmen Nordamerikas ausgezeichnet
- Hervorragende Kundenzufriedenheit mit einer Retention Rate von 98% und einem der höchsten NPS-Werte der Branche
- Kürzlich angekündigte strategische Partnerschaft mit SAP – die Onapsis-Plattform ist die von SAP unterstützte Anwendung für Cybersicherheit und Compliance
- Weltweit führendes Forschungslabor für Cyber-Bedrohungen – über 800 Zero-Day-Schwachstellen entdeckt; mehrere kritische globale CERT-Warnungen auf der Grundlage der neuartigen Forschung von Onapsis
- Etablierte Partnerschaften mit führenden Systemintegratoren und Beratungsunternehmen wie Accenture, Deloitte, IBM, PwC, Verizon, Optiv und anderen
- Globale Betriebe in den Vereinigten Staaten, Argentinien und Deutschland mit mehr als 380 Mitarbeitern, anerkannt als eines der "Top 3 Great Place to Work"
- Neue Unterstützung für unternehmenskritische SaaS-Anwendungen zum Schutz von intelligenten Unternehmen

Neuer Support für unternehmenskritische SaaS-Anwendungen

Onapsis startet außerdem ein Early-Access-Programm für die Onapsis-Plattform für Salesforce und SuccessFactors. Durch die Unterstützung dieser unternehmenskritischen SaaS-Anwendungen ermöglicht die Onapsis-Plattform den Kunden, Fehlkonfigurationen in Anwendungen, Schwachstellen und böswillige Aktivitäten schnell zu erkennen, zu bewerten, zu priorisieren und zu beseitigen. Diese könnten sich sonst auf das miteinander vernetzte unternehmenskritische Ökosystem und sensible Geschäftsdaten eines Unternehmens auswirken. Als Nächstes wird Onapsis die Unterstützung von Early-Access-Programmen für Workday, Oracle ERP Cloud und Oracle HCM Cloud sowie andere SaaS-Anwendungen einführen. Diese werden in den kommenden Monaten veröffentlicht.

"Da sich kritische Geschäftsprozesse und Funktionen wie HCM, CRM und ERP, auf die Cloud- und SaaS-Umgebungen ausdehnen, benötigen Unternehmen eine Möglichkeit, das Risiko ihrer hybriden Geschäftsplattformen zu reduzieren, Sicherheits- und Compliance-Baselines von on-premise bis zur Cloud durchzusetzen und die Anwendungssicherheit, Benutzeraktivitäten und Bedrohungen von der Entwicklung bis zur Produktion zu überwachen", sagte Mariano Nunez, CEO und Gründer von Onapsis. "Diese Finanzierung baut nur auf unserer anhaltend starken Dynamik auf, da wir uns weiterhin stark darauf konzentrieren, der Standard für die Sicherheit und Konformität geschäftskritischer Anwendungen in Cloud-, Hybrid- und lokalen Umgebungen zu sein. Wir fühlen uns geehrt, das Vertrauen neuer herausragender Investoren wie CDPQ und NightDragon sowie die anhaltende Unterstützung unserer bestehenden Partner zu haben. Wir werden Onapsis nun weiter skalieren und noch mehr Organisationen auf der ganzen Welt dabei unterstützen, den Schutz all ihrer kritischen Informationen und Prozesse zu gewährleisten." □

Um mehr zu erfahren, besuchen Sie die Onapsis-Website unter **onapsis.com/de**

UMZUG IN DIE CLOUD.
MIT ZUVERSICHT.

Offensichtlich ist, dass ein Umzug Ihrer unternehmenskritischen Systeme wie SAP ERP®, SAP S/4HANA® und Oracle® EBS in die Cloud viele Vorteile bringt. Weniger offensichtlich sind die Sicherheitsrisiken. Onapsis kann Ihre Cloud-Migration sicher unterstützen. Unsere Plattform bietet Ihnen tiefe Einblicke in Ihre ERP-Landschaft, eine kontinuierliche Überwachung und automatisierte Governance – damit Sie alles Wichtige beim Umzug von on-premise in die Cloud im Blick haben. Und durch die frühzeitige Einbindung von Onapsis in Ihren Migrationsprozess können Sie nicht nur die Transformation beschleunigen, sondern auch unerwünschte Überraschungen auf dem Weg vermeiden.

onapsis

onapsis.com

Jenseits von Car-Hacking

Die gefährlichsten Cyber-Bedrohungen für die Automotive-Branche.

IntSights reports

Autohersteller und Autohändler stehen bei der Verteidigung ihrer Sicherheitsbereiche gegen Cyberangriffe zahlreichen Herausforderungen gegenüber. Seit in die Konstruktion von Autos immer mehr Software integriert wird, sind Cyber-Angriffe gegen neuere Fahrzeugmodelle in den letzten Jahren immer häufiger geworden. Hacker haben die in modernen Autos installierten Hard- und Firmwarekomponenten erfolgreich angegriffen, was ihnen den Diebstahl oder ein ferngesteuertes Abschalten der betreffenden Fahrzeuge ermöglichen kann.

Unternehmen der Automotive-Branche sind aber Cyber-Bedrohungen ausgesetzt, die über diese auf ihre Produkte zielenden Angriffe noch hinaus gehen. Die vorgenannten, spektakulären Angriffe haben den größten Teil der Medienaufmerksamkeit gewonnen, da sie den Verbraucher direkt betreffen. Etwas in den Hintergrund sind dadurch die eher konventionellen Bedrohungen für die Netzwerk- und Datensicherheit bei Automotive-Unternehmen geraten. Angriffe auf die Produktsicherheit der Fahrzeuge zielen meist nur auf die vom Hersteller entwickelte Firmware, während sich Bedrohungen für die Netzwerke und die Infrastruktur auf die gesamte Branche auswirken.

Unternehmen der Automotive-Branche besitzen eine Infrastruktur und Daten, die sowohl für Kriminelle als auch für staatsnahe Bedrohungsakteure ein interessantes Ziel darstellen. Zu den wichtigsten Angriffen auf die Netzwerk- und Datensicherheit in der Automotive-Branche gehören das Ausspähen von Kunden- und Mitarbeiterdaten für Betrugs- und Erpressungszwecke oder weitere Angriffe, das Unterbrechen von Herstellungsprozessen und Zulieferketten, die Offenlegung von Daten bei Ransomware-Angriffen sowie der Zugriff auf geistiges Eigentum und wettbewerbsrelevantes Wissen.

Ransomware: Betriebsunterbrechung und Offenlegung von Daten

Automotive-Unternehmen sind dem Risiko von Ransomware-Angriffen ausgesetzt, die zur Unterbrechung der Herstellungsprozesse und Zulieferketten führen. Ein derartiges Szenario ist der Einsatz von Schadsoftware, die die industriellen Steuerungssysteme (ICS) angreift, welche die Montagelinien oder andere Aspekte des Autoherstellungsprozesses steuern. Ransomware-Angriffe auf Automotive-Hersteller und ihre Zulieferer sind eine konkrete Bedrohung mit dokumentierten Fallbeispielen, von denen einige zur Unterbrechung von Herstellungsprozessen oder Zulieferketten geführt haben.

Zugriff auf Kunden- und Mitarbeiterdaten

Kriminelle richten ihre Aktionen gegen Unternehmen verschiedenster Branchen, um bei ihnen an Kunden- und Mitarbeiterdaten zu gelangen, mit denen sie selbst oder kriminelle Käufer dieser Daten böswillige Zwecke wie Betrug, Erpressung oder weitere Angriffe verfolgen können. Der Wert dieser Daten oder Zugriffsmöglichkeiten auf dem Cyber-Schwarzmarkt hängt von ihrer Profitabilität und der Detailschärfe der darin enthaltenen Daten ab. Die Kunden- und Mitarbeiterdaten von Automotive-Unternehmen, insbesondere Kundendaten der Autohändler, der Kundendienstabteilungen und der Finanzdienstleister können ein Ziel solcher Angriffe darstellen und waren es in der Vergangenheit auch bereits.

Zugriff auf geistiges Eigentum und wettbewerbsrelevantes Wissen der Automotive-Branche

Automobilhersteller verfügen über wertvolles geistiges Eigentum, auf das vor allem staatsnahe Bedrohungsakteure gerne zugreifen möchten. Im Fall der staatlich geförderten Cyberspionage zielt diese typischerweise auf den Zugriff auf geistiges Eigentum ausländischer Unternehmen, um damit Unternehmen des eigenen Landes (insbesondere solche im Staatsbesitz) zur Nachahmung der Produkte der ausländischen Wettbewerber und zur Verbesserung der eigenen Wettbewerbsposition zu befähigen. In der Automotive-Branche ist das primäre Ziel solcher Angriffe der Zugriff auf selbst entwickelte Designs oder auf die Konstruktionspläne für Fahrzeugmodelle.

Ein anderes, damit verwandtes Ziel solcher Angriffe ist das Erlangen von wettbewerbsrelevantem Wissen, das zur Unterstützung von Unternehmen im Staatsbesitz oder anderer Unternehmen im eigenen Land genutzt werden kann. Zu diesem Wissen können Details aus Marketing-, Vertriebs- oder Preisgestaltungsplänen und -strategien gehören, die Wettbewerber im Markt gegen die geschädigten Unternehmen einsetzen können, oder das Wissen über Betriebsabläufe und Best Practice-Verfahren, die Wettbewerber nachahmen können, um ihre eigene Wettbewerbsfähigkeit zu stärken.

IntSights hat kürzlich einen Untersuchungsbericht veröffentlicht, der die für die Automotive-Branche relevanten Formen von Cyber-Bedrohungen auflistet. Downloaden Sie diesen Bericht, um eine umfassende Übersicht zum aktuellen Stand der Cyber-Bedrohungen gegen Automotive-Unternehmen zu erhalten. □

Weitere Informationen unter
intsights.com

INTSIGHTS
Defend Forward™

INTSIGHTS
Defend Forward™

Simplify threat intelligence with the only all-in-one External Threat Protection Suite

IntSights simplifies threat intelligence with the most comprehensive, flexible, and contextualized solutions on the market. The IntSights External Threat Protection (ETP) Suite monitors thousands of sources across the clear, deep, and dark web to identify threats that directly target an organization's unique digital footprint. The ETP Suite enables security teams to rapidly operationalize intelligence by delivering information when and where they need it – all within an intuitive interface. Frictionless integration of our real-time cyber threat intelligence with existing security infrastructure allows enterprises to maximize return on investment. IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo.

To learn more, visit: **intsights.com** | Contact us: **info@intsights.com**

Snyk adds developer-first SAST solution to cloud native application security platform

Platform now secures all components of modern cloud native application development; delivering speed, accuracy and developer usability.

Snyk reports

BOSTON, Oct. 21, 2020 /PRNewswire/ – Cloud native application security company Snyk announced today it has launched Snyk Code, a developer-first SAST (static application security testing) solution to complete its market-leading cloud native application security platform. With the addition of Snyk Code, Snyk now provides security visibility and remediation as a platform for all of the critical components of the modern application including the application code, open source libraries, container infrastructure, and infrastructure as code.

Until now, legacy SAST tools have been difficult for developers to use, often taking hours or days to complete a vulnerability scan; providing high false positive rates; and requiring deep security knowledge to address the issues and fix them quickly. With Snyk Code, Snyk is re-imagining SAST in a way that developers can actually use as a seamless part of their development process – enabling them to build software fast and securely. Snyk Code gives developers automated and real-time insight into issues and vulnerabilities within the code they are creating, combining those with insights from other Snyk security solutions for open source libraries, containers and Infrastructure as code. By approaching application security with this holistic, developer-first approach, software-driven organisations can ensure a continuous, scalable security posture even before deploying into production.

"Snyk Code has been a missing piece to complete our cloud-native application security platform and we are excited to announce today at SnykCon the availability of this integrated and holistic approach to securing modern applications," said Peter McKay, CEO, Snyk. "We are leveraging the machine learning based technology we acquired through DeepCode to bring speed, accuracy, and developer-first experience to SAST, a traditionally non-developer friendly aspect of the security process. Snyk Code will change the acceptable standards for how developers secure their own code and continue to transform the security market to keep up with the unrelenting pace of digital transformation."

Snyk Code offers developers a differentiated SAST experience unlike any other solution in the market today by ensuring:

- *Developer usability:* Snyk Code prioritises the developer experience, combining its speed and accuracy with the ability to scan source-code before an app is built, unlocking previously impossible seamless integrations in git and IDEs, and fix recommendations based on real-world, real-time data.
- *Speed: S*nyk Code is up to 50x faster than traditional SAST solutions, allowing seamless integration into the fast pace of continuous integration and delivery (CI/CD) pipelines, and unlocking vulnerability detection as you code, improving what has been a slow and disruptive extra step that can sometimes take many hours.
- *Accuracy:* Snyk Code is focused on providing actionable results that matter, automatically modelling APIs and learning practices from the world's code, then training those models on Snyk's expansive, hand curated vulnerability database, significantly reducing false positives.

"From its inception, Snyk has sought to rethink application security as a dev-first process, requiring developer-centric tooling, integrations and workflows," said Guy Podjardny, President and Co-founder of Snyk. "This was our approach to SCA, to container security and most recently to securing infrastructure as code. And this is now critical for SAST, where traditional SAST products are universally disliked by developers, but is a required aspect to maintaining an acceptable security posture. We've taken the same approach with Snyk Code, delivering a differentiated, developer-first SAST solution that prioritises the developer experience."

Snyk Code launched at SnykCon, Snyk's first annual user conference, drawing a global audience of customers, users and the broader devsecops community. □

Snyk, the cloud native application security leader, has a vision to empower every software developer in the world to develop fast and stay secure. Only Snyk provides a platform to secure all of the critical components of today's cloud native application development including the code, open source libraries, container infrastructure and infrastructure as code. Snyk's developer-first approach enables technology-driven companies to scale security in today's fast-paced digitally transforming world. Snyk's security platform is powered by its industry-leading proprietary vulnerability database, maintained by the expert Snyk security research team, that also powers security solutions from strategic partners such as Datadog, Docker, IBM Cloud, Rapid7, Red Hat and Trend Micro. The company works with global customers of all sizes to empower developers to automatically integrate security throughout their existing workflows.

For more information and to get started with Snyk for free today, visit **snyk.io**

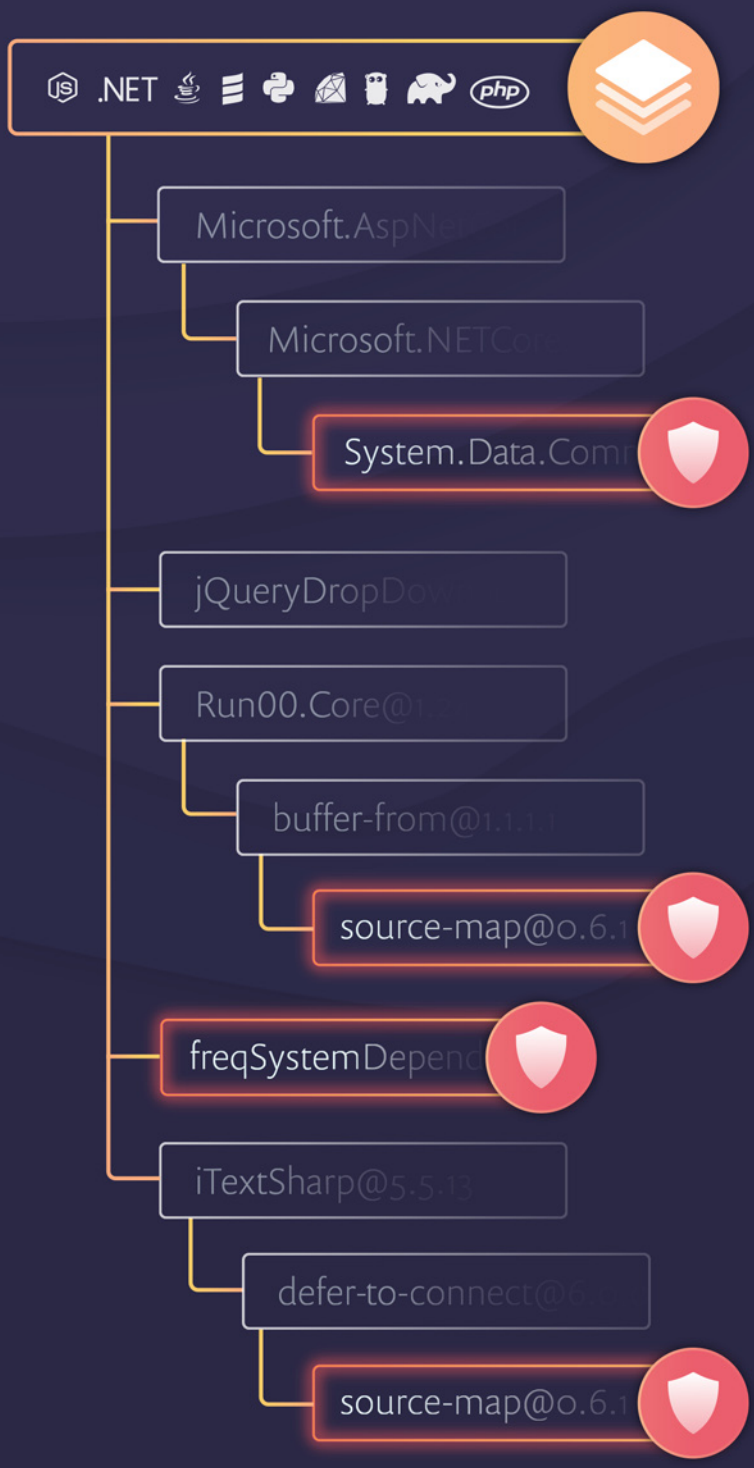
snyk

Securing Open Source Libraries **with Snyk**

Join more than 200,000 developers using Snyk to automatically find and fix vulnerabilities in in open source code packages.

Snyk is the leading developer- first security solution that continuously monitors your application's dependencies and helps you quickly respond when new vulnerabilities are disclosed.

Create a free account at Snyk.io



Customers protected by **snyk**

Microsoft · New Relic · skyscanner · Google · The Guardian · Adobe · salesforce · mongoDB

Forthcoming events

PCI LONDON VR

21st January 2021
Online

SECURING THE LAW FIRM VR

28th January 2021
Online

e-crime & cybersecurity CONGRESS VR

2nd & 3rd March 2021
Online

e-crime & cybersecurity MIDDLE EAST VR

10th March 2021
Online

e-crime & cybersecurity FRANCE VR

8th April 2021
Online

e-crime & cybersecurity APAC VR

6th May 2021
Online

e-crime & cybersecurity NORDICS VR

20th May 2021
Online

e-crime & cybersecurity DACH VR

16th June 2021
Online

SECURING FINANCIAL SERVICES VR

7th July 2021
Online

For more information, please call Robert Walker on +44 (0)20 7404 4597
or email robert.walker@akjassociates.com

Vielen Dank an alle unsere Sponsoren

Strategische Sponsoren

corelight

CYBERSPRINT
BREAKTHROUGH SECURITY

DARKTRACE

ExtraHop

Fidelis Cybersecurity

paloalto NETWORKS

Recorded Future

SentinelOne

Bildung Seminar Sponsoren

BeyondTrust

INTSIGHTS
Defend Forward

KENNA Security

onapsis

snyk

Synack