e-crime & cybersecurity BENELUX

8th December 2022
Amsterdam, The Netherlands

@eCrime_Congress
#ecrimecongress

#ecrimecongress

Plugging the third-party security gap

Forthcoming events

e-crime & cybersecurity GERMANY 18th January 2023 Frankfurt	PCI LONDON 25th January 2023 London	SECURING FINANCIAL SERVICES 26th January 2023 London	SECURING THE LAW FIRM 26th January 2023 London
e-crime & cybersecurity CONGRESS 1st & 2nd March 2023 London	e-crime & cybersecurity FRANCE 23rd March 2023 Paris	e-crime & cybersecurity NORDICS 26th April 2023 Stockholm	e-crime & cybersecurity CONGRESS 10th May 2023 Middle East
e-crime & cybersecurity GERMANY 7th June 2023 Munich	SECURING FINANCIAL SERVICES 5th July 2023 London	SECURING THE LAW FIRM 5th July 2023 London	SECURING THE PUBLIC SECTOR September 2023 London
e-crime & cybersecurity SWITZERLAND September 2023 Zurich	e-crime & cybersecurity MID-YEAR October 2023 London	e-crime & cybersecurity NORDICS November 2023 Copenhagen	e-crime & cybersecurity SPAIN November 2023 Madrid

For more information, please visit
akjassociates.com/contact-us

Plugging the third-party security gap

If core cybersecurity is hard enough to achieve with current resources, then is third-party security realistic? If not, then what? According to a recent study of CIOs, CISOs and CPOs, more than 96% of organisations surveyed in the Benelux region experienced a cyber-attack due to vulnerabilities in their supply chain. In the past 12 months, organisations reported being victims of a cyber-attack almost four times per year on average due to supply chain vulnerabilities.

This may be because 91% said they do not check their external suppliers for cybersecurity risks. And that may be because even firms investing in supplier cyber-risk management can find it impossible to use these budgets effectively. Almost no third-party vendors are under direct supervision, and it is impossible to communicate with every vendor on a frequent basis about their security posture.

Simply identifying suppliers and their data access and requirements is beyond many companies, as many relationships don't even come in through procurement. Even if identification is possible, then CISOs struggle with the technical challenge of providing third parties with enough access to perform their designated responsibilities and nothing more, especially when this changes depending on the underlying contracts.

The answer would seem to be some form of zero trust model, but according to a recent Ponemon Institute study, most organisations do not implement zero-trust policies because of the practical difficulties of visibility and understanding which vendors should have access to what. Even defining an organisation's most sensitive data turns out to be complicated because it is often highly context dependent.

These topics and many others will be the talking points at the 12th e-Crime & Cybersecurity Congress Benelux, as well as details of the latest technologies from some of the key providers. But one of the main aims of our events is to facilitate conversation and dialogue. So please, enjoy your event, and take the opportunity to mingle with peers, colleagues and solution providers. If you have any questions, please do not hesitate to ask any member of the team. Enjoy the day.

Simon Brady | Editor

@eCrime_Congress **#ecrimecongress**

8th December 2022
Novotel Amsterdam City

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

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

Forum organiser:
AKJ Associates Ltd
4/4a Bloomsbury Square
London WC1A 2RP
t: +44 (0) 20 7242 7820
e: simon.brady@akjassociates.com

Booklet printed by:
Method UK Ltd
Baird House
15–17 St Cross Street
London EC1N 8UN
e: hello@thisismethod.co.uk

Travelling to the future of cybersecurity

Booking.com is one of the world's leading marketplaces for travel. It makes sense, then, that they need world-class cyber defence capabilities.

The Cyber Detection and Response Group keeps Booking.com, its customers, partners and employees secure around the clock. The group oversees things like cyber-detection engineering, security product management and advanced cyber-incident response.

The group consists of over 45 highly talented, passionate security professionals, in charge of the cyber-defence of one of the biggest, most recognisable e-commerce companies in the world. So, maintaining Booking.com's overall security and compliance, as well as ensuring their customers' and partners' data is handled in-line with the highest international standards, is a core priority.

Starting out in the cybersecurity industry

Ariel Lemelson, Head of Cyber Detection & Response at Booking.com, describes his leadership style as 'empowering', inspiring his team with a shared vision and dedication to cybersecurity. "Build your team with people that share your passion and can become true partners that would share the excitement of the journey. Genuinely caring about your people and being consistently honest is also key in achieving an engaged, high-performing security group."

With over 17 years of cybersecurity domain experience, Ariel advises those starting out to be humble, always keep learning and continually look for tomorrow's practices: "Don't get stuck in the present," he says.

Cybersecurity is, of course, a constantly evolving and forward-looking industry. Ariel says that those who want to enter cybersecurity need to "get their hands dirty" and to not get disconnected from the practice as they grow, including "what is happening on the production floor". He adds that it is crucial to embrace the business context; security is not done in siloes: "We are here to serve and enable the business to innovate at speed, while keeping things secure and compliant." In short, Ariel believes that a can-do approach and high level of passion are drivers for success in this field.

What is unique about Booking.com and cybersecurity?

"We take online safety and the protection of consumer and partner data extremely seriously," says Ariel "We are continuously innovating our processes and systems to ensure optimal security on our platform, while constantly evaluating and enhancing the robust security measures we already have in place." "In line with the highest technical standards, our dedicated security and fraud teams monitor activity 24/7, utilising bespoke, state-of-the-art tooling to quickly detect and resolve any potentially suspicious activity, leveraging both internal and independent industry expertise to stay one step ahead of threats and adversaries."

It's no stretch to say that Booking.com hires top talent to make up their teams, as well as the best tooling and most advanced technologies available on the market – including the latest, most innovative methodologies.

What must companies do to prepare successfully for cyber-incidents?

"Observability and detection are vital for the response aspect of security. Simply put, if you can't detect it, then the chance for a timely response to a cyber-incident is low. In order to prepare, you need to define your process, your technology and your people on each of three components: observability, detection and response," says Ariel.

"As cyber-defence leaders, in order to be well prepared you would like to have identified your business priority risks and crown jewels, and have a thorough understanding of your threat landscape. To add to that, you want to have practical, well-practised and validated response procedures, as well as a trained and passionate cyber-incident response team, armed with top quality tooling."

Dealing with emerging threats

To stay one step ahead of emerging threats, you have to be able to correlate an abundance of information sources into a crisp reality image. This is done by smart contextualisation of the telemetry and alerts, correlating them with each other, with threat intelligence sources, and with business and risk information. Ariel says that "this allows you to keep your cyber-defence teams within a manageable amount of information of high value, and high effectiveness of security operations".

IT technologies have grown exponentially more complex over the years. In order to stay up to speed, cyber-defence teams have to be able to scale defence capabilities without requiring linear growth in resources.

Hunters reports

"Scale and effectiveness became an essential condition for success in cyber-defence, replacing manual efforts with automated ones," he says. "It is essential to work with the right tooling that allows us to contextualise all the dots and signals into a clear picture. This saves substantial amounts of time in prevention, detection, investigation and response, and increases the ROI of the security spending.

"The sophistication of the attackers requires better contextualisation, and a more adversarial point of view by the defence teams. Having the effective ability to defend the different dynamic environments and workloads on-prem and in-cloud requires robust automation and correlation capabilities to be up to speed with the pace of technology. Things that could have been manual in the past, can't be done in a manual fashion any more."

What is proactive defence?

"In the past, the common defence assumption of security teams was that an organisation was not compromised until proven otherwise. This was in alignment with the perimeter defence approach. With the changing of the paradigm into the mental model of 'Assumed Compromise', organisations now have to act as if the attackers are already in their environment. Still, making a working assumption that adversaries have access to the environment is different from assuming they have achieved their goals of stealing sensitive information or performing other impactful attacks like ransomware.

"In most mature organisations, for attackers to have a substantial impact or potential economic benefits, they would need to perform quite a complex operation, jumping from place to place carefully exploiting any potential 'digital holes' found.

"Proactive defence methodology assumes that the attackers are somewhere on their way from an initial access point towards the company data. In order to detect those potential attackers, defence teams deploy numerous types of cyber-traps called 'detections', and also actively hunt the attackers on their way," Ariel outlines.

For the uninitiated, these descriptions really give one a sense of cyber-warfare. In order to be successful in that, it is important to have the telemetry stored in an easily accessible fashion for longer terms, and to have tooling that can support security teams in making hunting efficient with all that information.

"In today's landscape, it is key to have more data rather than less, making less painful tradeoffs between which log source to save and for how long. With partial telemetry, the ability to efficiently hunt sophisticated attackers becomes limited."

Pitfalls in cyber-threat detection and response

"Some of the pitfalls cybersecurity defence teams encounter result from doing cyber-defence in a silo, without being fully aware of both the full attack surface and the most important business assets. This may lead to a security 'comfort zone', where there may be over-investment in defence of certain points, while other major blind spots are not properly defended and there's a lack of awareness and risk acceptance from the business. These disconnected situations may result in a negative scenario," says Ariel.

"There is also limited raw telemetry collection and retention, which impedes the ability to detect, hunt or investigate cyber-attacks. Cyber-defence teams do not always have a clear and open view of the threat landscape, or of the adversarial point of view. In such cases, it is almost impossible to provide proper cyber-defence to the business," he continues to explain. "The defence would be passive, driven by native alerts coming from security tools, lacking the holistic understanding of the '3D chess game' we play every day with our adversaries, as cyber-defence professionals."

Another potential pitfall in security defences is that it's common to see security organisations that simply don't measure the right KPIs. "If you don't define the KPIs properly," says Ariel, "you'll be creating the wrong incentives for the security teams, which will eventually lead to ineffective resource allocation, low team effectiveness and, potentially, to cyber-compromise."

Hunters

Empowering security teams to automatically identify and respond to incidents that matter across the entire attack surface, Hunters solves the data challenge with seamless, unlimited data ingestion and normalisation for all your security data at a predictable cost. Layered with built-in detection engineering, cross-stream data correlation, and automatic investigation, Hunters provides complete context to help your teams overcome volume, complexity, and false positives, to mitigate real threats more reliably than Security Information and Event Management (SIEM) tools.

"If you don't have unlimited human resources to throw at your SIEM, then Hunters is easily the best solution for you. It enables teams to do more with less. We don't need to manage our SIEM as we did before or babysit alerts and logic. We're now allowed to be security practitioners, look at events, and make meaningful strides to improve maturity, efficiency, and cost optimization."
John Fung, Deputy CISO at Cimpress □

HUNTERS

YOUR SOC PLATFORM

Helping security teams mitigate real threats faster and more reliably than SIEM

OUR SOLUTIONS

SIEM Replacement

Security Analytics / XDR

Threat Hunting

TRUSTED BY

Booking.com · cimpress · NETGEAR · snowflake

Continuous security testing is a must for organisations today

Securing constantly changing environments within rapidly evolving threat landscapes is particularly difficult.

Intigriti reports

The global cybersecurity market is flourishing. Experts at Gartner predict that the end-user spending for the information security and risk management market will grow from $172.5 billion in 2022 to $267.3 billion in 2026. However, costs and limitations involved in carrying out security testing spot checks, such as penetration tests (pentests), are already hindering the market growth. Consequently, many cybersecurity professionals are making moves to find an alternative solution.

The challenges of pentests for modern businesses

Pentesting can help businesses with specific cybersecurity challenges, like proving compliance to prospective customers. However, it's not always the best solution for every problem:

1. **Continuously changing environments**

Securing constantly changing environments within rapidly evolving threat landscapes is particularly difficult. This challenge is further complicated when new projects or releases need to be aligned with business risk. Pentests can only focus on one moment in time, so the results may not be the same after updates are made.

2. **Rapid growth**

It would be unusual for fast-growing businesses not to experience growing pains. For CISOs, maintaining visibility of their organisation's expanding attack surface can be particularly painful.

3. **Cybersecurity skills shortages**

Finding the available skillsets for internal cybersecurity teams is an ongoing battle. As a result, organisations don't have the dexterity to spot and promptly remediate specific security vulnerabilities. While pentests offer an outsider perspective, often it is from the viewpoint of just one or two people. For some organisations, there is an issue on trust when relying on the work of only a few experts.

4. **Time lags between tests and report delivery**

HelpNetSecurity reported that it takes 71% of pentesters one week to one month to conduct a pentest. Then, more than 26% of organisations must wait up to two weeks to get the report. Given the fast pace of threat evolution, this waiting period can leave companies unaware of potential security issues and open to exploitation.

5. **Poor-fitting security testing solutions for agile environments**

Penetration testing cycles (often performed annually) don't align with continuous development lifecycles. Vulnerabilities mistakenly created during long security testing gaps can remain undiscovered for some time.

Bringing security testing into the 21st-century

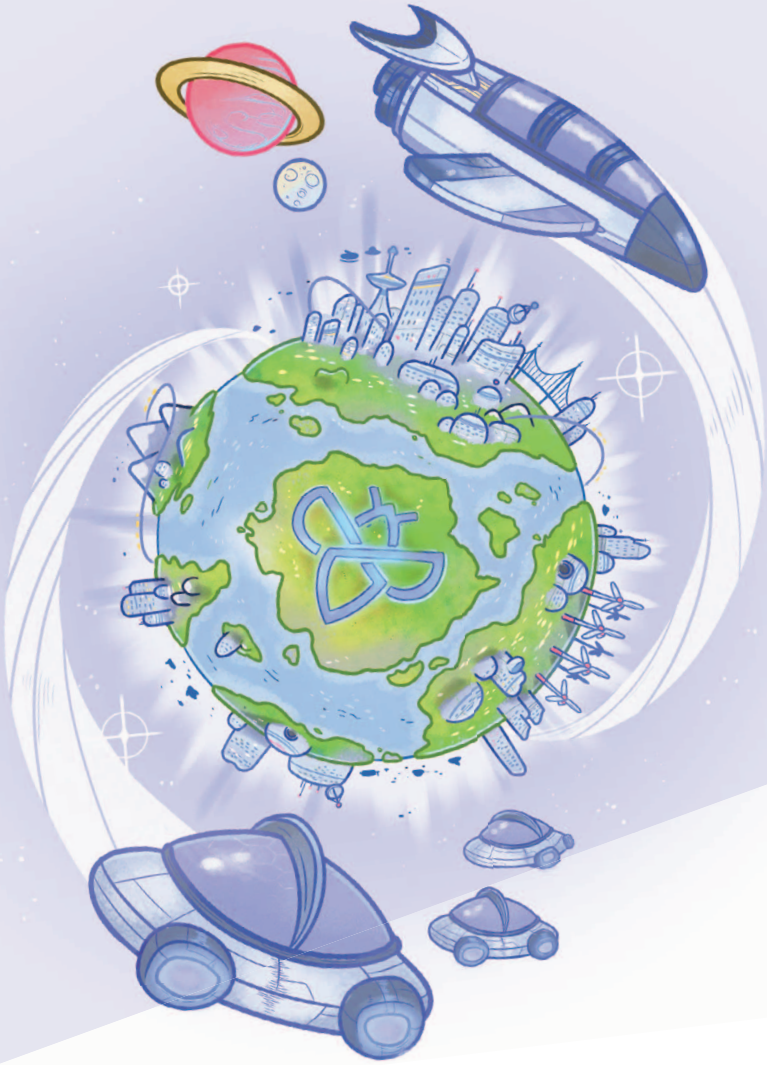
A proven solution to these challenges is to utilise and incentivise ethical hacker communities in addition to a standard penetration test. A common way to achieve this is through a bug bounty program.

The impact of bug bounty programs on cybersecurity

By launching a bug bounty program, organisations experience:

1. *More robust protection:* Company data, brand, and reputation have additional protection through continuous security testing.
2. *Enabled business goals:* Enhanced security posture, leading to a more secure platform for innovation and growth.
3. *Improved productivity:* Increased workflow with fewer disruptions to the availability of services. More strategic IT projects that executives have prioritised, with fewer security 'fires' to put out.
4. *Increased skills availability:* Internal security team's time is freed by using a community for security testing and triage.
5. *Clearer budget justification:* Ability to provide more significant insights into the organisation's security posture to justify and motivate for an adequate security budget.
6. *Improved relationships:* Project delays significantly decrease without the reliance on traditional pentests. □

Europe's #1 ethical hacking and bug bounty platform



About Intigriti

Intigriti's community of ethical hackers provides continuous, realistic security testing to help companies protect their assets and their brand. Discover how organizations can work with a globally distributed community of ethical hackers by downloading the report below.

www.intigriti.com

FREE INSIGHTS

Discover Intigriti's Ethical Hacker Insights Report 2022

Intigriti's Ethical Hacker Insights Report 2022 aims to demystify ethical hackers (security researchers) by deep diving into their motivations, drivers, challenges and ambitions. We also highlight the views of ethical hackers around bug bounty programs, penetration testing, and vulnerability reporting policies. Scan the QR code to download your free copy today!

Download the report

INTIGRITI

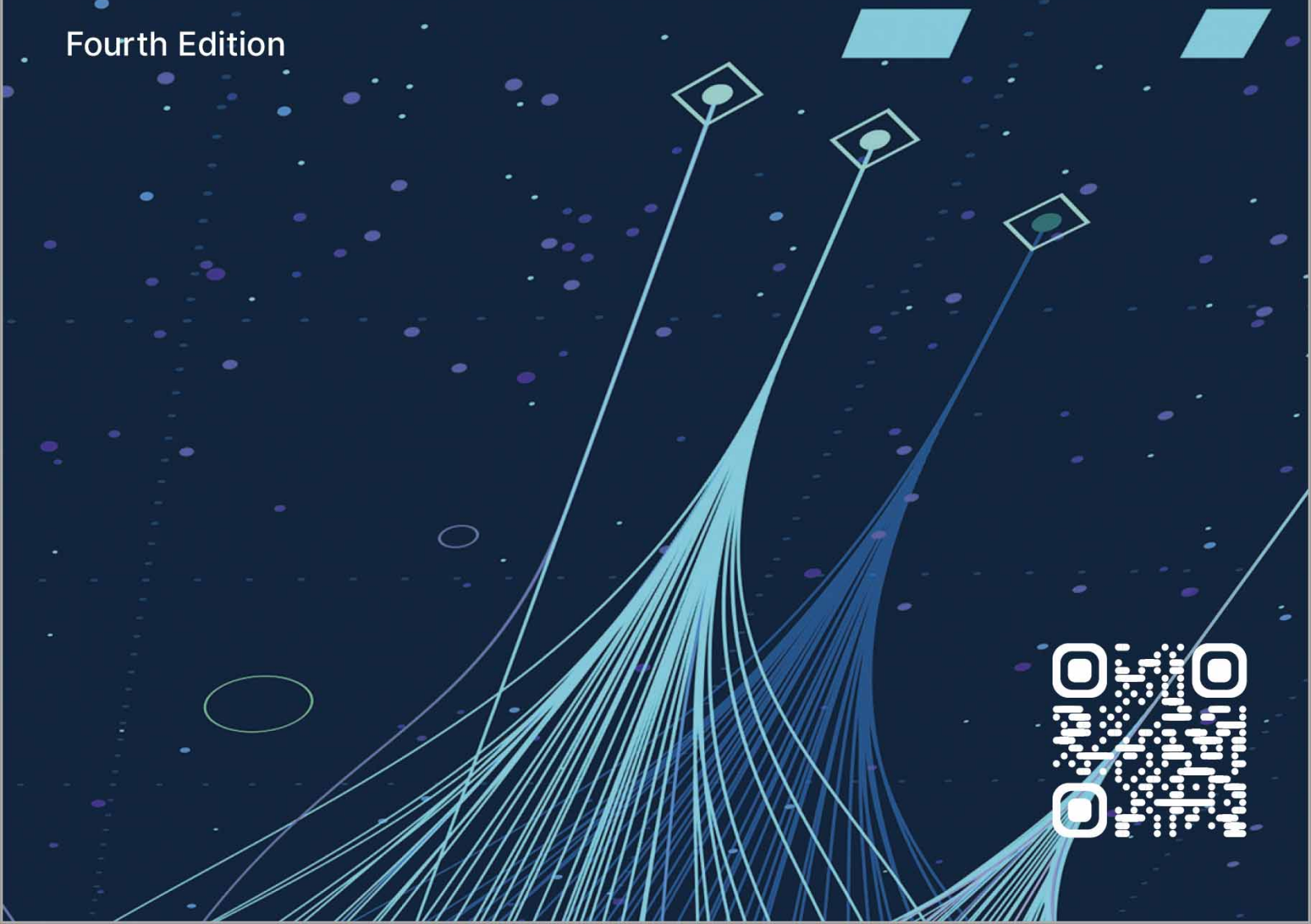
Agile Security Testing Powered by the Crowd

Recorded Future®

THE INTELLIGENCE HANDBOOK

A Roadmap for Building an Intelligence-Led Security Program

Fourth Edition



The business of fraud: Bank fraud

Recorded Future analysed current data between March 2021 and March 2022 to observe and identify how threat actors are conducting and advertising the following types of bank fraud: accounting, loan, checking, and wire transfer.

Recorded Future analysed current data from the Recorded Future® Platform, dark web and special-access sources, and open-source intelligence (OSINT) between March 2021 and March 2022 to observe and identify how threat actors are conducting and advertising the following types of bank fraud: accounting, loan, checking, and wire transfer. This report expands upon findings addressed in the first Insikt Group Fraud Series report, "The Business of Fraud: An Overview of How Cybercrime Gets Monetised".

Executive summary

Bank fraud is the use of illegal means to obtain money, assets, or other property owned or held by a financial institution or individual by fraudulently posing as a bank, another financial institution, or another individual. As the financial sector has incorporated online and internet-connected banking into its business model, traditional means of fraudulently acquiring funds from a bank have been replicated and updated to target today's online banking employee and consumer. Throughout Recorded Future's 'Business of Fraud' series of reports, we have identified many tactics, techniques, and procedures (TTPs) being used by cybercriminals to facilitate online criminal activities. Many of these same TTPs, from harvesting and using compromised personally identifiable information (PII) to social engineering, are also being used to conduct banking and online banking account fraud. In this report, we examined cybercriminal activities around the following types of bank fraud due to them often being overlooked and to identify parallels with other types of financial-related fraud: accounting, loan, check, and wire transfer.

Key findings

Threat actors are offering services and selling how-to guides and tutorials that include instructions on how to manipulate financial records, get approval for loans, and purchase compromised accounts that contain loan application information. Hackers-for-hire include the capability of accessing and manipulating records and documentations in their advertisements.

Counterfeit checks are still in high demand and are often coupled with threat actors looking to conduct wire transfers or cash out. The means of creating a counterfeit check has become more automated and customised, with threat actors operating shops that focus on this service and whose user interface is easy to follow.

Threat actors continue to use instant messaging platforms to advertise, negotiate, and sell services and listings that facilitate check, loan, wire transfer, and accounting frauds. These messaging platforms are all-encompassing when compared to the traditional dark web ecosystem (forums, marketplaces, and shops) in that they provide instantaneous communication, greater control in adding and removing listings, and are more readily available.

Background

Bank fraud is the use of illegal means to obtain money, assets, or other property owned or held by a financial institution, or to obtain money from depositors by fraudulently posing as a bank or other financial institution. While the specific elements of banking fraud laws vary depending on jurisdictions, the term 'bank fraud' applies to actions that employ a scheme or artifice, as opposed to bank robbery or physical theft. For this reason, bank fraud is sometimes considered a white-collar crime. Online banking services now allow customers to access bank accounts and records via personal computers and mobile devices. This convenience has not only increased the attack surface but has allowed cybercriminals to creatively leverage new and old methods for conducting nefarious activities.

Threat actors gain access to online banking accounts in multiple ways, such as using a stolen identity (identity theft) to open new accounts (application fraud) or obtaining valid credentials to existing accounts (account takeover) through phishing, credential reuse, different types of malware, or

Recorded Future reports

A majority of bank related fraud involves compromised payment data and accounts, compromised PII data and bypass methods (among others) used in accounting, loan, checking, and wire transfer. These types of fraud are being actively sought after and advertised across the entirety of the dark web criminal ecosystem.

purchasing them from dark web sources. Given the previous reporting done by Recorded Future that relates to financial crimes (laundering funds, using compromised PII and counterfeit documentation to open accounts, using sniffers, bank injects/overlays, infostealers to harvest banking credentials to take over accounts and payment cards, and recruiting mules and cashout services), this report will not focus specifically on compromised payment card data or one of the aforementioned topics. Rather, this report will examine how cybercriminals are conducting operations across a variety of dark web and special-access sources to facilitate the following types of bank fraud, which are not as commonly known or popularised: check, loan, wire transfer, and accounting fraud.

Types of bank fraud

Many of the aspects covered throughout our Fraud Series overlap with TTPs being used by threat actors to facilitate bank fraud:

- A majority of threat actors are not specifically advertising services for the 4 types of bank fraud addressed in this report; rather, are offering services and methods that include these activities in conjunction with other types of financial fraud.
- Like with most types of fraud, compromised credentials and PII to create or gain control of accounts are the lifeblood of bank fraud. Threat actors advertising these types of compromised data are using the same forums, marketplaces, and shops (both as sellers and buyers) to facilitate other types of fraudulent cybercrimes.

Threat actors are lately interested in synthetic identities, a type of fraudulent identity that combines the proprietary PII (such as date of birth, Social Security number) of several individuals to make a single, new identity. Although this report does not specifically investigate synthetic identities, the amount of compromised PII data widely available across dark web sources coupled with the widely shared knowledge of performing fraudulent activities (social engineering, phishing, among others) makes this attack vector an attractive tactic to be used by criminals in the future, specifically those wanting to commit bank and financial-related crimes such has registering account or loan applications. According to our data sets, there are multiple tutorials and how-to guides on creating synthetic identities across different dark web and special-access sources.

Outlook

The 4 types of fraudulent activities that facilitate bank fraud covered in the full report showcase how different types of fraud are using similar methods and require similar data to facilitate activities. A majority of bank related fraud involves compromised payment data and accounts, compromised PII data and bypass methods (among others) used in accounting, loan, checking, and wire transfer. These types of fraud are being actively sought after and advertised across the entirety of the dark web criminal ecosystem, with threat actors continuing to incorporate instant, encrypted messaging platforms into their methods for advertising, discussing, seeking, and selling services and products.

As highlighted in Recorded Future's 2020 series on the automation and customisation of the dark web, the threat actors highlighted in this report (as well as the many others) are continuing to customise their services, host automated shops and marketplaces with easy-to-use interfaces, and update their attack vectors to defeat security measures. We believe threat actors will continue to incorporate automation and customisation into their business model so as to attract customers and make profits. As the demand for these services show no signs of dissipating, we recommend working with Recorded Future so as to receive timely updates and notifications of events or listings that may affect your brand. Once an alert is received, we recommend triaging it for severity and working with us to identify solutions and steps to be taken in the future to harden your security measures.

Editor's note: This article is an excerpt of a full report. Click the PDF link to read the entire analysis. □

Mapping Web 3 threats

With this new generation of the internet and the tsunami of new technological use cases which will transform businesses, create new services and revenue streams, there will also be new threats that will need to be mitigated.

Lydia Kostopoulos, PhD reports

It has been said that "the only thing constant in life is change." This couldn't be more true for the rate of technological change. Just in the past two decades of this 21st Century we have seen mobile computing, the internet and GPS transform so many industries and our daily lives. Today, we are already at the cusp of another wave of technology transformations, which is bringing about a new way that we experience the internet. As this next generation of the internet is still in development, the definition for it remains to be agreed upon. Where there seems to be relatively more consensus is labelling it as Web 3.

The idea behind Web 3.0, is that the first version of our internet experience (Web 1.0) was characterised by read only websites and was overwhelmingly browser based. In the next generation of the internet (Web 2.0) social media, blogs and other platforms came about which democratised the exchange of information by allowing everyone to write, post and share. This version of the internet was also experienced outside browsers and on apps, mobile devices and other Internet of things (IoT). This next generation of the internet (Web 3.0 or simply Web 3) is one that is amplified by artificial intelligence, space technology and an increasing social movement for digital ownership. This will manifest itself in the spatial web where networked IoTs will be part of the human-machine teaming organisational work flow, where the digital twins will anticipate and provide greater strategic awareness of what it has cloned and where digital assets create new economies, yet to be imagined in virtual spaces across virtual and augmented reality space.

However, with this new generation of the internet and the tsunami of new technological use cases which will transform businesses, create new services and revenue streams, there will also be new threats that will need to be mitigated. Despite the changes in technology, the core areas of threats do not change and they are the main elements in our technological experiences: the people, the hardware, the software and the communication layer. Each of these will see new and evolving threats as the technology changes.

It is now widely understood by cybersecurity practitioners that there is no such thing as 100% security. Instead, there are continued and ongoing risks that require continuous management.

Hardware: Vulnerabilities at the edge

Digital twins, smart infrastructure, sensors and connected metaverse accessories will mean a continued increase in IoT devices. At the beginning of the pandemic, there were 9.8 billion IoT devices connected to the internet and a couple of years later there are now 13.4 billion. It is anticipated that by the end of this decade the number of internet devices will more than double reaching 29.4 billion. The increase in the number and diversity of devices will be more entry points and more third-party risks that will arise from different vendors and their varied levels of standards and compliance. Managing these risks will mean having as much situational awareness as possible about how third parties are managing their risks and identifying ways in which they can be reduced or minimised. Creating a digital twin can help pinpoint each area of the business and identify areas that are more sensitive to business continuity than others.

It is now widely understood by cybersecurity practitioners that there is no such thing as 100% security. Instead, there are continued and ongoing risks that require continuous management. The following four categories attempt to map out some of the key cybersecurity risks in the Web 3 environment.

Communications layer risks

Whether it is NFC, Bluetooth, 5G/6G, WiFi, fiber, satellite or any other means of communication that devices use to exchange information, there will be continued risks that will need to be managed. The risks remain constant and they include disruption such as a DDoS attack, an interception such as a breach or a sabotage to the service be it through a malicious attack on the electromagnetic spectrum or a physical attack. Communications layer risks will be all the more troublesome when we start to rely on the spatial web and augmented reality from bus schedules posted on top of the physical station, to enhanced retail and cultural experiences. Much of the Web 3 environment will be omnipresent, intuitive and networked and it will be the reliability of the communications layer that will make it seamless. Hackers will seek to disrupt and deny this layer in communications DDoS.

Security by design is not the standard practice but the hope is that with more awareness of risk there will be more security designed into code, procedure and awareness of cyber-scams and crime. There is much more to come as the next generation of the internet is only just starting to emerge.

Software: Processing layer risks

The software layer is where all the processing of information happens, whether it is in the cloud or on prem. It is where the analytics, big data, machine learning, automation and algorithms generate business value. This component will get even bigger with Web 3 as blockchain (and chain bridges), NFT contracts and tokens become additional elements in this software processing layer. There are many risks that will need to be managed such as the Confidentiality, Integrity and Authenticity (CIA) of data and its exposure. With the many different software, chain bridges, and algorithms resilience in deflecting hacking attempts and continuous patching will be of paramount importance. Vulnerability assessments on vendors will need to be done periodically to determine their reliability when it comes to backdoors and other threats. While still an emerging risk, algorithm hacking or decision hacking is one that will grow as malicious actors seek to game algorithms.

Wetware: Human risk

Last but certainly not least, human risk needs to be managed alongside the above cybersecurity risks. While there is no software patch for human risk, there is security awareness education which helps users understand the ways in which malicious actors seek to manipulate people into divulging sensitive information or granting them access they should not have. Phishing, vishing, smishing, tailgating techniques continue to plague companies resulting in costly ransomware attacks, loss of valuable intellectual property and breached data damaging brand reputations. Human related attack vectors will not disappear with Web 3, instead they will increase as there are many new attack vectors that malicious actors can use in these new spaces. Whether it is avatar spoofing, identity jacking or other attacks in the metaverse. The most effective way to mitigate and posture an organisation from evolving human risk is through a strong security culture where employees have been trained to spot anomalies and suspicious behaviour in these new spaces.

Security by design is not the standard practice but the hope is that with more awareness of risk there will be more security designed into code, procedure and awareness of cyber-scams and crime. There is much more to come as the next generation of the internet is only just starting to emerge. □

KnowBe4
Human error. Conquered.

Why security awareness training?

RANSOMWARE
PHISHING
CEO FRAUD
COMPLIANCE

That's why.

TEST

TRAIN

PHISH

RESULTS

KnowBe4, Inc. | 855-566-9234 | www.KnowBe4.com | sales@KnowBe4.com

CROWDSTRIKE

we stop **breaches**

crowdstrike.com

CrowdStrike's Annual Threat Hunting Report reveals one potential intrusion is identified every seven minutes

Findings from Falcon Overwatch threat hunters showed faster breakout times by e-crime adversaries and one million malicious events were prevented by the CrowdStrike Falcon platform.

CrowdStrike reports

AUSTIN, Texas – September 13, 2022 – CrowdStrike (Nasdaq: CRWD), a leader in cloud-delivered protection of endpoints, cloud workloads, identity and data, today announced the release of the fourth annual CrowdStrike Falcon OverWatch threat hunting report: *Nowhere to Hide: 2022 Falcon OverWatch Threat Hunting Report*. The global report reveals a record 50% year-over-year (YoY) increase of hands-on intrusion attempts, and distinct changes in attack trends and adversary tradecraft. Most notably, Falcon OverWatch threat hunters identified more than 77,000 potential intrusions, or approximately one potential intrusion every seven minutes. These are instances where proactive, human-led threat hunting uncovered adversaries actively carrying out malicious techniques at various stages of the attack chain, despite attackers' best efforts to covertly evade autonomous detection methods.

Falcon OverWatch calculated that the breakout time (i.e. the time, on average, it takes an adversary to move laterally from initial compromise to other hosts within the victim environment) for e-crime adversaries has fallen to one hour and 24 minutes – compared to one hour and 38 minutes as reported by Falcon OverWatch in the 2022 CrowdStrike Global Threat Report. Moreover, Falcon OverWatch found that in approximately one-third (30%) of those e-crime intrusions, the adversary was able to move laterally in under 30 minutes. These findings underline the speed and scale at which threat actors evolve their tactics, techniques and procedures (TTPs), and are capable of bypassing even the most sophisticated technology-based defence systems to successfully achieve their goals.

Falcon OverWatch calculated that the breakout time (i.e. the time, on average, it takes an adversary to move laterally from initial compromise to other hosts within the victim environment) for e-crime adversaries has fallen to one hour and 24 minutes – compared to one hour and 38 minutes as reported by Falcon OverWatch in the 2022 CrowdStrike Global Threat Report.

"Over the past 12 months, the world has faced new challenges spurred by economic pressures and geopolitical tensions, backdropping a threat landscape that is as complicated as ever," said Param Singh, Vice President, Falcon OverWatch at CrowdStrike. "To thwart brazen threat actors, security teams must implement solutions that proactively search for hidden and advanced attacks every hour of every day. The combination of the CrowdStrike Falcon platform with the telemetry, tooling, threat intelligence and human ingenuity of Falcon OverWatch managed threat hunting protects organisations globally against the most sophisticated and stealthy threats."

Other key findings from the report include:

- *e-Crime is the top threat type for interactive intrusion campaigns.* e-Crime accounted for 43% of interactive intrusions, while state-nexus actors accounted for 18% of activity. Hacktivists accounted for just 1% of interactive intrusion campaigns, with the remaining intrusions unattributed.
- *Adversaries continue shifting away from malware.* Malware-free threat activity accounted for 71% of all detections indexed by the CrowdStrike Threat Graph. The predominance of malware-free activity is related, in part, to adversaries' prolific abuse of valid credentials to facilitate access and persistence in victim environments. Another factor is the rate at which new vulnerabilities are being disclosed and the speed with which adversaries are able to operationalise exploits.
- *Technology is the top industry targeted for interactive intrusions.* The top five industries targeted overall were technology (19%), telecommunications (10%), manufacturing (7%), academic (7%) and healthcare (7%). Of note,

The telecommunications industry continues to be preyed on for fulfillment of state-sponsored surveillance, intelligence and counterintelligence collection priorities. Of note, telecommunications faced 163% more targeted intrusions by state-nexus actors than the second-most targeted industry.

technology was targeted 90% more frequently by interactive intrusions than the second-most targeted industry.

- *Telecommunications is the top industry for targeted intrusions by nation-state actors.* The top five industries targeted overall were telecommunications (37%), technology (14%), government (9%), academic (5%) and media (4.5%). The telecommunications industry continues to be preyed on for fulfillment of state-sponsored surveillance, intelligence and counterintelligence collection priorities. Of note, telecommunications faced 163% more targeted intrusions by state-nexus actors than the second-most targeted industry.
- *Healthcare finds itself in the crosshairs of Ransomware-as-a-Service (RaaS).* The volume of attempted interactive intrusions against the healthcare industry has doubled year-over-year. A significant majority of these intrusions have been attributed to e-crime.

The report includes insights from Falcon OverWatch's global threat hunting operations from 1st July 2021 through 30th June 2022, and outlines in-depth attack data and analysis, case studies and actionable recommendations.

Additional resources

- Download your copy of the full report *Nowhere to Hide: 2022 Falcon OverWatch Threat Hunting Report* on the CrowdStrike website and read the blog. □

For more information, please visit
www.crowdstrike.com

CROWDSTRIKE

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

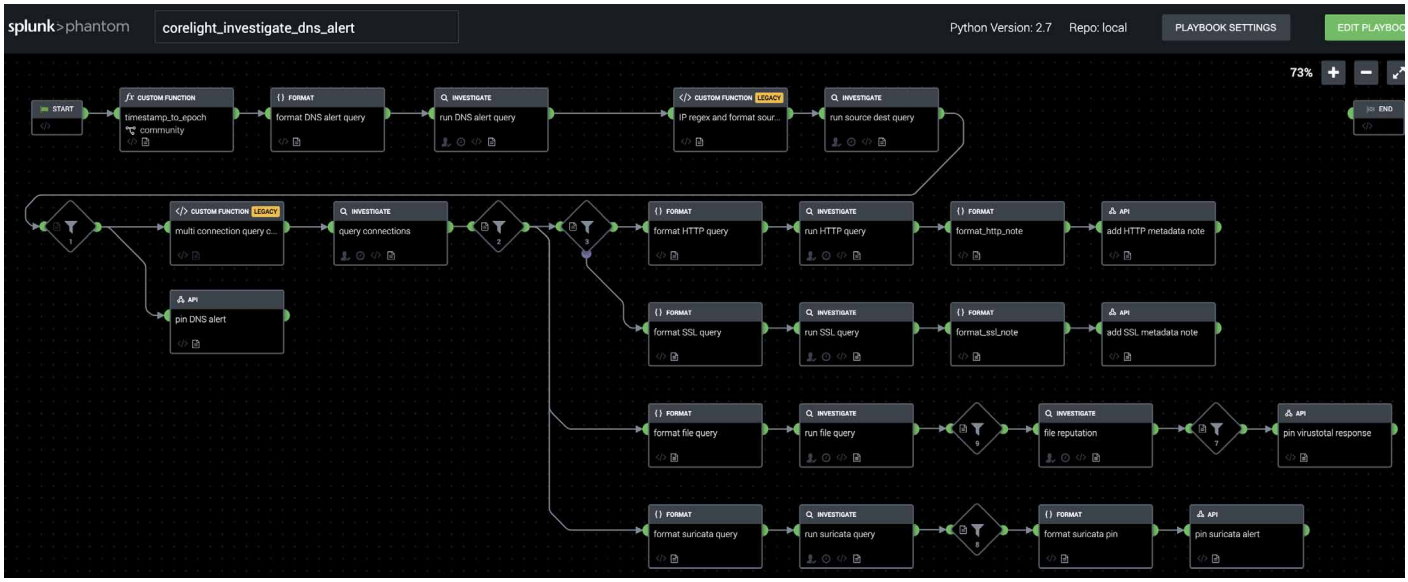
SOCs can resolve these operational pain points by shifting to a network traffic-centric logging model, enabled by open source Zeek (and its turnkey commercial implementation on Corelight appliances). Designed to parse live traffic streams and log relevant metadata across a wide variety of protocols, 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. □

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

Sponsors and exhibitors

Corelight | Strategic Sponsor

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders. Based in San Francisco, Corelight is an open-core company founded by the creators of Zeek, the widely-used NSM tool and providing an Open NDR Platform.

For more information, please visit corelight.com

CrowdStrike | Strategic Sponsor

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph, CrowdStrike Falcon correlates over 5 billion endpoint-related events per week in real time from across the globe, fuelling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.

Learn more at www.crowdstrike.com

Darktrace | Strategic Sponsor

Darktrace (DARK.L), a global leader in cybersecurity artificial intelligence, is on a mission to free the world of cyber-disruption. Breakthrough innovations in our Cyber AI Research Centre in Cambridge, UK have resulted in over 100 patents filed and research published to contribute to the cybersecurity community. Rather than study attacks, our technology continuously learns and updates its knowledge of 'you' and applies that understanding to optimise your state of optimal cybersecurity. We are delivering the first ever Cyber AI Loop, fuelling a continuous end-to-end security capability that can autonomously spot and respond to novel in-progress threats within seconds. Darktrace employs over 2,000 people around the world and protects over 7,400 customers globally from advanced cyber-threats. Darktrace was named one of TIME magazine's 'Most Influential Companies' in 2021.

To learn more, visit darktrace.com

Hunters | Strategic Sponsor

Hunters is an SOC platform that empowers security teams to automatically identify and respond to incidents that matter across their entire attack surface, at a predictable cost. Through built-in detection engineering, data correlation, and automatic investigation, we help teams overcome volume, complexity, and false positives. Hunters mitigates real threats faster and more reliably than SIEMs, ultimately reducing customers' overall security risk.

For more information, please visit www.hunters.ai

Intigriti | Strategic Sponsor

Intigriti is an award-winning cybersecurity company that specialises in incentivised security testing through bug bounty programs. Founded in 2016, Intigriti set out to conquer the limitations of traditional security testing, such as pentests. Its interactive platform enables clients to launch managed security testing at scale and better prioritise remediation by more accurately assessing risk.

Clients continuously test their digital assets for vulnerabilities by leaning on Intigriti's 50,000 security researchers. On average, companies receive 53 reports within one week of launching on the platform. Additionally, 71% receive a high to critical vulnerability report within 48 hours.

As a global market leader in bug bounty programs, clients of all sizes and from a wide range of business sectors utilise Intigriti's platform and services. The business works with over 300 clients, from small tech start-ups to large banks and airlines. Its focus lies on innovation and outstanding customer service.

Intigriti offers all its customers (no matter the size, maturity level or industry) full triaging services and a dedicated customer success manager. Intigriti's triage team provides a layer of quality assurance before escalating vulnerabilities to businesses. Internal security teams therefore only receive reports that are valid, unique and in scope. Customers are also supported by their success manager from preboarding and onboarding through to post-launch activities to ensure their bug bounty program reaches maximum potential.

In 2021, Intigriti received Deloitte's 2021 Fast 50 Award as recognition for the impact the platform has made. In 2020, the business won Deloitte's Rising Star award.

For more information, please visit www.intigriti.com

KnowBe4 | Strategic Sponsor

KnowBe4 is the world's largest security awareness training and simulated phishing platform that helps you manage the ongoing problem of social engineering.

The KnowBe4 platform is user-friendly and intuitive. It was built to scale for busy IT pros that have 16 other fires to put out. Our goal was to design the most powerful, yet easy-to-use platform available.

Customers of all sizes can get the KnowBe4 platform deployed into production twice as fast as our competitors. Our Customer Success team gets you going in no time, without the need for consulting hours.

For more information, please visit www.knowbe4.com

Recorded Future | Strategic Sponsor

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organisations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organisations around the world.

Learn more at recordedfuture.com

Abnormal Security | Education Seminar Sponsor

Abnormal Security provides a leading cloud-native email security platform that leverages AI-based behavioural data science to stop business email compromise (BEC) and never-seen-before attacks that evade traditional secure email gateways (SEGs). Abnormal delivers a fundamentally different approach that precisely detects and protects against the widest range of attacks including phishing, malware, social engineering, spam and graymail, supply chain compromise, and internal account compromise.

The Abnormal platform delivers inbound email security, internal and external account takeover protection, and full SOC automation. Abnormal's API-based approach enables customers to get up and running in 15 minutes and can augment a SEG or be used standalone to enhance native Microsoft security protection. Abnormal Security is based in San Francisco, CA.

More information is available at abnormalsecurity.com

Menlo Security | Education Seminar Sponsor

Menlo Security protects organisations from cyber-attacks by seeking to eliminate the threat of malware from the web, documents, and email. Our cloud-based Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions.

For more information, please visit www.menlosecurity.com

OPSWAT | Education Seminar Sponsor

OPSWAT is a global leader in critical infrastructure cybersecurity that helps protect the world's mission-critical organisations from malware and zero-day attacks. To minimise the risk of compromise, OPSWAT Critical Infrastructure Protection solutions enable both public and private organisations to implement processes that ensure the secure transfer of files and devices to and from critical networks. More than 1,000 organisations worldwide spanning financial services, defence, manufacturing, energy, aerospace, and transportation systems trust OPSWAT to secure their files and devices; ensure compliance with industry and government-driven policies and regulations, and protect their reputation, finances, employees and relationships from cyber-driven disruption.

For more information on OPSWAT, visit www.opswat.com

ReliaQuest | Education Seminar Sponsor

ReliaQuest, a global leader in cybersecurity, helps organisations achieve consistent security outcomes. ReliaQuest GreyMatter is a SaaS-based, unified threat detection, investigation and response platform aimed at reducing security complexity. Enhanced threat detection speeds response by force multiplying teams with curated integration and automation applied across the security operations process. Hundreds of security leaders trust ReliaQuest to deliver Open XDR outcomes – driving greater efficacy, efficiency and resilience, giving them the confidence to proactively advise on and manage risk for the business. ReliaQuest is a private company headquartered in Tampa, Fla., with five global locations.

For more information, visit www.reliaquest.com

Synack | Education Seminar Sponsor

Synack, the most trusted crowdsourced security testing platform, delivers on-demand security testing, intelligence, and operations through a continuous, offensive SaaS platform with crowdsourced talent. The company combines the world's most skilled and trusted ethical hackers with AI-enabled technology to create a scalable, effective security solution. Headquartered in Silicon Valley with regional offices around the world, Synack protects leading global banks, the top 10 global consulting firms and security companies, DoD classified assets, and over $2 trillion in Fortune 500 revenue. Synack was founded in 2013 by former NSA security experts Jay Kaplan, CEO, and Dr. Mark Kuhr, CTO.

For more information please visit us at www.synack.com

Vectra | Education Seminar Sponsor

Vectra® is a leader in threat detection and response for hybrid and multi-cloud enterprises. The Vectra platform uses AI to detect threats at speed across public cloud, identity, SaaS applications, and data centres. Only Vectra optimises AI to detect attacker methods – the TTPs at the heart of all attacks – rather than simplistically alerting on 'different'. The resulting high-fidelity threat signal and clear context enables security teams to respond to threats sooner and to stop attacks in progress faster. Organisations worldwide rely on Vectra for resilience in the face of dangerous cyber-threats and to prevent ransomware, supply chain compromise, identity takeovers, and other cyber-attacks from impacting their businesses.

For more information, visit vectra.ai

GATEWATCHER | Networking Sponsor

European leader in intrusion detection and advanced threat detection, GATEWATCHER has been protecting the critical networks of large companies and public institutions since 2015. Our solutions provide an immediate improvement to the current cybersecurity challenges and an adapted response to the growing needs in threat detection of organisations.

Our vision is to offer a flexible (cloud, on-premises, hybrid), scalable, innovative, open to new technologies and artificial intelligence without disrupting the existing architecture. But also to facilitate the operations of cybersecurity teams to enable them to be more efficient in prioritising their remediation actions.

AionIQ is an open NDR platform offering threat mapping and behavioural analysis for enhanced detection and unprecedented visibility into targeted attacks

Trackwatch is an ANSSI-qualified on-premise solution that combines advanced network flow analysis with innovative advanced threat detection techniques.

LastInfoSec is a Cyber Threat Intelligence feed that enriches your detection with contextual information about threats targeting your business.

For more information, please visit www.gatewatcher.com

Picus Security | Networking Sponsor

At Picus Security, we help organisations to continuously validate, measure and enhance the effectiveness of their security controls so that they can more accurately assess risks and strengthen cyber-resilience. As the pioneer of Breach and Attack Simulation (BAS), our Complete Security Control Validation Platform is used by security teams worldwide to proactively identify security gaps and obtain actionable insights to address them.

For more information, please visit www.picussecurity.com

RevealSecurity | Networking Sponsor

RevealSecurity detects malicious insiders and imposters by monitoring user journeys in enterprise applications. RevealSecurity's detection is ubiquitous – applied on any application, and across applications, including SaaS applications, cloud applications and custom-built applications. The detection protects enterprise organisations against cases in which either an authenticated user is taking advantage of their permissions to perform malicious activities, or when an impersonator successfully bypasses authentication mechanisms to pose as a legitimate user. RevealSecurity's tracking of user journeys does not rely on application-specific rules, and is instead powered by innovative user journey analytics, combined with a unique clustering engine to accurately detect abnormal journeys which reflect malicious activities.

For more information, please visit www.reveal.security

Silobreaker | Networking Sponsor

Silobreaker helps business, security and intelligence professionals make sense of the overwhelming amount of data on the web. By providing powerful tools and visualisations that cut through noise and analyse data from hundreds of thousands of open sources, Silobreaker makes it easy for users to monitor and research companies and industries, threats, compromises, actors, instabilities, geopolitical developments or any other topic, incident or event. Customers save time by working more efficiently through large data-sets and improve their expertise, knowledge and decision-making by examining and interpreting contextually relevant data more easily.

For more information, please visit www.silobreaker.com

OPSWAT.

Trust no file.

Trust no device.

Prevent targeted attacks with a strong line of defense purpose-built for IT/OT cybersecurity; protect your network perimeter with the OPSWAT MetaDefender family of solutions:

MetaDefender Kiosk scans portable media before it interacts with anything on your network.

MetaDefender Vault is a secure file storage and retrieval solution that protects critical data & keeps threats at bay.

MetaDefender Drive ensures transient cyber assets are safe to be on your network.

Visit opswat.com today to schedule a free demo and learn how OPSWAT can help keep your company protected from cybercrime.

AGENDA

08:00 Registration & networking

08:50 Chairman's welcome

09:00 **Balancing regulation/compliance and security**

Paul Van den Berg, Strategic Relations & Partnerships, NCSC-NL

Globally, stakeholders expect transparency on cyber-risks, and regulators are forcing organisations to act. Are CISOs and boards ready to engage in meaningful conversations?

- The importance of acknowledging the 'material' and increasing risk
- Addressing the communication gap between board and senior stakeholders
- Breaking down conservative attitudes
- How to engage in meaningful conversations

09:20 **The 2022 malware and vulnerability threat landscape**

Julian Kanitz, Lead Sales Engineer DACH, Recorded Future

The presentation examines trends in Malware use, distribution, development and high-risk vulnerabilities disclosed by major hardware and software vendors in the first half of 2022. It will cover:

- An overview of the threat landscape of malware and vulnerabilities
- Top referenced malware variants associated with cyber-attacks
- Top vulnerabilities associated with cyber-attacks
- Tips on how to strengthen your security posture and advisement for threat hunting teams and security operations centre teams
- Outlook for the rest of 2022 based on H1 2022 observations

09:40 **Mapping Web 3 threats**

Dr. Lydia Kostopoulos, Senior Vice President of Emerging Tech Insights, KnowBe4

- Contextualises the 4th industrial revolution and the technologies that are a part of it
- Unpacks the components of Web 3 including the metaverse, internet of things, digital twins and decentralised technology
- Categorises and explains the threats in the expanding cyber-terrain

10:00 **Fireside chat: A CISO's perspective on….**

Conference Chairman & **Dimitri van Zantvliet,** Chief Information Security Officer, Nederlandse Spoorwegen

- How the macroeconomic downturn will affect CISOs, budgets and security
- Dealing with the risks of state-sponsored cyber-attacks and spillovers
- Protecting critical national infrastructure
- The cyber-talent shortage – real or illusion?

10:20 **Education Seminars | Session 1** **See pages 28 and 29 for more details**

Synack	**Vectra AI**
Using security testing to drive change for the better	**Erasing surface, identity, complexity and unknowns**
Paul Mote, Senior Director, Solutions Architects, Synack	**Christian Borst,** EMEA CTO, Vectra AI

11:00 Networking break

11:30 **The value of strategy in information security**

Arash Rahmani, Head of Information Security, Nationale-Nederlanden C&C

- Why security culture matters for third-party risk management
- The strategic role of a CISO
- The EU impact on third-party risk management

11:50 **Fast and furious attacks: Using AI to surgically respond**

Rick Verhagen, Cybersecurity Enterprise Account Executive, Darktrace

Fast-moving cyber-attacks like ransomware can strike at any time, and security teams are often unable to react quickly enough. Join Rick Verhagen, Cybersecurity, Senior Account Executive at Darktrace, to learn how Autonomous Response uses Self-Learning AI's understanding of 'self' to take targeted action to stop in-progress attacks, without disrupting your business.

- Learn how Autonomous Response knows exactly the right action to take, at the right time, to contain an in-person attack
- How AI takes precise action to neutralise threats on the behalf of security teams
- Use of real-world threat finds to illustrate the workings of Autonomous Response technology

12:10 **How to address the skills shortages in a proactive manner to respond to adversaries**

Robert Elferink, Sr. Manager, Sales Engineering Benelux & Nordics, CrowdStrike

- Tooling and techniques to address skills shortages
- Automation and services to keep you ahead of attackers
- How technology can help you become proactive and stop breaches

12:30 Hunters: The SOC of the future

Hanan Levin, VP Sales EMEA, Hunters

Join Hunters to explore the key trends and paradigm shifts in data, detection and investigation, within the ever changing world of SOCs.

- Find out how you can increase data retention whilst reducing your costs, through using built-in-detection and automation in your SOC platform

12:50 Education Seminars | Session 2 **See pages 28 and 29 for more details**

Menlo Security
The next class of browser-based attacks
Tom McVey, Solution Architect, Menlo Security

OPSWAT
File upload protection: A critical gap in web app security
Rachid Mekdoud, Sales Engineer, OPSWAT

13:30 Lunch break

14:30 Cyber-resilience assessments and benchmarking

Raymond Kleijmeer, Senior Officer Cyber Resilience, De Nederlandsche Bank

Raymond will share practical experiences on:

- How to perform a self-assessment with Carnegie Mellon University's Cyber Resilience Assessment methodology
- Use the outcomes to make improvements
- Develop relevant benchmarking to enable peer comparisons

14:50 Is network evidence really needed for security operations?

Matthew Ellison, Director of Sales Engineering EMEA, Corelight

- Do you consider network evidence a crucial part of your SOC strategy?
- How do you really know which alerts are the most serious?
- What's the best way to shift from responding to alerts to hunting for threats?
- Understand how to stay ahead of ever-changing attacks by using a data-first approach for detection and response.

15:10 Defining 'ethical' hackers

Guus van Delft, Bug Bounty & Crowdsourced Security Account Executive, Intigriti

- Learn about the true meaning of ethics in hacking
- Walk through the thin line between criminal and lawful
- Discover what your company can do to reduce the grey zone to an absolute minimum

15:30 Education Seminars | Session 3 **See pages 28 and 29 for more details**

Abnormal Security
Key considerations for choosing the right cloud email security platform
David Lomax, Systems Engineer, Abnormal Security

ReliaQuest
The future of security operations: Threat intelligence, automation, and data-stitching
Rasham Rastegarpour, Sales Engineer, ReliaQuest

16:10 Networking break

16:30 How to make your company more cyber-resilient

Patrick Van den Branden, Group IT Security Officer, Euroports Group

- A pro-active and reactive approach
- A step-by-step process
- Working on 3 axes: Technical, Governance and Human
- The cybersecurity culture

16:50 The metaverse opportunity

David Palmer, Business Lead for Blockchain Technology, Vodafone

- What are the key enablers for virtual and real worlds to co-exist
- The key challenges
- Security, identity, jurisdiction, copyright and ownership

17:10 EXECUTIVE PANEL DISCUSSION Future challenges

Marc Berns, CISO, Allianz Benelux; **Arash Rahmani,** Head of Information Security, Nationale-Nederlanden C&C; **Frans Szabó,** IT Lead, Rabobank

Stepping back from the day-to-day necessities, what challenges in firms' digital environments cause greatest problems for the information security programme? How does the information security function mitigate and alleviate the burden on their IT and business colleagues to solve them? This panel will look at the challenges posed by:

- Asset inventories (devices, applications, identity, network, data)
- Overall technology landscape complexity
- 'Digital' transformations of the business/products
- Testing and measuring the effectiveness of the cybersecurity control environment
- Incident response and problem management
- Ensuring the same coverage/visibility over cloud environments as on-prem
- Managing supply chain risk in a world less tolerant to long delays around supplier assurance (post covid)
- Web 3.0 and the next generation of the internet: securing new technologies and services that are inherently decentralised?

17:30 Conference close

Education seminars

Throughout the day a series of education seminars will take place as part of the main agenda. Delegates will be able to choose to attend any of the seminars, all of which will provide vendor-neutral, hands-on advice. Seminars within each session run concurrently.

Session 1: 10:20–11:00

Synack

SESSION 1
10:20–11:00

Using security testing to drive change for the better

Paul Mote, Senior Director, Solutions Architects, Synack

Security testing is more than a list of open vulnerabilities. It's a practice that leverages live offensive security techniques to find where true risk lies. Most organisations have very different levels of effectiveness when it comes to proactive risk identification and mitigation. Some companies might be great at fixing problems but are only average at shipping secure code the first time or with every update.

In this session, you will learn:

- How to keep pace with digital transformation through continuous security testing
- How to effectively fit security testing into your strategy
- How great organisations have used security testing to make lasting, positive change – one security test at a time

Vectra AI

SESSION 1
10:20–11:00

Erasing surface, identity, complexity and unknowns

Christian Borst, EMEA CTO, Vectra AI

Threat intelligence has been a critical component to knowing threat types, methods, and profiles. As enterprises shift to cloud, security and risk leaders are facing an onslaught of unknowns. Unknown compromises, attack progressions and prioritisation challenges require more reliable, accurate, and timely insights into advanced attacks. In this session, learn how security operations need to shift their focus to be more proactive in identifying and stopping sophisticated ATP's.

During our presentation, we will cover:

- What is threat intelligence and how it benefits your organisation and SOC team
- How to analyse the data to understand the threat landscape, anticipate attackers' next moves and take prompt action to stop attacks
- The importance of ongoing intelligence to prevent emerging risks and threats

Session 2: 12:50–13:30

Menlo Security

SESSION 2
12:50–13:30

The next class of browser-based attacks

Tom McVey, Solution Architect, Menlo Security

There are two distinct characteristics that all threat actors tend to share. First, they focus on avoiding detection by any means. Second, while some go after specific targets, many opt to aim their tactics at the vectors that will reap the greatest rewards. After all, a big pond with many fish increases everyone's chances of success.

Between July and December 2021, there was a 224% increase in highly evasive adaptive threats (HEAT) attacks – a class of cyber-threats targeting web browsers as the attack vector. While malware once had to be downloaded to pose a real risk, now, it's a dynamically generated threat toolkit built in the web where employees are productive.

In this session, you will:

- Discover the anatomy of recent browser-based attacks
- Learn why network security today is broken
- Experience a live demo that enables you to discover the technology approach proven to eliminate these threats

OPSWAT

SESSION 2
12:50–13:30

File upload protection: A critical gap in web app security

Rachid Mekdoud, Sales Engineer, OPSWAT

Digital transformation is a must for today's organisations, resulting in a migration from paper-based to digital documents.

Millions of documents are now being shared among collaborators weekly and monthly – uploaded to either a web portal, customer portal (insurance or mortgage applications) or support portal (attaching files to your support ticket).

At the same time, an enormous amount of effort is invested into building high-availability, fault-tolerant systems and securing them.

However, file upload remains a major attack vector and far too often is not covered by traditional web application defences.

In this seminar, Rachid Mekdoud, Sales Engineer at OPSWAT will cover three types of risks to web applications and how to apply a Zero Trust model to both users and the files they upload and the devices from which these uploaded files originate.

Risks from:

- Threat actors who submit malicious files to gain access to the organisation's IT infrastructure
- User who submits sensitive data in violation of an application's terms of service
- Inadvertent hosting and distributing malicious files uploaded by a threat actor

Session 3: 15:30–16:10

Abnormal Security

SESSION 3
15:30–16:10

Key considerations for choosing the right cloud email security platform

David Lomax, Systems Engineer, Abnormal Security

Email is both a necessary communication medium, and the most vulnerable area for an attack. Year after year, adversaries find success in abusing email to gain a foothold into an organisation – deploying malware, leaking valuable data, or stealing millions of dollars.

Unfortunately, email threats are only growing in number. Business email compromise accounts for 35% of all losses to cybercrime, and the Verizon Data Breach Investigations Report holds that phishing remains the top entry point for breaches – a position it has held for years.

Does that mean email is doomed, and we should give up? Quite the opposite. But the shift to cloud email requires one major thing: a shift to cloud email security.

Attend the Abnormal Security session for answers to your most pressing questions, including:

- What are modern email threats, and how are they different from legacy attacks?
- Which email threats are most concerning, and how can we defend against them in the cloud environment?
- Which technical capabilities are required when protecting cloud email?
- How can cloud email security platforms detect the most dangerous attacks?

ReliaQuest

SESSION 3
15:30–16:10

The future of security operations: Threat intelligence, automation, and data-stitching

Rasham Rastegarpour, Sales Engineer, ReliaQuest

Enterprises are working to get the ROI out of their existing tools as well as accelerate their ability to detect, investigate, and respond. In attempting to accomplish these two goals, enterprises are considering a single data lake that stores their security data. There are several challenges with this approach from additional costs of data egress from cloud providers to the simple fact that the enterprise data will never be in one place. At ReliaQuest, we take a different approach using data-stitching and distributed investigations. In this talk, we will discuss the pros and cons of centralising security data and how an approach of data stitching solves those challenges.

- Security operations today
- Security's 'big data' problem
- Data lakes vs Data stitching
- Security operations platform
- Data stitching in action □

Speakers and panellists

e-Crime & Cybersecurity Benelux is delighted to welcome delegates, speakers and panellists. The event has attracted a large number of key names and decision-makers across industry.

Marc Berns

Chief Information Security Officer, Allianz Benelux

Marc is the CISO for Allianz Benelux, an insurance company based in Brussels, Rotterdam and Luxemburg, part of the Allianz SE group of companies. Throughout his career, he has worked in heavily regulated industries from investment banking to insurance. His focus is implementing risk-based governance over information security in IT operations outsourced to third parties.

Christian Borst

EMEA CTO, Vectra AI

Christian Borst, EMEA CTO at Vectra AI has more than 15 years of experience in IT and cybersecurity. Before joining Vectra AI in 2022, he built and executed the global cybersecurity strategy for Richemont – a leading luxury goods group. As a former consultant and current Advisory Board & Board Member, he is actively engaged in the cybersecurity community across different countries & industries.

Robert Elferink

Sr. Manager, Sales Engineering Benelux & Nordics, CrowdStrike

Robert Elferink is Sr. Manager, Sales Engineering Benelux & Nordics at CrowdStrike. During his 20 years of experience, he held various technical leadership roles at companies such as Dell, NetApp and Nutanix. At CrowdStrike, he leads the sales engineering team in the Benelux and Nordics. Robert and his team are known as renowned trusted advisors in the region and inform their clients about the latest developments in the world of cybersecurity, where a lot changes on a daily basis.

Matt Ellison

Director of Sales Engineering EMEA and APAC, Corelight

Matt Ellison is the Director of Sales Engineering for EMEA and APAC with over 20 years' experience in providing technology solutions for companies around the globe. He has specialised in cybersecurity for over 15 years across endpoint, network and user technologies and has led teams in product management, product marketing and technical sales. Matt's experience covers roles with vendors such as Symantec, LogRhythm and BAE Systems. Outside of vendors, he has had roles with technology channel partners and managed security services as well as end customers. This experience has allowed him to work with numerous organisations across EMEA and APAC, in many different markets, helping them understand how best to address their unique challenges.

Julian Kanitz

Lead Sales Engineer, Recorded Future

Julian Kanitz is Lead Sales Engineer at Recorded Future supporting the DACH region. He holds a Master of Science in Industrial Engineering and served 12 years in the German Military. He has been evangelising threat intelligence for various enterprise security programmes for the past three years.

Raymond Kleijmeer

Senior Officer Cyber Resilience, De Nederlandsche Bank

Raymond Kleijmeer is working at De Nederlandsche Bank as Senior Officer for Cyber Resilience. De Nederlandsche Bank (DNB) is the central bank and financial prudential supervisor of the Netherlands. DNB seeks to safeguard financial stability and enhance the cyber-resiliency of financial institutions and the financial system as a whole. Raymond has been involved in international working groups hosted by the Bank for International Settlements (BIS) publishing among others, the CPMI-IOSCO guidance on cyber-resilience for financial market infrastructures in June 2016 and the Financial Stability Board Cyber Incident Response and Recovery toolkit published in 2020. At a national level, he worked on the initiation and implementation of the Threat Intelligence Based Ethical Red teaming framework in the Netherlands from 2015 until 2019, when he was seconded to the BIS Financial Stability Institute to

publish an FSI Insight on international red team testing frameworks. At the BIS Cyber Resilience Coordination Centre, Raymond was seconded from 2020–2022 to establish a programme for central banks to perform cyber-resilience assessments with methodology developed by Carnegie Mellon University. This CRA methodology is performed as a self-assessment on a critical business service to help identify areas for improvements. It enables organisations to use the outcomes to benchmark themselves with relevant peers.

Dr. Lydia Kostopoulos

Senior Vice President of Emerging Tech Insights, KnowBe4

Dr. Lydia Kostopoulos is Senior Vice President of Emerging Tech Insights at KnowBe4. She is a multi-disciplinary professional whose expertise lies at the intersection of strategy, security and emerging technologies. Dr. Kostopoulos brings a systems thinking approach to her work, examining technology opportunities and risks in the context of global macro trends, geopolitics, international economics, climatic factors and demographic change. She continues to work with US Special Operations, speaks at NATO events and has worked with the United Nations and the IEEE Standards Body. In the realm of technology ethics, she is an advisor for the Data Ethics Consortium for Security and for Ethical Intelligence Associates. Passionate about spreading awareness on emerging technologies, Dr. Kostopoulos makes art about technology and has a multilingual, reflective game on emerging technologies called Sapien 2.0, which explores the human and machine relationship.

Hanan Levin

VP Sales EMEA, Hunters

Hanan Levin has over 20 years of experience in creating, delivering and selling innovative enterprise cyber-solutions. Prior to his role as VP Sales EMEA at Hunters, Hanan served as VP Products at various companies like ForeScout and Illusive Networks. Earlier in his career, Hanan was part of the initial engineering team at Check Point developing Firewall-1, VPN-1 and Provider-1. Hanan served as a Major in the Israeli Air Force.

David Lomax

Systems Engineer, Abnormal Security

David Lomax is an experienced Systems Engineer with over 18 years' experience in the cybersecurity landscape, working across email, network, data and applications, he is also seasoned in cloud-based threat detection and response. His knowledge extends to multiple industry sectors including banking, manufacturing, legal, pharma and critical national infrastructure.

Tom McVey

Solutions Architect, Menlo Security

Tom McVey is an EMEA Solutions Architect at Menlo Security, where he works to achieve his customer's technical requirements and architects web and email isolation deployments for organisations across many different industries. Coming from a background in UEBA & insider threat, he provides expert cybersecurity advice and strategic guidance to his clientele. Prior to Menlo, he always had a passion for cybersecurity and IT. In his spare time, Tom likes to play music and watch Formula 1 cars go around a track very quickly.

Rachid Mekdoud

Senior Sales Engineer, OPSWAT

Rachid Mekdoud is a Senior Sales Engineer at OPSWAT. With more than 20 years of experience with various international integrators and software editors, he is at the service of several companies to help them with their cybersecurity projects. He trains partners to bring the OPSWAT vision and promotes the programme 'OPSWAT Academy' which is free, open to all and allow all to learn about cybersecurity from scratch. He has significant experience in various areas of IT allowing him to specialise in the Critical Infrastructure Protection (CIP). It allows OPSWAT's customers to benefit from the best cybersecurity solutions. He is very interested in the impact and effectiveness of AI (Artificial Intelligence) applied to cybersecurity in the industrial field, OT (Operation Technology).

Paul Mote

Senior Director, Solutions Architects, Synack

Paul Mote has extensive experience in the realm of cybersecurity. His career spans over a decade where he has held roles ranging from intrusion analyst all the way to his current role of World Wide Sr. Director of Solutions Architects at Synack. Paul knows that organisations must get out of the 'whack-a-vuln' game and supports clients across every vertical as they transform their security testing programmes.

David Palmer

Business Lead for Blockchain Technology, Vodafone

David Palmer is a digital visionary and global platform innovator. He is the Vodafone Business Lead for Blockchain Technology, and he has been key to exploring the application of blockchain to telecoms and wider business. David is an expert on the convergence of digital technologies and new business models, and he is currently exploring the opportunities associated with IoT, Blockchain, DeFi and Metaverse.

Arash Rahmani

Head of Information Security, Nationale-Nederlanden C&C

Arash Rahmani is a Trusted Advisor Information Security where he helps organisation leaders align their business and information security strategy and mitigate their information security risks. He is currently the Head of Information Security C&C at Nationale-Nederlanden. He also held positions in IT & information security at Royal Schipol Group and Aegon, amongst others. Arash believes that information security adds value to the business, can help drive strategy execution and should be business-driven, not just IT-driven. He focuses on technology, people, processes, and culture to achieve organisational goals. Arash has a track record in increasing the digital resilience of large organisations and managing multidisciplinary teams.

Rasham Rastegarpour

Sales Engineer, ReliaQuest

Rasham Rastegarpour has over 21 years of experience in IT, which was mostly focused on enhancing the security stance of many organisations. Since the start of his career, Rasham has held multiple positions and therefore, he has been and participated in many different disciplines, which makes him a jack of all trades and master of a few. With his education and experience ranging from operational to various training, consulting and managerial roles, he is able to speak the language of multiple stakeholders within security teams. His wealth of in-depth technical and organisational knowledge within multiple subject matters across many companies, makes him a valuable asset to any type of organisation at any level of security maturity. Currently active as Sales Engineer for ReliaQuest, Rasham is solving complex challenges across IT, OT and Cloud environment by optimising security ROI, increasing visibility, measuring team performance whilst improving the overall security posture for all types of organisations in EMEA.

Frans Szabó

Lead IT for Operational Technology, Rabobank

Frans Szabó has more than 33 years of experience in the banking industry, working in – amongst others – the fields of core IT, service and delivery management, continuity management and marketing and customer support. In more recent previous positions, Frans protected the bank's customers against fraud through cybercrime and later headed the Red Team of Rabobank. In his current role, Frans is responsible for managing all operational technology related to topics like building management, access control, physical safety and security etc. Further, Frans with his team support several DevOps teams in achieving their goals of delivering an optimal (physical) employee journey at Rabobank. Security and compliance are key drivers in both areas of work.

Guus Van Delft

Bug Bounty & Crowdsourced Security Account Executive, Intigriti

Guus is a happy family man with a healthy passion for security. He is leading the Intigriti commercial team in the Netherlands, and since 2019 he has advised companies on their crowdsourced security approach, Bug Bounty, and working with ethical hackers. The world of security is evolving rapidly, and so he loves to share his knowledge in a pragmatic approach, inspiring organisations to embrace a more agile way of working that supports continuous security testing. After all, crowdsourced security is a must-have.

Paul van den Berg

Strategic Relations & Partnerships, NCSC-NL

Experienced, innovative and results-oriented business leader with a convincing track record in IT strategy, governance, project management and consulting; active in both Fortune 500 multinationals as well as in the public sector, in the Netherlands and abroad. Paul is currently focusing on cybersecurity and privacy compliance requirements for boards.

Patrick Van den Branden

Group IT Security Officer, Euroports Group

Patrick joined Euroports in 2020 as Group Information Security Officer. He has been in the IT trenches for

more than 30 years as a programmer, a system admin, as head of IT infrastructure and an IT manager. As the GISO of Euroports, his worldwide responsibilities cover all aspects of cybersecurity: assisting the infrastructure team in deploying secure infrastructure, evaluating new applications (including SAAS) on security, implementing and guarding an adequate governance and last but not least user awareness.

Dimitri van Zantvliet

Chief Information Security Officer, Nederlandse Spoorwegen

Dimitri joined NS (Dutch Railways) in 2021 as their Chief Information Security Officer. He has been in the field for three decades as CIO, CTO and CISO. His responsibilities span cybersecurity matters on governance, mobilitychains, IT-, IoT- and OT strategy and European Railway Cyber Projects. Next to that he is co-chair to the Dutch and European Rail ISAC.

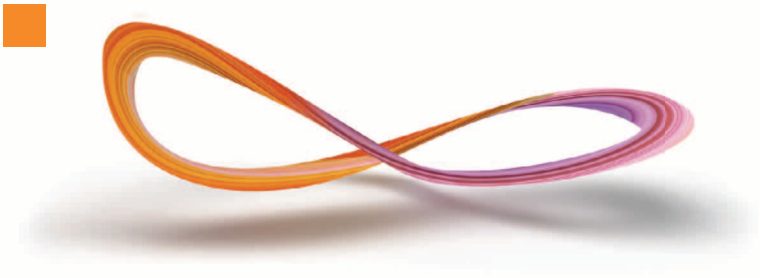
Dimitri holds a master's degree from the University of Derby and CISSP, CRISC, CISA, CISM, CDPSE, CIPP/E, CIPM and FIP cybercertificates.

Rick Verhagen

Cybersecurity Enterprise Account Executive, Darktrace

Rick Verhagen is a Cybersecurity Enterprise Account Executive at Darktrace, a global leader in cybersecurity AI. At Darktrace, Rick works with leading organisations in a range of industries to deploy and operationalise cutting-edge technologies. During Rick's tenure at Darktrace, the company has grown to over 7,500 customers and has been the recipient of numerous achievements, including being named one of TIME magazine's 'Most Influential Companies' for 2021. Rick holds a bachelor's degree from deMontfort University in Leicester and a master's degree from Maastricht University and is based in Darktrace's Amsterdam office. □

CYBER SECURITY ISN'T A PRODUCT. IT'S A STATE OF BEING.



We believe that cyber security should cover you from all angles, all the time. It's why Darktrace detects threats, responds to them, and helps proactively prevent them. And it's all powered by our industry-first Cyber AI Loop - which uses Self-Learning AI to constantly optimize your state of security.

DARKTRACE

Evolving threats call for evolved thinking

Darktrace.com

DARKTRACE

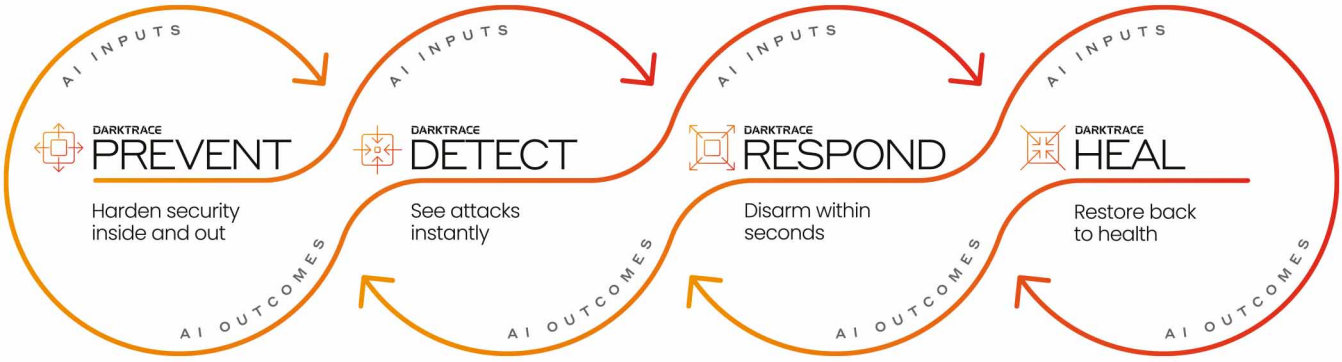
Why Darktrace?

AT A GLANCE:

- Reduce risk by prioritizing vulnerabilities and hardening systems
- Gain instant visibility of previously unknown and unpredictable attacks
- Minimize disruption with a targeted, autonomous response to cyber-attacks
- Augment and empower security teams with always-on, AI-driven capabilities

The Only Comprehensive, Always-On, End to End Cyber Security

Cyber AI Loop™



Self-Learning AI empowers a complete, always-on solution with autonomous feedback continuously improving the state of security

Darktrace delivers the first-ever Cyber AI Loop: an interconnected set of cyber security solutions that continuously and autonomously hardens your security.

The Cyber AI Loop comprises four AI-powered product families – Darktrace PREVENT™, Darktrace DETECT™, Darktrace RESPOND™, and Darktrace HEAL™ – that work across your entire organization, including internal and external data, simultaneously. With each technology augmenting and feeding information into the others, your cyber resilience is systematically improved.

Each component of the Cyber AI Loop is powered by Self-Learning AI: proprietary Darktrace technology that learns *you*. By understanding your bespoke organization, your users and devices and how they interact, it can build an evolving sense of what's normal to identify what's not. This enables Darktrace to shine a light on previously unknown and unpredictable threats.

Darktrace PREVENT learns your organization from the inside and outside, prioritizing risks and hardening defenses.

AI brought to your data, wherever it resides

Darktrace technology works for organizations of all sizes and can be brought to any environment, from cloud and email systems to endpoints, zero trust technologies, and IT/OT networks. With one-click integrations, the platform can instantly ingest new forms of telemetry, share bespoke AI insights across established workflows, and interoperate with a wide range of technologies.

AI Research Centre – Leading AI Innovation

Darktrace's research-led solutions are rooted in innovation. The Darktrace AI Research Centre™, with more than 100 patent applications granted or pending, includes teams of mathematicians and other experts investigating how AI can be applied to real-world problems. The center has produced numerous breakthroughs, which now form the AI capabilities comprising our products contained in the Cyber AI Loop.

DARKTRACE DETECT + RESPOND

Autonomous Response: Disarm Attacks in Seconds

Darktrace DETECT + RESPOND uses its deep understanding of your organization to tailor actions to individual threats. This means malicious activity is neutralized without affecting normal business operations.

This is in contrast to automated solutions that rely on playbooks to respond to attacks, resulting in imprecise, heavy-handed actions. Most successful attacks today are novel in some way – meaning configurations will not be in place to defend against them.

CYBER AI ANALYST

Uplift and Augment Your Security Team with AI Investigations

Darktrace's Cyber AI Analyst was built to optimize threat investigation by continuously examining every security threat that arises. It illuminates the highest priority threats at any one time and rapidly synthesizes all of the context around an attack into a natural language report.

The result is that time-to-meaning and time-to-response are dramatically reduced – allowing your team the time to use their expertise where it really matters.

DARKTRACE PREVENT

Hardening Security and Reducing Risk

Darktrace PREVENT empowers CISOs and security teams to shift from being reactive to proactive, getting ahead of the attacker and stopping attacks before they happen. It enables you to prioritize threats and vulnerabilities, optimize and harden defenses, and reduce the overall cyber risk to your organization.

About Darktrace

Darktrace (DARK.L), a global leader in cyber security AI, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. We protect more than 7,400 customers from the world's most complex threats, including ransomware, cloud, and SaaS attacks. Darktrace is delivering the first-ever Cyber AI Loop, fueling a continuous security capability that can autonomously spot and respond to novel in-progress threats within seconds. Darktrace was named one of TIME magazine's "Most Influential Companies" in 2021.

To learn more, visit **darktrace.com**

Scan to LEARN MORE

See the Abnormal solution to the email security problem

Protect your organisation from the attacks that matter most with Abnormal Integrated Cloud Email Security.

Lane Billings reports

Whether it's a sales outreach message, a promotional newsletter, or simply outright spam, sifting through unwanted mail takes time and energy away from more important tasks.

In many cases, graymail – an email message from a legitimate sender that is safe to engage with but promotional in nature – is the largest culprit. This category of messages includes emails like event invitations, vendor cold calls, external surveys, feedback request emails, and other types of promotional communications. And unlike spam, graymail generally provides some level of value – at least when it is sent to the right person.

That being said, vendor cold calls can target hundreds of people within your organisation, and promotional newsletters are often sent to everyone. As the volume of graymail steadily increases, effective graymail management will become even more critical. And ignoring the issue will only lead to overflowing employee inboxes, wasted time, and lower productivity.

The challenge of stopping graymail

Graymail takes many shapes and forms, and every employee within an organisation has a slightly different response to it. One executive may want to field cold emails from potential vendors, while another opts to send these messages straight to the trash.

The breadth of individual preferences makes filtering out graymail with a simple global policy problematic. It's especially unpopular with IT and messaging teams because they know users will inevitably complain when emails they want to receive are rerouted and vice versa. After all, no one wants to be responsible for the CEO not receiving his favourite newsletter each morning.

The existing approaches for managing graymail mean IT leaders have to decide between two unpleasant scenarios. The first option is to push the responsibility of sorting graymail downstream to employees. Taking this route requires the IT team to:

- Process graymail through end-user quarantine web portals in a separate UI, which often haven't been updated or improved by SEG providers in the last decade.
- Parse through daily spam digests that summarise all external emails, wasting exorbitant amounts of time to find needles in the haystack.
- Manually build and maintain their own safelists and blocklists to control what is delivered to end-user inboxes.

The other option is to have the IT team set bulk email thresholds and attempt to detect the most glaring examples of graymail that are impacting users. In addition to being inefficient and less effective, this approach also requires IT to constantly adjust the filtering in response to an endless cycle of one-off employee requests.

Neither approach is practical or scalable, and both create mountains of support tickets and headaches for IT. To effectively control graymail, enterprises must implement a solution that employs advanced detection techniques and utilises innovative technology.

Limiting time-wasting email without rules or policies

The ideal approach to limiting time-wasting email requires no rules or policies – from end users or IT teams. It involves implementing a solution that understands business context by utilising natural language processing (NLP) derived from a strong API integration with Microsoft 365.

Microsoft can provide tens of thousands of signals about relationships, behaviour, and preferences. Instead of relying on basic filtering rules and policies, enterprises can use an innovative solution that utilises these valuable data points to build an organisation-specific behavioural profile, which helps in the fight against graymail.

The solution should also leverage behavioural AI that adapts the model based on user actions and supports a completely hands-off approach. Organisations that attempt to filter graymail using static rules and

Graymail takes many shapes and forms, and every employee within an organisation has a slightly different response to it.

Using technology specifically designed to manage graymail provides IT leaders with visibility into which employees are the most frequently targeted, top senders, and the time-savings from limiting the volume of unwanted mail users receive.

policies are unsuccessful because this system doesn't address the variance in content across these messages. It also can't be scaled to support thousands of users' specific preferences.

Behavioural AI synthesises tens of thousands of signals to precisely categorise all emails across the full spectrum of email content – from advanced attacks to unwanted email. And with this accurate, adaptive graymail detection, there's no longer a need for fine-grained policies or continuous updates to detection rules.

Rather, the detection engine can assess each message and take remediation actions based on an ever-evolving, always-improving, organisation-specific definition of graymail. The result is the highest level of graymail detection efficacy with the lowest administrative effort.

The benefits of adopting a modern approach

With this technology, IT leaders can achieve the following:

1. **Refine graymail protection for individual employees via adaptive personalisation**
User actions like opening specific emails and moving messages from the inbox to other folders provide valuable inputs that a behavioural AI/ML model can use to personalise, adapt, and improve protection over time. Allow and block lists can also be automatically updated based on observed user preferences.

2. **Eliminate the need for end-user quarantines and portals**
Messages are sorted into a promotions folder, not an end-user quarantine portal. Plus, direct integration between the cloud email security provider and the email infrastructure provider allows for a native end-user experience and frees end users to use the email client of their choice.

3. **Demonstrate instant ROI, with unique insights into email's impact on productivity**
Using technology specifically designed to manage graymail provides IT leaders with visibility into which employees are the most frequently targeted, top senders, and the time-savings from limiting the volume of unwanted mail users receive.

The solution to graymail is Abnormal

Only Abnormal Security combines an API-based integration model with advanced, behavioural AI-based detection to address and mitigate risks and inefficiencies across the full spectrum of email.

Our Email Productivity add-on layers onto the core Inbound Email Protection product and applies the same behavioural AI, natural language processing (NLP), and natural language understanding (NLU) models that help stop the most sophisticated email-based attacks to limit graymail. Make your workforce more productive by putting time-wasting email on autopilot with Email Productivity from Abnormal.

To see how Inbound Email Protection and Email Productivity can benefit your organisation, request a personalised demo today. □

Lane Billings is Group Product Marketing Director at Abnormal.

For more information, please visit **abnormalsecurity.com**

Abnormal

Prevent the Attacks That Matter Most

Abnormal protects the modern workforce from never-before-seen email attacks, including:

- Business Email Compromise
- Ransomware & Malware
- Account Takeover
- Executive Impersonation
- Supply Chain Compromise
- Credential Phishing

Visit our booth today to learn more

→ Book a Demo
abnormalsecurity.com/demo

Abnormal

cybermanchester.events/

Testing early and often can reduce flaws in app development

Security needs to be much more than an afterthought.

Kirsten Gibson reports

Security is too often an afterthought in the software development process. It's easy to understand why: Application and software developers are tasked with getting rid of bugs and adding in new features in updates that must meet a grueling release schedule.

Asking to include security testing before an update is deployed can bring up problems needing to be fixed. In an already tight timeline, that creates tension between developers and the security team.

If you're using traditional pentesting methods, the delays and disruption are too great to burden the development team, who are likely working a continuous integration and continuous delivery process (CI/CD). Or if you're using an automatic scanner to detect potential vulnerabilities, you're receiving a long list of low-level vulnerabilities that obscures the most critical issues to address first.

Instead, continuous pentesting, or even scanning for a particular CVE, can harmonise development and security teams. And it's increasingly important. A shocking 85% of commercial apps contain at least one critical vulnerability, according to a 2021 report[1], while 100% use open-source software, such as the now infamous Log4j. That's not to knock on open-source software, but rather to say that a critical vulnerability can pop up at any time and it's more likely to happen than not.

If a critical vulnerability is found – or worse, exploited – the potential fines or settlement from a data breach could be astronomical. In the latest data breach settlement, T-Mobile agreed to pay $350 million[2] to customers in a class action lawsuit and invest additional $150 million in their data security operations.

This is why many companies are hiring for development security operations (DevSecOps). The people in these roles work in concert with the development team to build a secure software development process[3] into the existing deployment schedule. But with an estimated 3.5 million cybersecurity jobs globally that are likely went unfilled in 2021[4], it might be hard to find the right candidate.

If you want to improve the security of your software and app development, here are some tips from Synack customers:

- *Highlight only the most critical vulnerabilities to the dev team.* The development team has time only to address what's most important. Sorting through an endless list of vulnerabilities that might never be exploited won't work. Synack delivers vulnerabilities that matter by incentivising our researchers to focus on finding severe vulnerabilities.
- *Don't shame, celebrate.* Mistakes are inevitable. Instead of shaming or blaming the development team for a security flaw, cheer on the wins. Finding and fixing vulnerabilities before an update is released is a cause for celebration. Working together to protect the company's reputation and your customers' data is the shared goal.
- *Embrace the pace.* CI/CD isn't going away and the key to deploying more secure apps and software is to find ways to work with developers. When vulnerabilities are found to be fixed, document the process for next time. And if there's enough time, try testing for specific, relevant CVEs. Synack Red Team (SRT) members document their path to finding and exploiting vulnerabilities and can verify patches were implemented successfully. SRT security researchers can also test as narrow or broad a scope as you'd like with Synack's testing offerings and catalogue of specific checks, such as CVE and zero day checks.

Security is a vital component to all companies' IT infrastructure, but it can't stand in the way of the business. For more information about how Synack can help you integrate security checkpoints in your dev process, request a demo. □

1 https://venturebeat.com/business/85-of-commercial-software-apps-have-critical-vulnerabilities-study-finds/#:~:text=85%25%20of%20commercial%20apps%20have,'%20vulnerabilities%2C%20study%20finds%20%7C%20VentureBeat

2 https://apnews.com/article/technology-lawsuits-class-action-8f03e9f76fa75f474f1a2584ce3a55f0

3 https://niccs.cisa.gov/education-training/catalog/security-innovation/secure-software-development

4 https://cybersecurityventures.com/jobs/

Kirsten Gibson is Senior Content Marketing Manager at Synack.

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

Synack

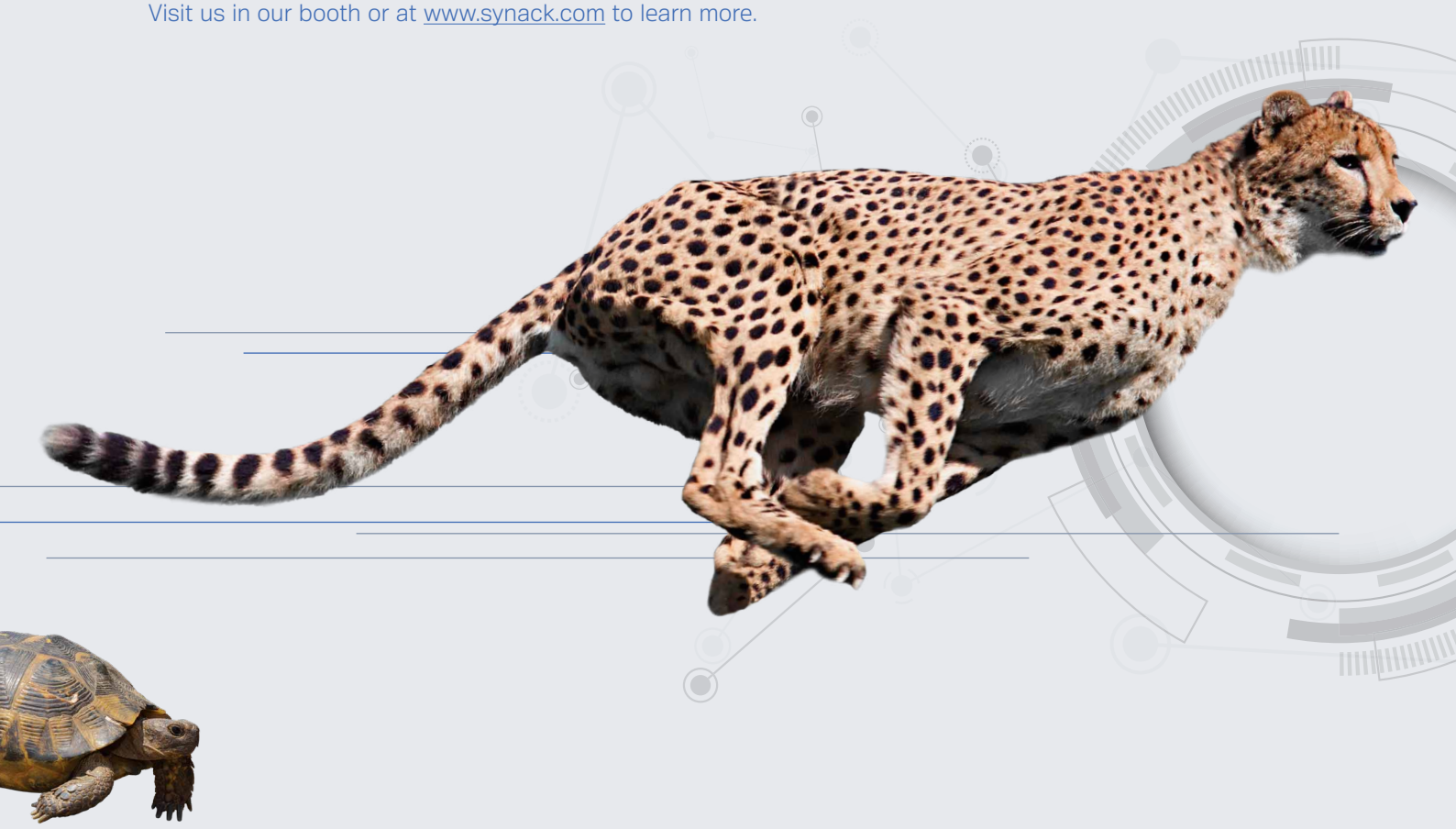
THE PREMIER SECURITY TESTING PLATFORM

A BETTER WAY TO PENTEST

Traditional pentesting is like a turtle chasing a cheetah

Find the vulnerabilities that matter with continuous and on-demand security testing.

Visit us in our booth or at www.synack.com to learn more.



Erase the unknowns, transform the SOC

Today, the unknown threat poses the single biggest risk to organisations as threat coverage is now required across the extended enterprise – public cloud, SaaS, identity and network.

Vectra reports

The unknown threat facing SOC teams today

Every SOC team knows the threat landscape is different than it was just a couple of years ago. The cloud means more exposure, which means more coverage is required. Attackers are more advanced, which means we need more than signatures and anomalies to understand their behaviour. And the more tools that get deployed mean more alerts that need more tuning. The common theme – 'more'. More complexity, more rules to maintain and more work and burnout.

Yet, if asked these questions:

- Where are we exposed right now?
- Where are we compromised right now?

It wouldn't be a stretch to say that a lot of organisations wouldn't have a clear answer. In fact, in a recent study, 72% of security practitioners 'think' they may have been breached, but don't know it. Not knowing where you're compromised or where exposure exists means you're at risk of unknown threats causing all types of problems for your organisation and you don't even know it's there. Today, the unknown threat poses the single biggest risk to organisations as threat coverage is now required across the extended enterprise – public cloud, SaaS, identity and network.

Knowing why unknowns exist

- *Attack surface:* no longer containable to the network data centre
- *Attacker methods:* always changing and can easily bypass prevention controls
- *More noise:* analysts are overburdened as they attempt to focus on the malicious

These three dynamics are why unknowns exist today, but it's important for security teams to know specifically for their organisations, where they have exposure and where they're compromised. What's the difference? The best way to think about it is that exposure is 'where is there a door open?' While compromise is 'where has there been a door open, through which the attacker has already come in?'

To start understanding how to answer these questions, we must recognise that the answers aren't going to come by doing things the way they've always been done. Hybrid and multi-cloud environments are an entirely new challenge and need to be treated as such. This is where security and risk organisations should take a close look at three critical areas to get ahead and stay ahead of modern attacks.

- *Attack coverage:* attacker methods across your entire attack surface need to be exposed. This comes from monitoring for attacker TTPs throughout the entire cyber kill chain across all your vectors – network, SaaS, cloud, identify and endpoint.
- *Signal clarity:* rich signal to automate manual tasks related to threat detection, triage, and prioritisation because analysts can't be expected to do these tasks on a manual basis.
- *Intelligent control:* having targeted response actions that don't require you to jump from tool to tool and can arm your human intelligence to better respond to unknown threats.

The burden of the unknown falls squarely on the shoulders of SOC teams, but if you have detection methods in place that know how attackers think and exactly what they'll do next – your organisation can stay ahead of them. For example, if you understand how an attacker behaves across the kill chain – how they got in, how they will do the recon and discovery work – you'll be able to stop them because you'll know for certain that an attack is in place.

In our case, we empower our customers to do this with Security AI. When customers deploy the Vectra Threat Detection and Response platform, harnessing AI-driven Attack Signal Intelligence – defenders can think like an attacker by knowing their TTPs, and they know what threats are malicious so it's easy to focus on the more urgent threats. □

To learn more about Vectra Attack Signal Intelligence, please visit
www.vectra.ai/products/attack-signal-intelligence

For more information, please visit
www.vectra.ai

VECTRA®

VECTRA®

THREAT DETECTION & RESPONSE

for hybrid and multi-cloud enterprises

Erase the Unknown

Have coverage.
Get attack visibility across your expanding attack surface.

Get clarity.
Harness Attack Signal Intelligence™ and reduce noise more than 80%.

Seize control.
See and stop attacks with less tools, less rules, less work.

www.vectra.ai

How tool hopping holds back security workflows

Security engineers now hop between visibility tools to try to make sense of a jumbled, inconsistent picture of the network.

ReliaQuest reports

Visibility tools are a crucial part of network security. They help spot the risks, hunt the threats and provide the data needed to improve the overall security of the network. So it's understandable why so many organisations have turned to these tools to better defend themselves. However, they've acquired more tools than they can use effectively. Security engineers now hop between visibility tools to try to make sense of a jumbled, inconsistent picture of the network.

Expanding attack surfaces are making security harder, and organisations' ability to properly police them is not growing fast enough. The 2021 ISC^2 Cybersecurity workforce study found that the current talent pool would need to grow by 65% in order to keep up with ever-growing demand for security specialists.

Tool sprawl

In short, there are too many tools, overseeing too much, with not enough staff to effectively man them. A 2021 study from ReliaQuest and Ponemon found that just under half of companies had one staff member responsible for between 4 and 10 visibility tools.

Adding to the chaos, organisations often find themselves with yet more tools in the wake of mergers and acquisitions. The visibility tools of the acquired company become one with the acquiring company – leading to a disorganised, uneven security stance.

These tools are complex, and in more than one way. Some use sophisticated tools like AI, and some may have been custom-built and include quirks that require specialist training to sort out.

On top of all that, these tools often don't integrate use common metrics. This causes engineers to hop between tools and pull together disparate data points, leaving enterprise security on the back foot.

Tool hopping and the security operations workflow.

When security engineers are forced to use manual processes to collect and understand data, the whole security operations workflow – and the resilience of the enterprise – becomes cumulatively weakened.

Preparation

When engineers have to tool hop, preparation gets disrupted. Tools become ineffectively utilised and poorly optimised, making it difficult to gauge the effectiveness of security controls. This limits visibility and the availability of contextual intelligence.

Detection

While visibility tools are critical to detection, they're also machines and they need guidance to do their job. Without the proper threat data and context – that preparation would have otherwise provided – they can't detect known or unknown threats.

Investigation

As a result, engineers have to collect data manually, resulting in false positives and even more difficulty seeing the context that is crucial for investigations.

Respond

When the time comes to actually respond to a threat – engineers' focus is diluted. Between the multiple tools they have to manage and the repetitive, manual and inconsistent processes that they bring, responding to threats becomes sluggish and ineffective.

Measure

With too many tools, security teams find it difficult to use metrics that give them a unified view of their own environment, and their lack of visibility blinds them to where and how they're vulnerable. They're then unable to determine their current security status and what to do next.

The true cost of tool-hopping

When it comes to visibility tools, many enterprises can't see the forest for the trees. It's one thing to have the technology to enable visibility, it's another to be able to use it effectively. As it stands, many organisations don't have enough skilled staff to manage their visibility tools which, ironically, results in inconsistent and ineffective visibility.

When engineers are burdened by tools and visibility is clouded, the problems might start in security, but they ultimately end on the bottom line. □

RELIAQUEST®

Make Security Possible

Force multiply your security operations team with our Open XDR platform and proven security expertise.

Why ReliaQuest?

Increase Visibility

Decrease Complexity

Reduce Risk

GreyMatter Cloud Native Platform
Unify on-prem, hybrid, and cloud security workflows to reduce noise and speed response.

Integrate Your Current Tech Stack
Unified visibility for actionable security insights and ROI on your tools.

Security Expertise: Anytime, Anywhere
Proactive threat research, incident response, threat hunting, and optimization.

Greymatter Platform Capabilities

Operationalize your security investments and ensure teams focus on the right problems

- Reduce Complexity
- Detection & Response
- Extend Your Team
- Security Metrics
- Security Automation
- Threat Hunting

Visit ReliaQuest.com

Preventing highly evasive threats that lead to ransomware

Ransomware continues to torment cybersecurity leaders around the world.

Menlo Security reports

More than 70% of organisations were hit by ransomware attacks in 2021, according to the 2022 CyberEdge Cyberthreat Defense Report – a staggering increase from 55% in 2018. These attacks shut down businesses, disrupt public infrastructure, and cost organisations billions of dollars in ransom payments.

Attackers know that ransomware is incredibly easy to execute and scale, and new digital payment methods such as cryptocurrencies make it easy to hide identities and bury a paper trail – all of which has put CISOs on high alert.

The surge in these attacks can be attributed to multiple factors:

- *Ransomware is more targeted than ever before.* Threat actors no longer have to rely on the inefficient 'spray and pray' approach – social engineering allows them to gather volumes of data on targets and craft personalised content to entice a user to click on a malicious link.
- *Ransomware can hide in plain sight.* Today's ransomware attacks are sophisticated and evasive, leveraging seemingly innocuous technologies such as Java communications and VPNs to spread laterally throughout the network. Threat actors are targeting web browsers with a new category of threats, termed Highly Evasive Adaptive Threats (HEAT), which bypass traditional security defences. These HEAT attacks can be used to deliver ransomware payloads and take advantage of today's expanded attack surfaces.
- *Ransomware is extremely lucrative.* Threat actors aren't content with the small fish anymore. Over the past two years, the average ransomware payment skyrocketed from $12,000 to $322,000 as targets shifted from individuals to large organisations with deep pockets, according to the 2022 CyberEdge Cyberthreat Defense Report.

How to prevent ransomware

Preventing ransomware requires that organisations shift from a traditional detect-and-respond approach to a Zero Trust mindset powered by isolation technology. This proactive, preventative approach safeguards mobile, distributed, and often unmanaged endpoints by routing all content through the Secure Web Gateway (SWG), where it's executed in an elastic sandbox in the cloud. Given that many of us now spend around three-quarters of our day using a web browser, isolation can also protect users against HEAT attacks from delivering malicious payloads leading to ransomware.

Here are three ways that Zero Trust powered by isolation technology can help stop ransomware attacks:

1. *Isolation automatically closes vulnerabilities.* Unfortunately, the expansion of attack surfaces means that it's virtually impossible for security leaders to completely close off initial access points for ransomware. With isolation, however, it doesn't matter if these access points are closed, because all traffic – whether it's suspicious or not – is routed through the isolation layer in the cloud and is never executed on the endpoint.
2. *Isolation helps detect abnormal behaviour.* Routing all traffic through an abstracted layer in the cloud gives organisations the visibility they need to identify and stop abnormal behaviour that, on the surface, may seem innocuous. Visibility into entities, where they are located, and the commands they are executing, enables a Zero Trust approach to cybersecurity.
3. *Isolation allows you to execute a recovery plan.* When mistakes happen, it's critical that CISOs have a recovery plan in place to determine how to respond. Answering questions like '*Can we recover lost data?*' and '*Should we pay the ransom?*' requires visibility into the network. Isolation technology makes this possible.

Take action today

Ransomware is a top concern among businesses today, and it will continue to vex security leaders in the future. Taking a Zero Trust to security and coupling it with isolation technology while it's delivered through a SASE framework provides the best defence against these highly-evasive and disruptive attacks. □

For more information, please visit
www.menlosecurity.com

MENLO SECURITY

HEAT attacks: The new era of web threats

Highly Evasive Adaptive Threats (HEAT) are currently evading multiple layers of security detection in current security stacks.

The result is the delivery of ransomware payloads and account takeovers. Discover how Menlo Security helps prevent these attacks and protect productivity, allowing your users to work without limits, while you work without worry.

Learn more at
menlosecurity.com

MENLO SECURITY

21st e-Crime & Cybersecurity Congress

"While this e-Crime was different, it was more valuable than ever, bringing my home-desk straight to the key topics, issues, speakers and solutions, to consider e-crime risks and controls in the New Normal!"

Snr IT Risk Manager IT Infra Assurance, Diligenta Limited

"I found the event highly relevant for the issues faced across the industry. The ranges of topics and multiple viewpoints being discussed helped to confirm existing strategies, inform others underway and prompt further discussion. Overall a good two days investment; congratulations to the AKJ team."

Principal Advisors, Mastercard

"e-Crime & Cybersecurity Congress 2021 is one of the best cyber conferences on the UK circuit. This year was a first being carried out remotely and very different to the normal 2-day event in person in London due to Covid-19. I found this remote approach worked very well and there was a great selection of speakers available and some excellent educational seminars. I also found the panel discussions very informative with a great selection of representative experts from their respective fields to provide a good and balanced view. I also found the resources very useful and thought it was a great touch that you could pause a session if required and that it was also available for 20 mins or so after it started in case you needed to attend to another matter prior to attending. Very good overall as ever, fingers crossed the mid-year review will be back in person again covid depending!"

Information Security Officer, North Group

"Great job done by all involved. The virtual conference operated flawlessly given the variables of presentations given. I also enjoyed still having the ability to join with likeminded people, learn the challenges people are facing, or what is going right as well as of course the nod to the products out there."

Security Consultancy Specialist Cyber Threat Management, BT

"The e-Crime & Cybersecurity Congress is a must for people within many areas of industry, as the speakers excellent, the content very relevant, the presentations fantastic, and the event excellent. I left feeling more informed and ready for new challenges."

Senior Manager Operational Risk (IT Risk)/ Data Protection Officer, UBL

2022 Congress sponsors included:

Strategic sponsors

BeyondTrust · Beyond Identity · CrowdStrike · DarkTrace · illumio · Imperva · Menlo Security · NetAcea · Okta · proofpoint · Recorded Future · Red Sift · SenseOn · Tessian

Education Seminar Sponsors

data Solutions · Cequence Security · Cofense · CybelAngel · cybersixgill · Devo · Firemon · helpsystems · Intel 471 · Cisco Kenna Security · ManageEngine · OPSWAT · Picus · Synack · Vectra

Branding Sponsors

C2 Cyber Ltd Resilience Realised · Orchestra · Telesoft

For more information, please visit
akjassociates.com/contact-us

Thank you to all our sponsors

Strategic Sponsors

corelight

CROWDSTRIKE

DARKTRACE

HUNTERS

INTIGRITI

KnowBe4
Human error. Conquered.

Recorded Future®

Education Seminar Sponsors

Abnormal

MENLO SECURITY

OPSWAT.

RELIAQUEST

Synack

VECTRA

Networking Sponsors

GATEWATCHER

PICUS

Reveal security

Silobreaker