Post event report

e-Crime & Cybersecurity Germany

22nd January 2026, Frankfurt

Strategic Sponsors

CROWDSTRIKE

Delinea
Securing identities at every interaction

rubrik

THREATLOCKER®
ZERO TRUST PLATFORM

Education Seminar Sponsors

Constella

intruder

invicti

nagomi

Recorded Future®

RED SIFT

tines

VARONIS

Networking Sponsors

CybelAngel

HarfangLab

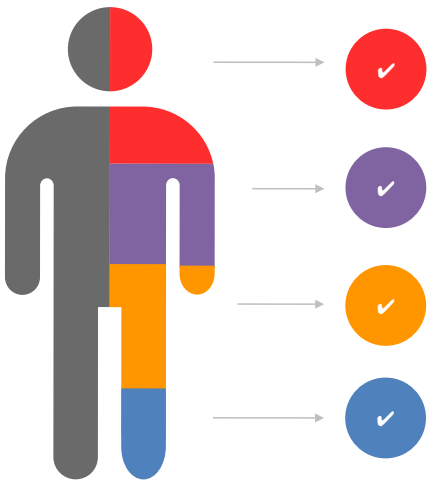
VirtualBrowser

Inside this report:

Key themes

- Making the best use of threat intelligence
- Dealing with regulations
- Security posture management
- Improving continuous attack surface discovery
- Defending against the latest ransomware variants
- The power of automation
- Adversary simulation and behavioural analysis
- Achieving visibility across ecosystems
- Transitioning OT to the Cloud?
- Why zero trust, isolation and segmentation are key
- OT and the regulations
- Pen testing for OT / SCADA

Who attended?



Cyber-security
We have a 15-year track record of producing the events cyber-security professionals take seriously

Risk Management
We attract senior risk officers with responsibility for information risk assessment and mitigation

Fraud, Audit, Compliance
We provide the go-to events for fraud prevention and compliance owners at the world's key corporates

Data Protection & privacy
We are a key venue for decision-makers with budget and purchasing authority

Speakers

Dan Andrew, Head of Security, **Intruder**

Thomas Barkias, Team Lead – Banking Supervision, **European Central Bank**

Sheeba Baskaran, Lead Security Architect, Lenovo, **Deutschland GmbH**

Susann Burnell, Principal Solution Engineer, **Tines**

Nick Coleman, Sales Engineer, **Nagomi Security**

Rupert Collier, Senior Sales Director, Europe, **Constella Intelligence**

Julian Dube, Information Security Officer, **E.ON Digital Technology**

Sachin Gaur, Cybersecurity Manager, **Continental**

Tobias Gerhardt, Sales Engineer, **Varonis**

Joël Giger, Senior Intelligence Consultant, **Recorded Future**

Dr. Gulnara Hein, CISO, **Chintai**

Tamim Mamozai, Regional Sales Director DACH, **Nagomi Security**

Billy McDiarmid, Senior Director of Sales Engineering, **Red Sift**

Eoin Molloy, Account Executive, **ThreatLocker**

Maximilian Moser, Consultant Industrial & Product Security, **VDMA**

Andreas Mueller, Regional Sales Director CEUR, **Delinea**

Igor Podebrad, Director, Office of the CISO, **Google Cloud**

Riccardo Riccobene, MD – Senior Information Security Officer, **State Street Bank International**

Manit Sahib, Ethical Hacker & Former Head of Penetration Testing & Red Teaming, **Bank of England**

Mark Schembri, Field Software Engineering Manager, **Invicti Security**

Frank Schwaak, Field CTO, **Rubrik**

Nikolei Steinhage, Senior Sales Engineer, **CrowdStrike**

Andrea Szeiler, Group CISO, **MVM Ltd**

Agenda

08:00 Breakfast networking break

09:00 Chair's opening remarks

09:10 **Operational resilience by design in the age of DORA**

Thomas Barkias, Team Lead – Banking Supervision, European Central Bank

- Redefining resilience beyond compliance, moving past DORA as a checkbox into a true resilience mindset
- Identifying the minimum viable business, mapping the critical services and dependencies that must endure disruption
- Shifting from perimeter-based security to risk-based resilience, prioritising continuity over threat-specific controls
- Integrating ICT, third-party, and operational risk, into a single, unified resilience strategy

09:30 **Countering cyber-threats with zero trust cyber & identity resilience**

Frank Schwaak, Field CTO, Rubrik

- In a world of increasingly sophisticated cyber-attacks, pure prevention is reaching its limits
- Why companies need to rethink their strategies: moving away from mere defence and towards genuine cyber and identity resilience
- How organisations cannot only prevent attacks but also respond effectively and maintain critical business processes during and after incidents
- Operational resilience thus becomes a key strategic competency for sustainable security

09:50 **Managing a live cyber-attack: The Volt Viper Scenario**

Julian Dube, Information Security Officer, E.ON Digital Technology

- Prepare and defend: Respond to a simulated cyber-attack using a fictive budget
- Take action: Discuss and make critical decisions while the attack unfolds in real time
- Play along: Your choices determine whether you stay secure or go bankrupt

10:10 **Education Seminars | Session 1**

Recorded Future	Tines	Varonis
Purchase scams uncovered: A look at the dark web's 'opportunity economy' and advanced resilience tactics **Joël Giger,** Senior Intelligence Consultant, Recorded Future	**Adapting to AI in security: Best practices for autonomous AI and human interaction** **Susann Burnell,** Principal Solution Engineer, Tines	**Preventing data breaches – Why is it so complicated across the company?** **Tobias Gerhardt,** Sales Engineer, Varonis

10:50 Networking break

11:20 **How to define and manage ICT risk in line with regulatory requirements (such as DORA and MiCA)**

Dr. Gulnara Hein, CISO, Chintai

- Building visibility by combining top-down business and bottom-up technology perspectives to map processes, systems, information assets and third parties
- Distinguishing real risks from control gaps, and why this matters for prioritisation, reporting and decision-making
- Do current risk structures underestimate the role of ICT controls in mitigating broader operational risks such as process failure, human error, and third-party disruption?

11:40 **Knowledge is the best defence – What do you know about identities?**

Andreas Mueller, Regional Sales Director CEUR, Delinea

- Recognise all identities in the company!
- AI is on everyone's lips, what does AI do to your identities?
- Manage the permissions of your critical accounts

12:00 **European threat reality 2025: How adversaries operate today**

Nikolei Steinhage, Senior Sales Engineer, CrowdStrike

- Why Europe faces an intensified threat environment and why organisations across the region are increasingly targeted by extortion- and espionage-driven campaigns
- Which adversary groups are most active right now – including their preferred tactics, from rapid ransomware operations to highly convincing social engineering
- Which industries are most at risk and the clear patterns emerging from recent attacks across Europe
- What organisations must prioritise now to build resilience against today's European adversary techniques

Agenda

12:20 — Zero Trust controls at the endpoint

Eoin Molloy, Account Executive, ThreatLocker

- Discover how ThreatLocker applies Zero Trust at the endpoint, eliminating implicit trust by continuously verifying every application, executable, and action before authorisation
- Learn how a deny-by-default, malware-proofing approach reduces ransomware risk, stopping unauthorised software and scripts even when other security layers are bypassed
- Understand how least-privilege enforcement limits attacker capability, ensuring applications and users can perform only explicitly approved actions on enterprise devices
- Explore how granular, policy-based endpoint control safeguards against modern threats, reducing enterprise exposure to ransomware and other advanced attacks

12:25 — Education Seminars | Session 2

Constella Intelligence	Intruder	Red Sift
The invisible signals that can predict cybercrime: Turning OSINT and breach data into early warning indicators **Rupert Collier,** Senior Sales Director, Europe, Constella Intelligence	**Your perimeter is on the front lines: Attack surface reduction as a primary defence** **Dan Andrew,** Head of Security, Intruder	**Defending against multi-channel brand impersonation** **Billy McDiarmid,** Senior Director of Sales Engineering, Red Sift

13:05 — Lunch networking break

14:00 — Zero Trust – Beyond the buzzword: Separating strategy from implementation

Igor Podebrad, Director, Office of the CISO, Google Cloud

- How the core principles of Zero Trust differ from how it's commonly implemented across enterprises
- Insights into real-world challenges and pitfalls organisations face when operationalising Zero Trust
- Strategies for aligning policy, identity, and architecture to achieve genuine Zero Trust outcomes
- Practical guidance on measuring Zero Trust maturity and closing the gap between intent and execution

14:20 — Ransomware 3.0: Weaponising AI for the next generation of ransomware attacks

Manit Sahib, Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England

- LIVE DEMO – Inside the first AI-powered ransomware attack – See how my custom Agentic Ransomware Gang can take down a network in under 8 minutes
- Firsthand insights from real-world red team ops – from legacy tech and broken access controls to the critical lack of real-world security testing
- Why traditional security fails – compliance checklists and conventional tools don't stop modern ransomware
- What CISOs and security leaders must do now – real-world, field-tested steps to prove your controls work before attackers do it for you

14:40 — Education Seminars | Session 3

Invicti Security	Nagomi Security
Shadow API: Find them, test them, fix what matters **Mark Schembri,** Field Software Engineering Manager, Invicti Security	**How continuous threat exposure management turns exposure data into proof of risk** **Tamim Mamozai,** Regional Sales Director DACH, Nagomi Security & **Nick Coleman,** Sales Engineer, Nagomi Security

15:20 — Networking break

15:50 — PANEL DISCUSSION — Building cyber-resilience and managing risk across critical industries

Sachin Gaur, Cybersecurity Manager, Continental (Moderator); **Sheeba Baskaran,** Lead Security Architect, Lenovo, Deutschland GmbH; **Andrea Szeiler,** Group CISO, MVM Ltd; **Riccardo Riccobene,** MD – Senior Information Security Officer, State Street Bank International; **Maximilian Moser,** Consultant Industrial & Product Security, VDMA

- How should boards and executive teams manage cyber-risk as an enterprise-wide issue rather than a technical one?
- With IT and OT convergence happening in industries from energy to transportation to manufacturing, what are the key challenges in securing both business systems and operational environments?
- How can organisations strengthen resilience against third-party and supply chain risks in today's globally interconnected economy?
- As digital transformation accelerates through technologies like AI, IoT, and automation, how can leaders balance innovation with effective cyber-risk oversight?
- Looking ahead, what governance models, cross-industry collaborations, and cultural shifts will be most essential to strengthening resilience across critical national infrastructure

16:25 — Chairs closing remarks

16.30 — End of conference

Education Seminars

Constella Intelligence

The invisible signals that can predict cybercrime: Turning OSINT and breach data into early warning indicators

Rupert Collier, Senior Sales Director, Europe, Constella Intelligence

Despite significant investment in security tooling, many organisations continue to experience cyber-incidents that feel sudden and unavoidable. In reality, many attacks are neither random nor instantaneous. They are preceded by weeks or months of external activity that leaves detectable signals – signals that are routinely overlooked because they sit outside traditional security visibility.

This session explores how cybercrime increasingly begins with exposed identities rather than exploited systems. Stolen credentials, identity reuse, and publicly available information are leveraged by attackers long before they attempt to access an organisation's environment. While most security teams focus on internal telemetry such as logs, alerts, and endpoint activity, attackers operate upstream, harvesting credentials, mapping organisational relationships, and preparing access paths in advance.

Attendees will be introduced to the concept of early warning indicators derived from breach data, open-source intelligence (OSINT), and identity exposure. The presentation examines how these external signals can be correlated to identify which identities are most likely to be exploited, which roles carry the greatest risk, and where targeted preventive action can meaningfully reduce attacker success.

Rather than focusing on tools or alerts, the session presents a practical, vendor-agnostic model for turning external intelligence into decision-quality insight. Through real-world examples and operational framing, the talk demonstrates how organisations can move detection earlier in the attack lifecycle, shifting from reactive response to proactive risk management.

This presentation is designed for security practitioners, incident responders, threat intelligence teams, and security leaders seeking to better understand how identity-centric risk signals can change the timing, effectiveness, and cost of cyber-defence.

Attendees will learn:

- Why many cyber-attacks are predictable earlier than most organisations realise
- How stolen credentials and identity reuse function as leading indicators of compromise
- The role of breach data and OSINT in pre-incident cyber-risk detection
- How to distinguish between raw exposure data and actionable risk signals
- A practical framework for turning external intelligence into targeted preventive action

Intruder

Your perimeter is on the front lines: Attack surface reduction as a primary defence

Dan Andrew, Head of Security, Intruder

This education seminar will provide a deep-dive into core concepts and practical recommendations for Attack Surface Management (ASM) and Asset Discovery. Your perimeter is on the front line, and good patch management alone is not enough to protect it. You should leave this session with a better idea of how to blend ASM and asset discovery with patch management for a robust exposure management process.

We'll run through examples of attack surface risks, real-world vulnerabilities affecting internet exposed tech, and why implementing an ASM process is critical alongside patch management. It may be tempting to fall back on just patching your biggest *known* threats, but some of the biggest risks are vulnerabilities that are not yet publicly known. These threats do not have a CVSS score, and attack surface management is your primary defence. Learn how to future-proof your perimeter.

Asset discovery is also an essential part of managing your attack surface. Keeping track of your internet exposed IPs and domains is far from trivial, and cloud environments in particular make this challenge harder. Losing track of some of your assets is no longer an embarrassing mistake – it's an unavoidable reality. We will show some examples of how this happens, and give a practical approach to asset discovery which helps you keep track, and avoid systems slipping outside of your exposure management process entirely.

Attendees will learn:

- Integrating ASM into your patch management process – defining ASM as a primary defence that's proactive, not reactive
- Prioritisation considerations and why informational risks are criticals waiting to happen. Why not all 'criticals' are equal, and why CVSS is not king
- The importance of asset discovery to find shadow IT and build a realistic view of your attack surface. Practical recommendations on how to approach this

Education Seminars	
Invicti Security **Shadow API: Find them, test them, fix what matters** **Mark Schembri,** Field Software Engineering Manager, Invicti Security	Your business is increasingly API-driven, yet partially blind when it comes to API security. Often, security teams are unsure of the number of APIs they have, let alone which ones are exposed, undocumented, or vulnerable. Join us to learn how you can apply Invicti's multilayered approach to shadow API discovery and schema reconstruction. Once discovered, you test these APIs with the industry's best DAST. Validating difficult-to-find vulnerabilities like BOLA and BLFA, business logic errors, and the presence of weak authentication with proof-based scanning to achieve AppSec's charter that only secure apps reach production. **Attendees will learn:** • Sensorless API discovery and schema reconstruction • API management system integration • Network traffic analysis (NTA) across F5, NGINX, and Cloudflare • OWASP Top 10 for API testing and reporting
Nagomi Security **How continuous threat exposure management turns exposure data into proof of risk** **Tamim Mamozai,** Regional Sales Director DACH, Nagomi Security & **Nick Coleman,** Sales Engineer, Nagomi Security	Senior security leaders don't need another recap of tool sprawl or vulnerability overload – you live it. The question is: how do you prove which exposures actually raise breach risk in your environment, and eliminate them faster than the threat changes? That's where continuous threat exposure management becomes practical. In this 30-minute, interactive session, we will skip definitions and go straight to execution. Expect a fast, lively walkthrough of what works, what fails, and the assumptions continuous threat exposure management routinely overturns. No pitch – just repeatable methods and hard-earned lessons to make CTEM measurable and defencible. **Attendees will learn:** • Verify what you actually own, revealing true scope and exposure at the foundation of your attack surface • Continuously validate controls, catching drift and coverage gaps before they fail silently • Identify real exposure beyond CVEs, including misconfigurations, identity abuse paths, and control weaknesses • Focus remediation on what matters most, based on how active attackers actually operate • Practical continuous threat exposure management moves you can apply immediately to reduce real risk
Recorded Future **Purchase scams uncovered: A look at the dark web's 'opportunity economy' and advanced resilience tactics** **Joël Giger,** Senior Intelligence Consultant, Recorded Future	Purchase scams are a major emerging fraud threat using fake e-commerce stores to steal data and accept payments for non-existent goods. The dark web's 'opportunity economy' amplifies these scams through market promotions for criminal services and emerging AI tools for content generation and scale. Threat actors also employ advanced strategies to ensure resilience, which complicates detection and investigation. Effective mitigation requires scam merchant intelligence and increased customer awareness. **Attendees will learn:** • The role of the dark web 'opportunity economy' and emerging AI tools in rapidly scaling and amplifying purchase scam infrastructure and campaigns • The advanced resilience tactics prolonging the scams' lifespan and complicating investigations • How to mitigate purchase scam risk using scam merchant intelligence for proactive detection and the importance of robust customer awareness and education programmes for card issuers and merchant acquirers

Education Seminars	
Red Sift **Defending against multi-channel brand impersonation** **Billy McDiarmid,** Senior Director of Sales Engineering, Red Sift	Even with SPF and DMARC in place, cybercriminals are now impersonating organisations across email, web, and social media to deceive customers and partners. During this session, Red Sift expert Billy McDiarmid will reveal how lookalike domains, forgotten DNS records, and fake social profiles erode brand integrity. With brand and social media monitoring, you'll see how security teams can detect and shut down impersonation campaigns across every digital channel. **Attendees will learn:** • How attackers leverage DNS gaps and high-risk lookalikes to launch cross-channel impersonation attacks • The power of AI-driven detection and agentic automation that makes response faster and smarter • How to build a robust defence against exact-domain spoofing and lookalike domain attacks
Tines **Adapting to AI in security: Best practices for autonomous AI and human interaction** **Susann Burnell,** Principal Solution Engineer, Tines	Artificial intelligence holds great promise for cybersecurity professionals, who see AI as a key tool in the complex and critical effort to stay ahead of cyber-threats. Layering AI-driven capabilities onto existing frameworks like SOAR (security orchestration, automation, and response) and SIEM (security information and event management) can be labour- and skills-intensive. **Attendees will learn:** • How Tines address many of the challenges around integrating AI into SecOps • The common challenges driving organisations to modernise SecOps • The latest market trends driving use of AI as a component of modern cybersecurity
Varonis **Preventing data breaches – Why is it so complicated across the company?** **Tobias Gerhardt,** Sales Engineer, Varonis	If you know you would be screwed if data gets stolen, I can show you how to close a few often-existing gaps. In our modern IT world, we are constantly focused on preventing external threats. However, we often overlook the golden nugget: sensitive data. However, the root cause of this problem is not as easily solved as one might think. That is because companies still misinterpret who could be an enemy and who could be a target. Furthermore, a 9-to-5 job has its limits and so does the company's pocket. Therefore, I will explain a common but still underestimated attack vector. It will also outline the situation in which you end up, when you think that's enough. In turn, we will dig into three vectors that could still allow stealing data and how a little 'control the controllables' by the help of the Varonis Data Security Platform could tackle them. **Attendees will learn:** • You will learn which aspects around holistic data security exist • Why too much effort into a single aspect or point solution can cause problems • How Varonis does support data security across different domains