Black Hat 2024

Cybersecurity Pulse Report

10 Pillars of Modern Cybersecurity: From AI to Zero Days
Expert Insights and Emerging Trends from Black Hat 2024

iSMG

Table of Contents

Introduction

Welcome to the latest edition of our Pulse Report series, the 2024 Black Hat Edition.

At ISMG, we are spearheading the use of advanced Generative AI platforms and workflows to uncover detailed insights from extremely large data sets and bring those insights to you faster and in a concise and digestible format. This report series exemplifies our commitment to leveraging cutting-edge technology in service of cybersecurity knowledge sharing.

Our innovative AI-driven process has transformed hundreds of pages of video interview transcripts from the 2024 Black Hat conference into this comprehensive yet accessible report. This approach allows us to rapidly extract key insights from a vast amount of raw video and text data, connecting cutting-edge research with practical application in record time. By harnessing the power of AI, we're able to identify trends, highlight critical information, and synthesize diverse expert opinions into a cohesive narrative - all while maintaining the nuanced perspectives that make these conferences so valuable.

Our AI-powered workflow doesn't just get you the information faster; it enhances the quality and depth of our analysis, uncovering connections and patterns that might be missed by traditional methods.

The report covers critical areas shaping cybersecurity:

- AI-powered threats and defensive strategies
- Legal and regulatory challenges facing CISOs
- Vulnerabilities in critical infrastructure
- Breakthroughs in security testing and automation
- Emerging privacy concerns & data leakage risks
- And much more...

Black Hat has long been a crucible for advanced cybersecurity thinking. By capturing and analyzing discussions from this influential forum, we've created a resource that encapsulates current industry thought leadership.

For marketing professionals, this report offers a goldmine of information on emerging trends and pain points, providing clear direction for targeted strategies.

This report is also essential reading for those at the forefront of cybersecurity. Whether you're a CISO developing security strategies or a practitioner seeking to enhance your knowledge and understanding, you'll find invaluable perspectives here.

I encourage you to approach this report with an eye toward practical implementation. The ideas and innovations discussed are actively shaping our industry's future. By leveraging this knowledge, we can collectively strengthen our defenses and build a more secure digital ecosystem.

Sincerely,

Daniel Verton

Dan Verton
Vice President, Content Intelligence and AI Innovation
ISMG

Executive Summary

AI-Driven Analysis: Mapping Black Hat Themes to ISMG Interviews

Our AI-powered analysis and integration of data has masterfully woven the tapestry of Black Hat's cutting-edge themes with a comprehensive report outline based on subject matter expert interviews. This analysis reveals how the pulse of the cybersecurity world, as reflected in Black Hat's agenda, directly informs and shapes our journalistic approach.

Black Hat's emphasis on "AI ML & Data Science" finds its mirror in our report's robust "AI and Machine Learning in Cybersecurity" section. While Black Hat delves into technical aspects like "Deep Backdoors in Deep Reinforcement Learning Agents," our interviews with industry titans such as Sam Curry of Zscaler and Sherrod DeGrippo of Microsoft explore the broader implications of AI as an "accelerant in cyber threats."

The conference's "Exploit Development & Vulnerability Discovery" theme aligns seamlessly with our "Vulnerabilities and Exploits" section. Black Hat's technical sessions on topics like "Bypassing ARM's Memory Tagging Extension" are complemented by our interviews with experts like Thijs Alkemade of Computest Sector 7, who breaks down complex exploits for our audience.

Black Hat's "Enterprise Security" track finds its counterpart in our "Cybersecurity in Enterprises" section. While the conference explores specific attack vectors like "Hook Line and Sinker: Phishing Windows Hello for Business," our interviews with leaders like Ravi Ithal of Normalyze examine the broader challenges of securing cloud environments and managing the proliferation of AI in corporate settings.

The urgency reflected in Black Hat's "Cyber-Physical Systems & IoT" theme is echoed in our "Critical Infrastructure and Ransomware" section. As the conference tackles topics like "Nope S7ill Not Secure: Stealing Private Keys From S7 PLCs," our interviews with Joe Marshall of Cisco Talos and Bryson Bort of SCYTHE provide a strategic view of the threats facing our most vital systems.

While not explicitly featured in the Black Hat themes, our "Legal and Regulatory Challenges" section fills a crucial gap. Interviews with legal experts like Jess Nall of Baker McKenzie LLP provide essential context to the technical discussions at Black Hat, exploring the real-world implications of cybersecurity failures in the courtroom and boardroom.

Black Hat's forward-looking "Threat Hunting & Incident Response" theme is mirrored in our "Emerging Threats and Red Teaming" section. As the conference explores "Modern Kill Chains," our interviews with experts like Brandon Kovacs of Bishop Fox dive into the alarming advancements in real-time deep fakes and their potential for social engineering attacks.

The theme of resilience, touched upon in various Black Hat sessions, is given dedicated focus in our "Security Testing and Resilience" section. While Black Hat examines technical aspects of resilience, our interview with Theresa Lanowitz of LevelBlue provides a strategic outlook on cyber resilience for the coming year.

Black Hat's exploration of cutting-edge security tools in sessions like "5 Ways to Break Your Copilot" is complemented by our "Innovations in Cybersecurity Tools" section. Interviews with pioneers like Jeff Williams of Contrast Security shed light on emerging concepts such as Application Detection and Response (ADR).

The critical role of threat intelligence, a theme woven throughout the Black Hat conference, is spotlighted in our "Threat Intelligence and Research" section. As Black Hat sessions dissect specific threats, our interviews with experts like Malachi Walker of DomainTools provide insight into the broader landscape of cyber threat intelligence.

While Black Hat touches on privacy concerns in various sessions, our "Privacy, Data Leakage, and API Vulnerabilities" section provides a dedicated exploration of this critical area. Interviews with researchers like Karel Dhondt and Victor Le Pochat of KU Leuven bring to light the often-overlooked vulnerabilities in location data and APIs.

This AI-driven analysis demonstrates the symbiotic relationship between the technical depth of Black Hat and the strategic approach of ISMG's editorial interviews. It showcases how cutting-edge AI can distill complex conference agendas into actionable journalistic frameworks, ensuring comprehensive coverage of important knowledge sharing events.

Methodology

This comprehensive Cybersecurity Pulse Report was created using a innovative, AI-driven approach that combines cutting-edge technology with expert insights to deliver a thorough analysis of the current cybersecurity landscape. It is sourced from comprehensive interviews conducted by Tom Field, Senior Vice President of Editorial at ISMG, Michael Novinson, ISMG's Managing Editor of Business, and Aseem Jakhar, co-founder of EXPLIoT.

STEP 1

AI Analysis of Black Hat Conference Agenda

We employed advanced AI workflows to analyze the entire Black Hat 2024 conference agenda. This process allowed us to:

- Extract and categorize key themes and topics
- Identify trending subjects and emerging areas of focus
- Map the landscape of current cybersecurity concerns and innovations

STEP 2

AI Processing of Expert Interviews

Our editorial team conducted in-depth interviews with 50 subject matter experts, resulting in hundreds of pages of video interview transcripts. These were then processed using AI to:

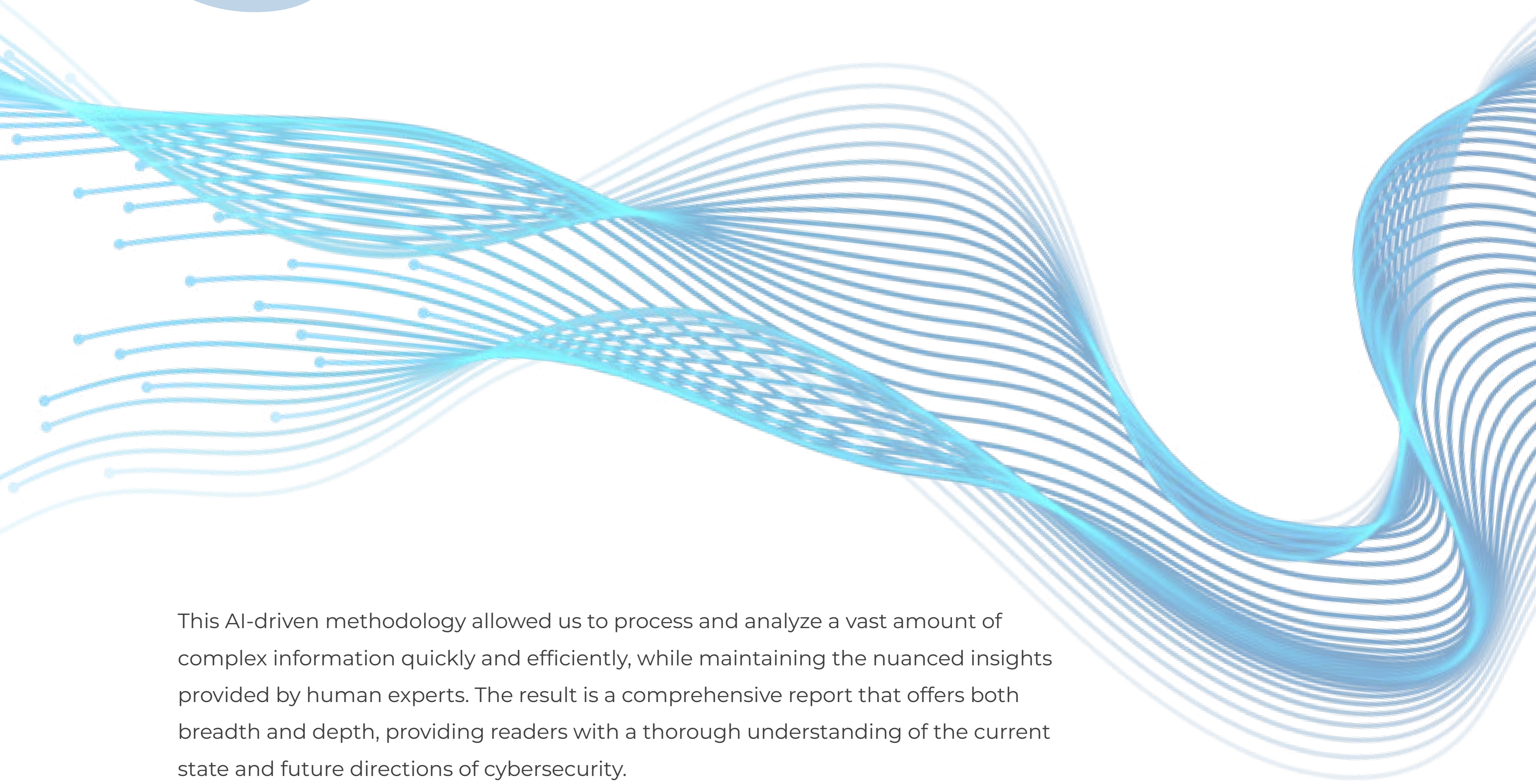
- Transcribe and analyze hundreds of pages of interview content
- Extract key insights, opinions, and predictions
- Identify common threads and unique perspectives across the expert pool

STEP 3

AI Integration and Synthesis

In the final phase, we leveraged AI to integrate the expert interview insights with the key themes extracted from the Black Hat agenda. This process involved:

- Mapping expert commentary to relevant conference themes
- Identifying areas of consensus and debate among experts
- Synthesizing diverse viewpoints into coherent narratives for each key theme



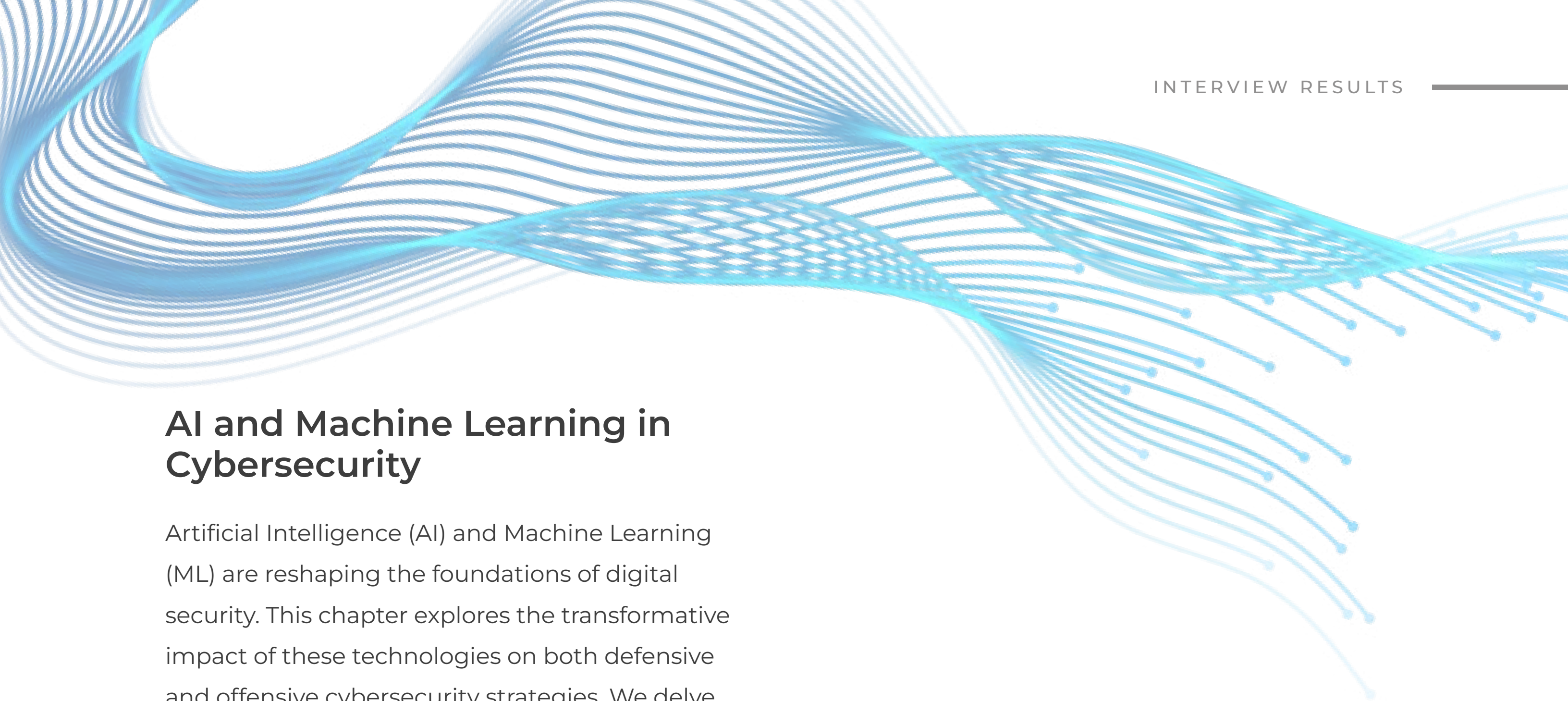
This AI-driven methodology allowed us to process and analyze a vast amount of complex information quickly and efficiently, while maintaining the nuanced insights provided by human experts. The result is a comprehensive report that offers both breadth and depth, providing readers with a thorough understanding of the current state and future directions of cybersecurity.

By leveraging multiple Large Language Models and automated AI workflows throughout the process, we were able to identify patterns, connections, and insights while still preserving the valuable context and expertise provided by human subject matter experts.

Topical Analysis

AI and Machine Learning in Cybersecurity

This chapter explores the transformative impact of AI and ML on digital security. Experts discuss how generative AI has crossed the “uncanny valley,”reshaping both defensive and offensive strategies. The dual nature of AI as both shield and weapon is examined, along with the risks of treating ML models as executable code. From accelerating cyber threats to introducing new vulnerabilities in AI-generated code, the chapter underscores the need for adaptive security measures. It concludes by emphasizing the critical importance of balancing AI’s potential with robust, AI-specific security protocols.



AI and Machine Learning in Cybersecurity

Artificial Intelligence (AI) and Machine Learning (ML) are reshaping the foundations of digital security. This chapter explores the transformative impact of these technologies on both defensive and offensive cybersecurity strategies. We delve into the complexities of generative AI, examining its potential to revolutionize threat detection while simultaneously creating new vulnerabilities.

Through expert insights from the Black Hat conference, we uncover the challenges of securing AI systems themselves, the emergence of AI-enhanced cyberattacks, and the evolving role of machine learning models in security infrastructures. This exploration reveals not just the technical advancements, but also the profound ethical and strategic implications of AI integration in the cybersecurity domain.

> “It’s like tanks in World War One… they didn’t have as big an effect as they probably should have. I think we have yet to figure out how best to employ [AI] in a conflict theater.”
>
> **Sam Curry**
> Vice President and Chief Information Security Officer (CISO) at Zscaler

Generative AI and Its Impacts

Generative AI has crossed the “uncanny valley” and become deeply integrated into various sectors, including cybersecurity. Sam Curry, Vice President and Chief Information Security Officer (CISO) at Zscaler, reflected on the profound societal and cybersecurity implications of this technology. He noted that generative AI has reached a point where it can easily be anthropomorphized, leading to significant societal impacts, especially when misused for manipulating public opinion. “It crossed the uncanny valley right? So people started to actually see it and even personify it or anthropomorphize it. And I think that’s fairly significant,” Curry said.

Curry also highlighted the dual role of AI in cybersecurity, where it can both enhance defenses and facilitate more sophisticated cyberattacks. He compares the current state of AI in cybersecurity to the early days of tanks in warfare, suggesting that the full potential of AI in this field is yet to be realized. “It’s like tanks in World War One… they didn’t have as big an effect as they probably should have… I think we have yet to figure out how best to employ [AI] in a conflict theater,” he added.

AI in Cyberattacks and Defense

The integration of AI into cyberattacks is becoming increasingly sophisticated. Michael Sikorski, Vice President of Threat Intelligence and Chief Technology Officer (CTO) at Unit 42, Palo Alto Networks, discussed how attackers are leveraging AI to automate and enhance various stages of their operations, from phishing to malware creation. “A lot of the way that generative AI specifically has been leveraged by attackers has been focused on things like phishing attacks. What they’re starting to experiment with and get into is things like how do they build malware more efficiently,” Sikorski said.

On the defensive side, AI is being used to simulate adversarial activities, helping organizations strengthen their security postures through automated red teaming and threat simulation. Despite these advances, Sikorski underscored the importance of defense-in-depth strategies, especially as certain attacks, such as zero-day exploits and supply chain compromises, are difficult to prevent.

> Basically the model allows you to insert code into it and then when you load the model… you get code execution. Almost everybody I know who works with models wasn’t aware of that fact.
>
> **Shachar Menashe**
> Senior Director of Security Research at JFrog

ML Models as Executable Code

The security of ML platforms presents unique challenges that differ significantly from traditional systems. Shachar Menashe, Senior Director of Security Research at JFrog, pointed out that many in the field are unaware that ML models can be treated as executable code, which poses a significant security risk.

“Basically the model allows you to insert code into it and then when you load the model… you get code execution. Almost everybody I know who works with models wasn’t aware of that fact,” Menashe said.

Menashe’s research highlighted the vulnerabilities inherent in ML platforms, particularly in how they handle models and datasets. The ability of these platforms to execute code upon loading a model or dataset opens up avenues for exploitation, much like historical vulnerabilities found in document formats like Word and Excel. He warned that the immaturity of MLOps platforms, combined with these vulnerabilities, will likely lead to an increase in security incidents as adoption grows.

Security Challenges Unique to AI/ML Systems

AI/ML systems present novel security challenges that necessitate a different approach from traditional cybersecurity methods. Michael Brown, Principal Security Engineer at Trail of Bits, underscored the importance of understanding that AI/ML systems interact with data in fundamentally different ways. "One of the things that we think is really important to understand and acknowledge right off the bat when dealing with security issues in AI/ML systems is that they are not conventional computing systems. They interact with data and have a relationship with data in an entirely different way," Brown said.

These differences introduce new attack surfaces and vulnerabilities, particularly in large-scale AI systems like large language models (LLMs). Brown stresses the need for secure development practices tailored to the unique characteristics of AI/ML, as the scale and complexity of these systems make them particularly challenging to secure.

AI as an Accelerant in Cyber Threats

AI is not only transforming defensive strategies but is also serving as an accelerant in cyber threats. Sherrod DeGrippo, Director of Threat Intelligence Strategy at Microsoft, discussed how threat actors are using AI to enhance their operations, particularly in social engineering. "AI is an accelerant. It makes things go much, much faster. It enables people who don't have skills to be able to increase their skills for good or for ill," DeGrippo said.

She also warned of the potential for AI to be used in creating new types of malware, though this has not yet become widespread. The dual nature of AI—as both a tool for innovation and a threat—makes it imperative for organizations to adopt safe and responsible AI practices.

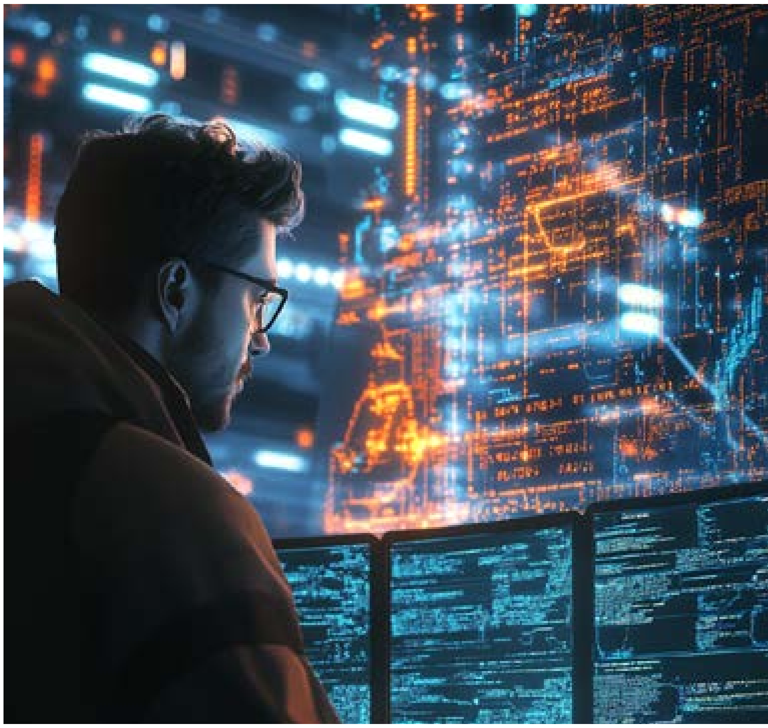
Michael Brown, Principal Security Engineer at Trail of Bits. View the full interview here.

> AI is an accelerant. It makes things go much, much faster. It enables people who don't have skills to be able to increase their skills for good or for ill.
>
> **Sherrod DeGrippo**
> Director of Threat Intelligence Strategy at Microsoft

Generative AI and Application Security

While boosting productivity in software development, Generative AI also introduces new security risks. Chris Wysopal, Co-Founder and CTO of Veracode, highlighted that AI-generated code often inherits the same vulnerabilities as code written by humans. “Around 30 to 40 percent of the code that’s generated will have a vulnerability in it. It was trained on human generated code,” Wysopal said.

To mitigate these risks, Wysopal advocates for the use of specialized AI models trained on secure coding practices. He also emphasized the importance of integrating automated security testing and remediation into the development process to manage the increased volume of code produced by AI tools.

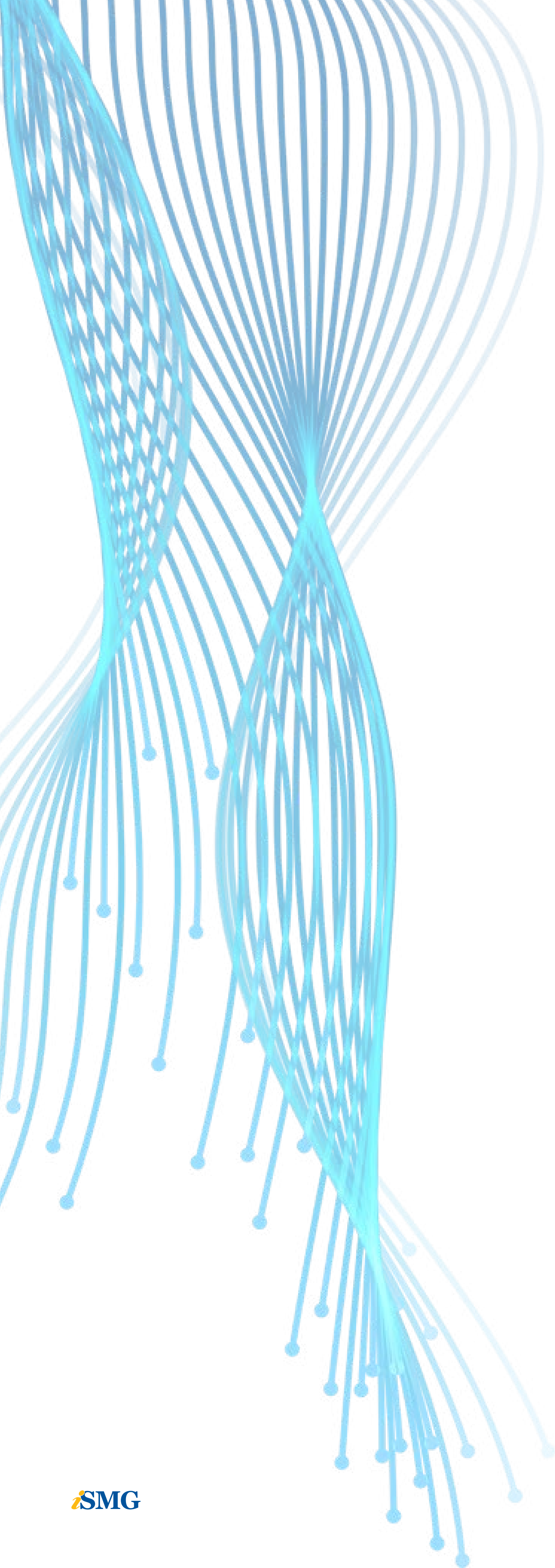


AI and Automation in Cybersecurity

AI and automation are becoming integral to modern cybersecurity strategies. Alberto Yépez, Co-Founder and Managing Director of Forgepoint Capital, discussed the dual role of AI as both a defensive tool and a threat vector. He said that while AI can drive efficiency and innovation, it also poses challenges, particularly in terms of data security and the emergence of “shadow AI.”

“The threat vectors and the adversaries are getting more efficient through the use of automation and AI. The threat landscape is only getting more advanced,” Yépez said.

Yépez also highlighted the growing focus on using AI to secure small to mid-sized businesses (SMBs), which have traditionally been underserved in the cybersecurity space. The evolving threat landscape, driven by AI and automation, requires continuous adaptation and investment in new security technologies.



Conclusion

The integration of AI and ML into cybersecurity presents a paradigm shift, offering both unprecedented opportunities and formidable challenges:

1. Generative AI demonstrates dual potential, enhancing defenses while also enabling more sophisticated attacks.
2. AI-generated code introduces new security risks, necessitating specialized models trained on secure practices.
3. Machine learning models, when treated as executable code, present unique vulnerabilities that demand innovative protection strategies.
4. AI serves as an accelerant in cyber threats, particularly in social engineering and potential malware creation.
5. The security of AI/ML systems themselves emerges as a critical concern, requiring approaches distinct from traditional cybersecurity methods.

As AI and ML continue to evolve, cybersecurity strategies must adapt in tandem. Organizations need to embrace a multi-faceted approach that leverages AI's defensive capabilities while actively mitigating its potential for misuse. This includes developing AI-specific security protocols, integrating continuous automated testing in AI-driven development processes, and fostering a deep understanding of AI/ML vulnerabilities among security professionals.

Vulnerabilities and Exploits

This chapter delves into the evolving landscape of cybersecurity vulnerabilities, from persistent SQL injection threats to cutting-edge AI system risks. Experts highlight the enduring danger of traditional exploits alongside emerging risks in IoT devices, like EV chargers. The discussion spans hardware vulnerabilities, cloud environment risks in Amazon Machine Images, and new attack vectors in AI tools such as Microsoft Copilot. The chapter emphasizes the increasing sophistication of attacks, exemplified by the Black Lotus exploit, and stresses the critical need for adaptive, comprehensive security strategies to address both longstanding and novel threats.

Vulnerabilities and Exploits

Cybersecurity vulnerabilities represent a constantly shifting battlefield. From longstanding threats like SQL injection to cutting-edge risks in AI-driven systems, the spectrum of potential exploits continues to expand and evolve. This chapter delves into the critical vulnerabilities identified by leading industry experts, offering a comprehensive exploration of the current cybersecurity landscape.

Our journey through this digital minefield begins with persistent challenges such as SQL injection and memory safety issues in programming languages. We then navigate the treacherous terrain of hardware vulnerabilities in IoT devices, exemplified by the surprising weaknesses found in electric vehicle chargers. The chapter also sheds light on the often-overlooked risks lurking in cloud environments, particularly within Amazon Machine Images.

We also examine the emerging vulnerabilities in machine learning platforms and AI tools like Microsoft Copilot, where the line between productivity enhancement and security risk becomes increasingly blurred. The discussion extends to sophisticated attacks like the Black Lotus, which exploit downgrade vulnerabilities in operating systems.

Through the insights of security researchers and professionals, this chapter not only identifies these vulnerabilities but also explores the strategies needed to address them. As we navigate this complex landscape, one thing becomes clear: the need for vigilance and adaptability in cybersecurity practices has never been greater.

Paul Gerste, Vulnerability Researcher at Sonar. View the full interview here.

> SQL injections tend to have a high impact if they happen because databases are high-value targets. They contain customer data, personal data, and also things relevant to authentication.

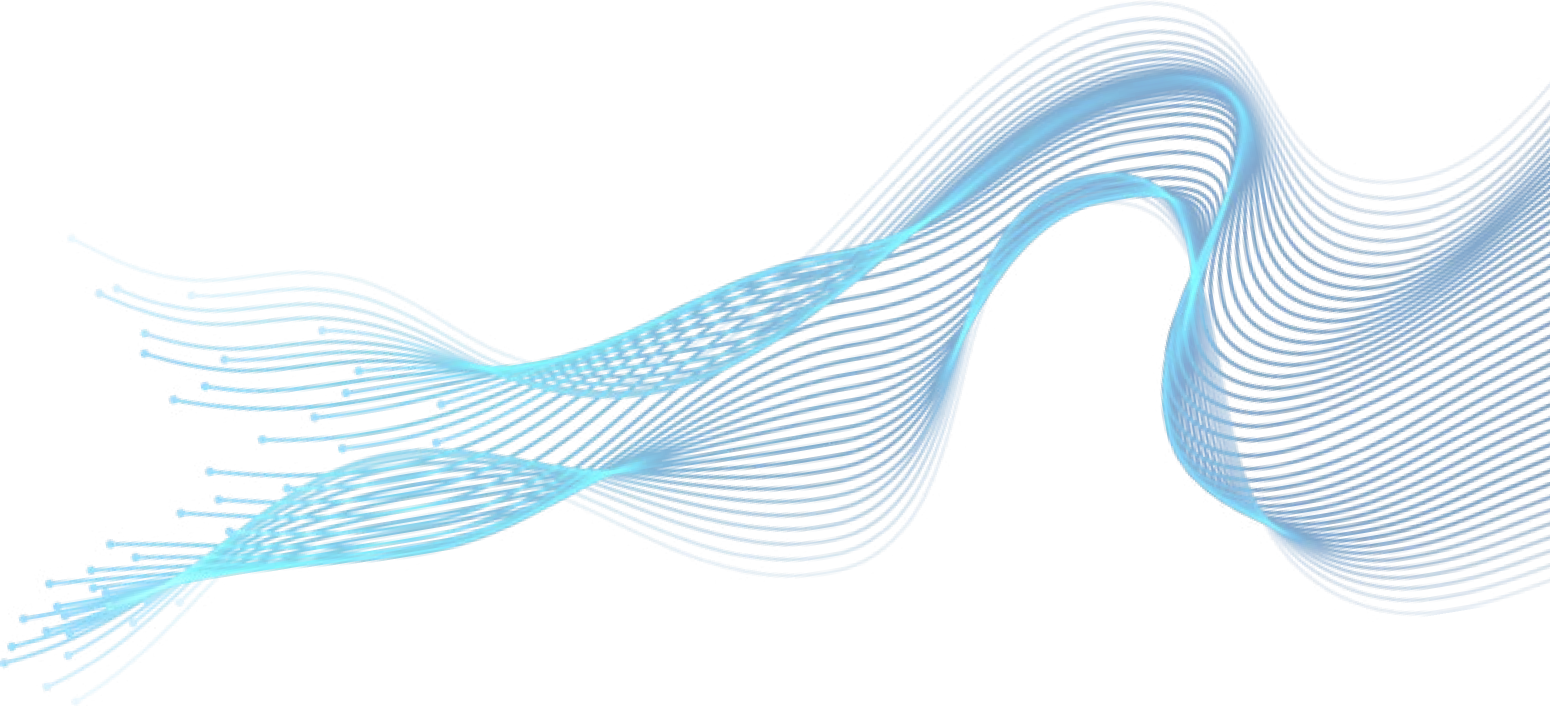
Paul Gerste
Vulnerability Researcher at Sonar

Persistence of SQL Injection Vulnerabilities

Paul Gerste, a Vulnerability Researcher at Sonar, provides a detailed analysis of the persistent threat posed by SQL injection attacks, highlighting their enduring relevance and impact despite advances in security practices. According to Gerste, SQL injection vulnerabilities remain a significant concern because databases, are high-value targets for attackers. He points out that although modern developers have access to various tools and best practices designed to secure their code, these vulnerabilities continue to occur, often due to lapses in proper implementation.

“SQL injections tend to have a high impact if they happen because databases are high-value targets. They contain customer data, personal data, and also things relevant to authentication,” Gerste said.

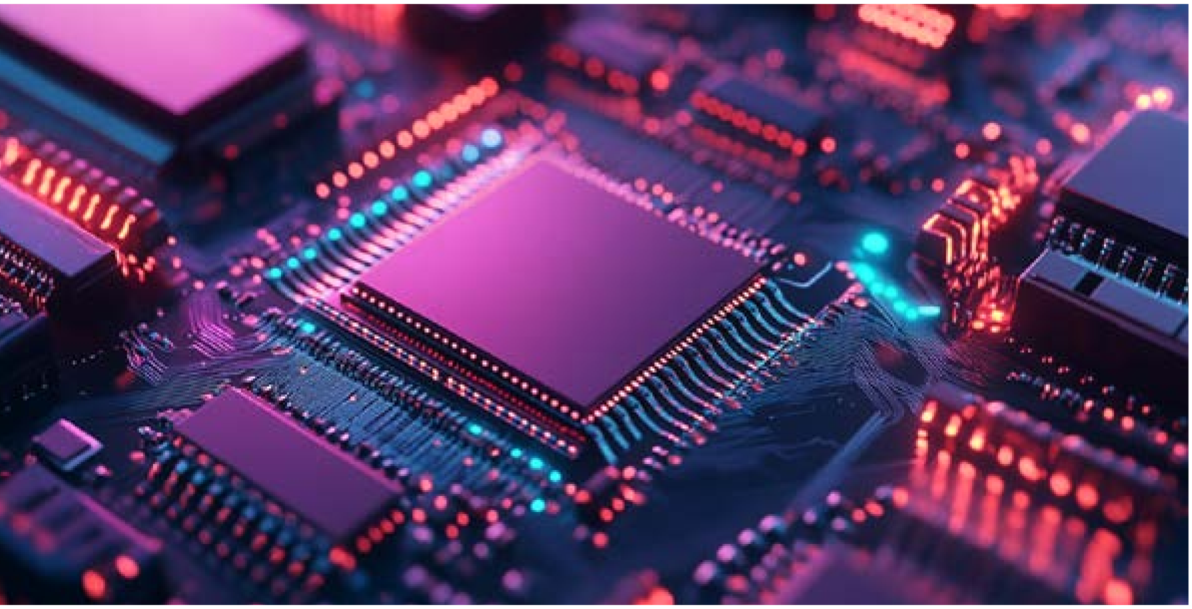
Gerste emphasizes that the risk of SQL injection is exacerbated by improper coding practices. Specifically, he notes that the use of insecure methods or incorrect libraries in database queries can open the door to exploitation. Even when developers use the right libraries, the complexity of certain queries might lead them to take shortcuts, such as manually building query strings, which increases vulnerability to attacks. He illustrates this with a stark warning: “If you just use the wrong library that doesn’t give you all the safeguards then it’s easy to take the convenient but insecure route to just build the query string yourself and hope for the best. But of course, the attackers are going to get you,” Gerste said.



Memory-Safe vs. Memory-Unsafe Languages

In the context of memory-safe environments, Gerste also explores the potential for data-only attacks, where attackers might exploit vulnerabilities through mishandled integers in messages between applications and databases. These vulnerabilities can allow attackers to inject harmful SQL commands, further underscoring the importance of robust security measures.

While memory-unsafe languages like C require developers to be vigilant against severe errors, memory-safe languages can create a false sense of security. “In memory-unsafe languages, developers are more trained to look out for these things because they have a higher impact or more severe impact if something like an integer overflow happens,” says Gerste. However, even in memory-safe languages, improper handling of data can lead to significant vulnerabilities, such as data-only attacks.



Vulnerabilities in EV Chargers

Thijs Alkemade, a Security Researcher at Computest Sector 7, discussed the vulnerabilities his team uncovered in electric vehicle (EV) chargers during the Pontoon automotive security challenge. He detailed how his team successfully exploited these vulnerabilities across different brands of EV chargers, identifying weaknesses primarily in Bluetooth and Wi-Fi connectivity that allowed them to gain control over the devices. These exploits often involved achieving arbitrary code execution, including through techniques like buffer overflow attacks.

“We could get arbitrary code running on the charger. Sometimes by being on the same Wi-Fi network. Sometimes just connecting over Bluetooth,” Alkemade details.

Alkemade emphasized that IoT devices, including EV chargers, tend to have more vulnerabilities compared to traditional servers or desktops. This higher prevalence is partly due to the difficulties researchers face in accessing the firmware of these devices, which limits the discovery and remediation of potential security issues.

Additionally, Alkemade provided practical advice for other security researchers, stressing the importance of acquiring firmware and debugging information when investigating IoT devices. He suggested starting with hardware reconnaissance and thoroughly examining memory copy operations as critical initial steps in identifying and exploiting vulnerabilities.

Code Execution and Buffer Overflow Exploits

Buffer overflow exploits remain a critical threat in the cybersecurity landscape. Alkemade provides insight into how these exploits are used to achieve arbitrary code execution, particularly in the context of EV chargers. By exploiting stack buffer overflows, attackers can manipulate these devices, turning them into tools for unauthorized control or data theft.

Specifically, he mentions finding this vulnerability in a device called “JuiceBox,” where they turned log messages into a mechanism that could overflow the stack buffer. This lack of proper security, like the absence of authentication on Bluetooth, allowed them to easily connect to the charger and begin executing arbitrary code.

“We found a way to turn log messages into a way that would also overflow stack buffer,” he said. “There’s also no authentication on Bluetooth so you just connect to the charger just one payload and you’re on your arbitrary code journey.”

Vulnerabilities in Machine Learning Platforms

Machine learning platforms, integral to modern AI applications, also present significant security challenges. Shachar Menashe, Senior Director of Security Research at JFrog, discussed the inherent vulnerabilities in ML platforms, particularly the dangers of treating ML models as mere data rather than executable code.

"Basically the model allows you to insert code into it and then when you load the model... you get code execution," Menashe warned.

Menashe also pointed out the dangers posed by malicious datasets and the security risks within Jupyter notebooks. He explained that some ML platforms permitted code execution when loading datasets, which could be exploited by attackers. Additionally, in Jupyter notebooks, cross-site scripting (XSS) vulnerabilities could escalate to full remote code execution (RCE), posing severe risks to users.

Addressing the broader challenges, Menashe noted that MLOps platforms were relatively immature, contributing to a high number of vulnerabilities. He pointed out that these platforms had seen numerous CVEs (Common Vulnerabilities and Exposures) in recent years, a trend that he expected to continue as the platforms evolved.

To mitigate these risks, Menashe advised implementing several security measures, such as disabling unused features, enforcing the use of secure model formats that did not allow code execution, and ensuring robust authentication mechanisms. He stressed the importance of educating users to treat ML models as potentially executable code to prevent security breaches.

Shachar Menashe, Senior Director of Security Research at JFrog. View the full interview here.

> Basically the model allows you to insert code into it and then when you load the model... you get code execution.
>
> **Shachar Menashe**
> Senior Director of Security Research at JFrog, on the dangers of treating ML models as mere data rather than executable code.

Vulnerabilities in Sonos Devices

Alexander Plasket and Robert Herrera from NCC Group focused on vulnerabilities in Sonos devices, highlighting two major issues: a memory corruption flaw in the wireless kernel module and a weakness in the Secure Boot chain. They emphasized the critical importance of addressing both hardware and software vulnerabilities holistically to prevent exploitation. The pair also detailed their methodology for identifying these vulnerabilities, which includes reverse engineering, code review, and fuzzing. Additionally, they noted the varying levels of security maturity among vendors and stressed the importance of improving supply chain security through rigorous audits and thorough tracking of devices during production.

Herrera explained that the vulnerability was related to a memory corruption issue, specifically a stack buffer overflow, in the MediaTek Wi-Fi stack implementation within the Sonos device's wireless kernel module. He emphasized that they were able to exploit this vulnerability due to the lack of security mitigations in place, which could allow an attacker to take control of the device. "We found a bug in the wireless kernel module that's in charge of parsing Wi-Fi messages going over the air in the Sonos device namely a MediaTek Wi-Fi stack implementation...a memory corruption vulnerability or really just the classic stack buffer overflow," Herrera said, underscoring the severity of the flaw.

Herrera and Plasket stressed the importance of a holistic approach to security, addressing both hardware and software vulnerabilities to ensure comprehensive protection.

Vulnerabilities in Amazon Machine Images (AMIs)

Matei Josephs, Senior Security Researcher and Founder of HiveHack, discussed the significant vulnerabilities associated with Amazon Machine Images (AMIs) and their broader implications for cloud security. He highlighted the risks posed by public AMIs, which can expose sensitive information like AWS access keys and source code, potentially leading to severe breaches such as unauthorized access to corporate AWS environments.

"We found this public AMI and within that AMI... a Stripe API key which gave us access to this Stripe account with about $30,000 attached to it," Josephs recounted. "That was a pretty fun one for us. So we found this public AMI and within that AMI there is a supposedly private Git repository. Within that Git repository we found some secrets including the Stripe API key. Now that was very interesting because what that meant is that we could have transferred money at will," Josephs recounted, emphasizing the ease with which they could have exploited this vulnerability.

He emphasized the critical need for organizations to follow best practices for securing cloud environments, warning that even minor oversights, like leaving sensitive data in public AMIs, can lead to catastrophic security breaches.

Vulnerabilities in Microsoft Copilot and AI Tools

AI-driven tools like Microsoft Copilot offer significant productivity benefits but also introduce new security risks. Michael Bargury, Chief Technology Officer at Zenity, discussed how AI tools can be manipulated through techniques like prompt injection, where attackers can hijack the tool to execute commands or search for sensitive information using the victim's identity.

"Just by sending you an email or a Teams message… I use that as a way in and then I use prompt injection to completely take over Copilot on your behalf," Bargury warned.

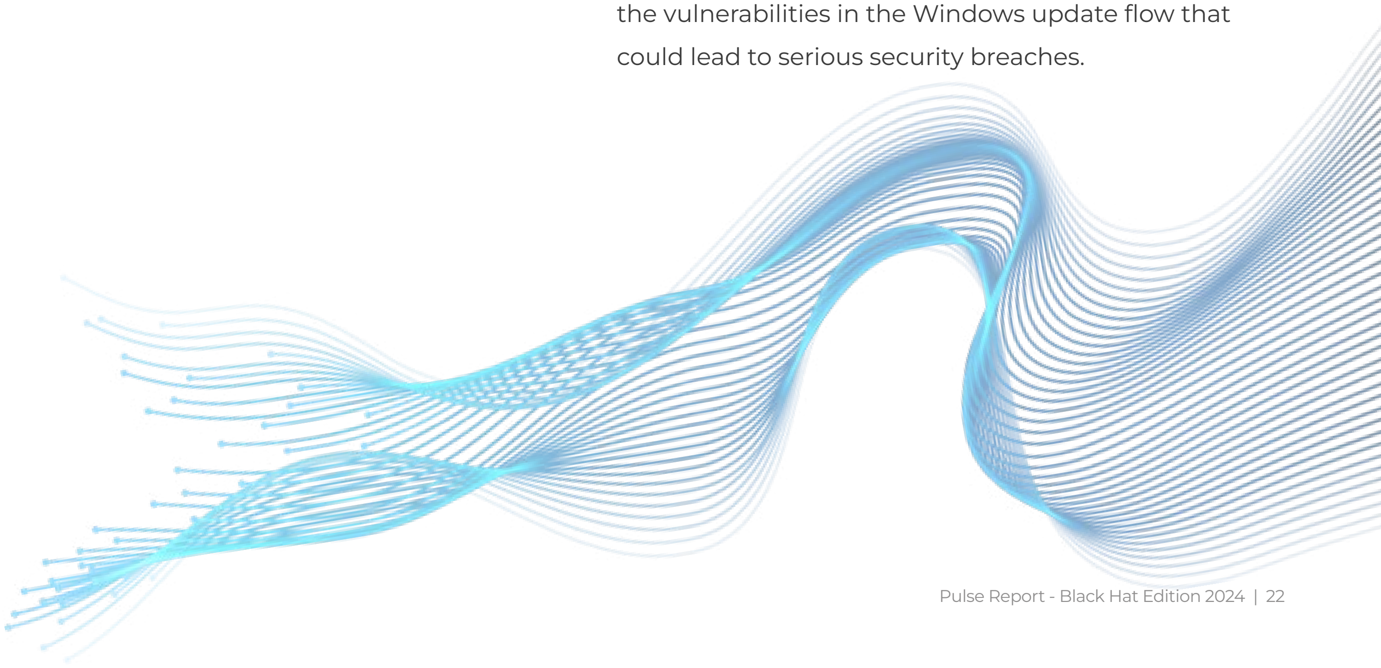
Bargury also warned about the dangers posed by Copilot Studio, where non-technical users can easily create bots that may introduce security risks, particularly through identity exploitation and misconfiguration. Additionally, he stressed the significant security threats from unauthorized actions that can be initiated via plugins, urging vigilance in securing AI applications, especially as their adoption in large enterprises grows rapidly.

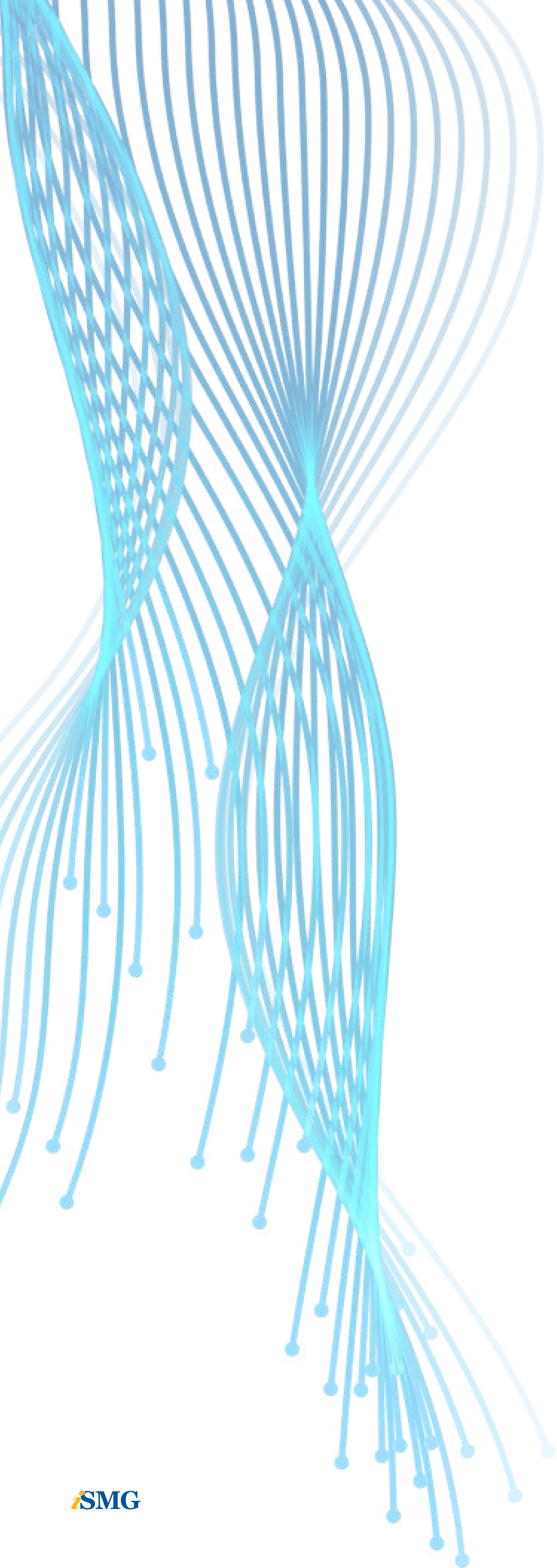
Black Lotus Attack and Downgrade Vulnerabilities

Alon Leviev, a security researcher at SafeBreach, highlighted the critical vulnerabilities exposed by the Black Lotus attack, particularly its ability to exploit downgrade vulnerabilities in Windows systems. Leviev explained that the attack leveraged an older vulnerability by downgrading the Windows Boot Manager, which allowed it to bypass secure boot protections even on fully updated machines. This capability raised significant concerns about the robustness of current security defenses against such sophisticated attacks.

"The main concern with Black Lotus… was the fact that it was able to bypass secure boot and fully updated machines," Leviev said, underscoring the severity of the issue. He went on to discuss the broader implications of such attacks, pointing out weaknesses in the Windows update process that could be exploited by attackers to downgrade key system components like kernels and drivers.

"What I found was that we have in the Windows Update… this user called trusted installer which is enforcing all of the updates," Leviev said. "But I found there's a specific registry key… not enforced to this user which I was able to control… to then control all of the update actions," Leviev said, highlighting the vulnerabilities in the Windows update flow that could lead to serious security breaches.





Conclusion

Key Lessons in Cybersecurity Vulnerabilities

The diverse vulnerabilities explored in this chapter reveal several critical insights for cybersecurity professionals:

- Persistence of Old Threats: Traditional vulnerabilities like SQL injection remain dangerous, underscoring the need for continued vigilance in basic security practices.
- Emerging Technologies, New Risks: From EV chargers to AI tools, new technologies introduce novel vulnerabilities, emphasizing the importance of security-first development.
- Expanding Attack Surface: The proliferation of IoT devices and cloud services has significantly broadened potential attack vectors, requiring a more comprehensive security approach.
- Sophistication of Modern Exploits: Attacks like Black Lotus demonstrate the complex, multi-layered nature of current threats, challenging traditional security measures.
- AI and ML Security Challenges: As highlighted by vulnerabilities in machine learning platforms, the line between data and executable code is blurring, creating new security paradigms.

Moving forward, cybersecurity professionals must:

1. Stay informed about both traditional and emerging threats.
2. Advocate for integrated security in all stages of technology development.
3. Adapt quickly to new technological paradigms and their associated risks.

The universe of cybersecurity vulnerabilities continues to evolve rapidly. By remaining adaptable and applying these lessons, professionals can better prepare to meet the challenges of securing our digital future.

Cybersecurity in Enterprises

This chapter examines the critical challenges facing enterprise cybersecurity in the digital age. It explores the rising threat of non-human identities in cloud environments and the double-edged impact of AI integration. Experts discuss the complexities of securing enterprise browsers, now as crucial as operating systems, and the vital role of advanced Network Detection and Response. The chapter also addresses the ongoing struggle to secure cloud environments and the influence of economic uncertainty on cybersecurity investments. It concludes by emphasizing the need for a holistic, adaptive approach to enterprise security in the face of rapidly evolving digital threats.

Cybersecurity in Enterprises

The digital transformation of enterprises has ushered in a new era of cybersecurity challenges. This chapter explores the critical issues at the forefront of enterprise cybersecurity, as identified by industry experts. We delve into the risks posed by the proliferation of non-human identities, the security implications of AI and large language models (LLMs), and the complexities of securing enterprise browsers and cloud environments. Additionally, we examine how economic uncertainties are shaping the cybersecurity landscape.

As traditional security measures prove insufficient, this chapter aims to provide insights into the evolving strategies needed to protect modern enterprises.

Adam Cheriki, CTO and Co-Founder of Entro Security. View the full interview here.

The Rise and Risk of Non-Human Identities

In the modern enterprise, the adoption of cloud services and automation has led to a significant increase in non-human identities—digital identities used by applications, services, and devices to communicate and perform tasks.

Adam Cheriki, CTO and Co-Founder of Entro Security, discussed the growing challenges associated with securing non-human identities as companies increasingly adopt cloud services and automated applications. He emphasized that the rise in non-human identities has created a vast, often unmonitored attack surface, making these identities prime targets for attackers. “A great quote from Gartner is that for every human identity there will be 45 non-human identities created. So easy for attackers to go and use them,” Cheriki said, highlighting the scale of the challenge and the ease with which attackers can exploit these unmonitored identities.

Cheriki further elaborated on the risks, noting that many security teams mistakenly believe that securing human identities alone is sufficient. However, non-human identities require dedicated solutions for monitoring and management, which existing tools have struggled to provide effectively.

“Many CISOs and security teams thought that securing the human identities would also secure the non-human identities,” Cheriki said. “But it’s not like that. You need to secure your non-human identities and monitor them,” he said.

Proliferation of AI in Enterprises

The integration of AI into enterprise operations is accelerating, with large language models (LLMs) playing a key role in this transformation. Ravi Ithal, Co-Founder and CTO of Normalyze, discussed the rapid adoption of generative AI tools within large enterprises, emphasizing the growing reliance on off-the-shelf large language models (LLMs) provided by major cloud service providers such as AWS, Azure, and Google Cloud Platform. These tools are increasingly integrated into custom applications, where they are often augmented with proprietary data to enhance their functionality. Ithal highlighted the critical security and privacy concerns that arise from this widespread use of AI, particularly the risks associated with "shadow AI," where unsanctioned AI tools are employed within organizations without proper oversight, leading to potential exposure of sensitive data.

"We are seeing among our customers… mostly off-the-shelf LLMs that are offered by cloud service providers like AWS, Azure, and GCP," Ithal said, elaborating on how companies customize these models by integrating them with internal data repositories to create more tailored AI experiences.

Ithal also highlighted the dangers of shadow AI, where employees use AI tools without proper oversight, potentially exposing sensitive data. He stresses the importance of discovering and inventorying all AI tools within an organization to understand their usage and associated risks. "Discovery is the number one task for everyone," Ithal said, emphasizing the need for tools that can help security teams monitor AI instances and the data they access.

> Discovery is the number one task for everyone.
>
> **Ravi Ithal**
> Co-Founder and CTO of Normalyze, speaking on the need for tools that can help security teams monitor AI instances and the data they access.

Security and Privacy Concerns with LLMs

As AI becomes more embedded in enterprise environments, the security and privacy concerns associated with LLMs continues to grow. Ithal underscored the significant risks posed by these models, particularly in terms of data confidentiality and privacy. "The biggest concern, especially for enterprises, is the confidentiality and privacy of data that these LLMs are handling," Ithal said. He advocates for a layered approach to data security that addresses the semantic layer, where AI operates, as the final frontier in protecting sensitive information.

Securing Enterprise Browsers

John Wrobel, Chief Revenue Officer at Menlo Security, discussed the critical importance of securing enterprise browsers as they have evolved to become as complex and integral as operating systems. Wrobel emphasized that modern browsers are the primary interface through which users interact with the digital world, handling everything from work tasks to accessing sensitive data. This makes them a prime target for cyberattacks, and thus, they must be protected with the same level of scrutiny and security controls typically reserved for operating systems.

"If you think of what the user does... everything we do is within the browser," Wrobel said, highlighting the necessity of securing this crucial component of daily operations.

Wrobel further elaborated on Menlo Security's approach to browser security, which stands out by allowing organizations to enhance the security of their existing browsers rather than replacing them. This method involves rendering all active content in the cloud before it reaches the user's device, effectively preventing malware and other threats from penetrating the browser environment.

"At Menlo, we believe that we can turn your existing browser into an enterprise browser... we don't force you to replace your browser," Wrobel explained, stressing the importance of maintaining user familiarity while enhancing security.

He also touched on the tactics adversaries use to exploit common vulnerabilities in popular browsers like Chrome and Edge, noting that as more of users' time and tasks are conducted within these browsers, attackers have become increasingly sophisticated in targeting them. Wrobel emphasized the need for proactive security measures to mitigate these risks.

John Wrobel, Chief Revenue Officer at Menlo Security. View the full interview here.

> If you think of what the user does... everything we do is within the browser... It's millions of lines of code. It's as complex as an operating system.
>
> **John Wrobel**
> Chief Revenue Officer at Menlo Security

The Role of Network Detection and Response (NDR)

Brian Dye, CEO of Corelight, highlighted the critical role that Network Detection and Response (NDR) plays in modern cybersecurity practices. Dye emphasized that NDR provides the “ground truth” necessary for effective detection and response to cyber threats, such as ransomware.

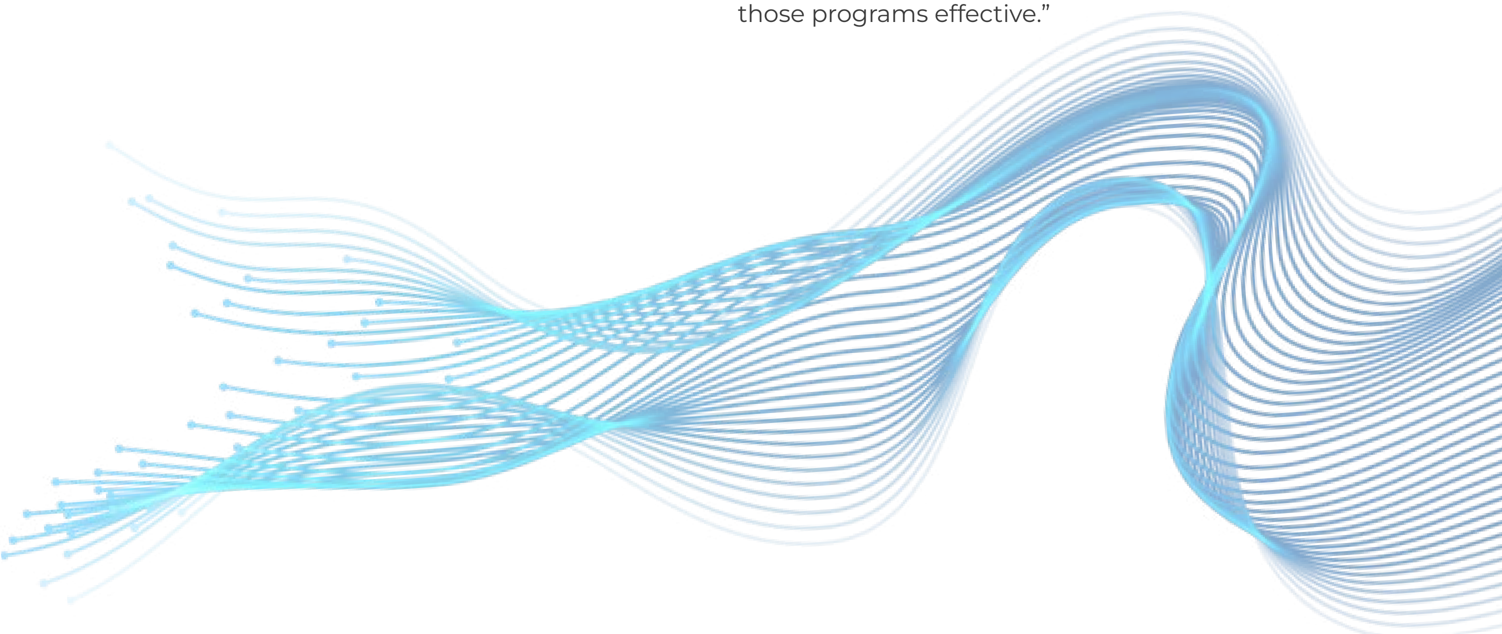
“The network really gives you ground truth of what’s happening. The ability to prove what the actual situation is, scope the real totality of the attack, and then take your decisions accordingly is really, really important,” he said. This visibility allows organizations not only to detect the different stages of an attack but also to accurately verify the extent of damage post-incident, ensuring a precise and informed response.

Dye also addressed the challenges of securing cloud environments, noting that while cloud services have become integral to many organizations, they present unique security difficulties. Specifically, he pointed out the limitations of native cloud security tools like Virtual Private Cloud (VPC) flow logs, which are not designed for thorough security analysis. A VPC Flow Log is a feature within Amazon Web Services (AWS) that allows users to capture information about the IP traffic going to and from network interfaces in a virtual private cloud. VPC Flow Logs provide detailed records of all network traffic, including the source and destination IP addresses, ports, protocol types, and the amount of data transferred.

“VPC flow logs… have all the same problems in the cloud that they’ve had on-premise for the last 20 years,” Dye said. “They are useful but they just weren’t designed for a security analyst,” he said, underscoring the need for more robust tools to effectively secure cloud-based systems.

Another key point Dye discussed was the importance of unified and consistent telemetry data for security operations. He argued that such consistency is vital for enabling advanced threat detection, automation, and the use of AI in Security Operations Centers (SOCs).

“What you really want to do for any modern SOC is drive your own in-house threat detection engineering, drive as much automation as you can,” he said. “Getting consistency and clarity in the underpinning data becomes essential to making all those programs effective.”



Economic Uncertainty and Its Impact on Cybersecurity

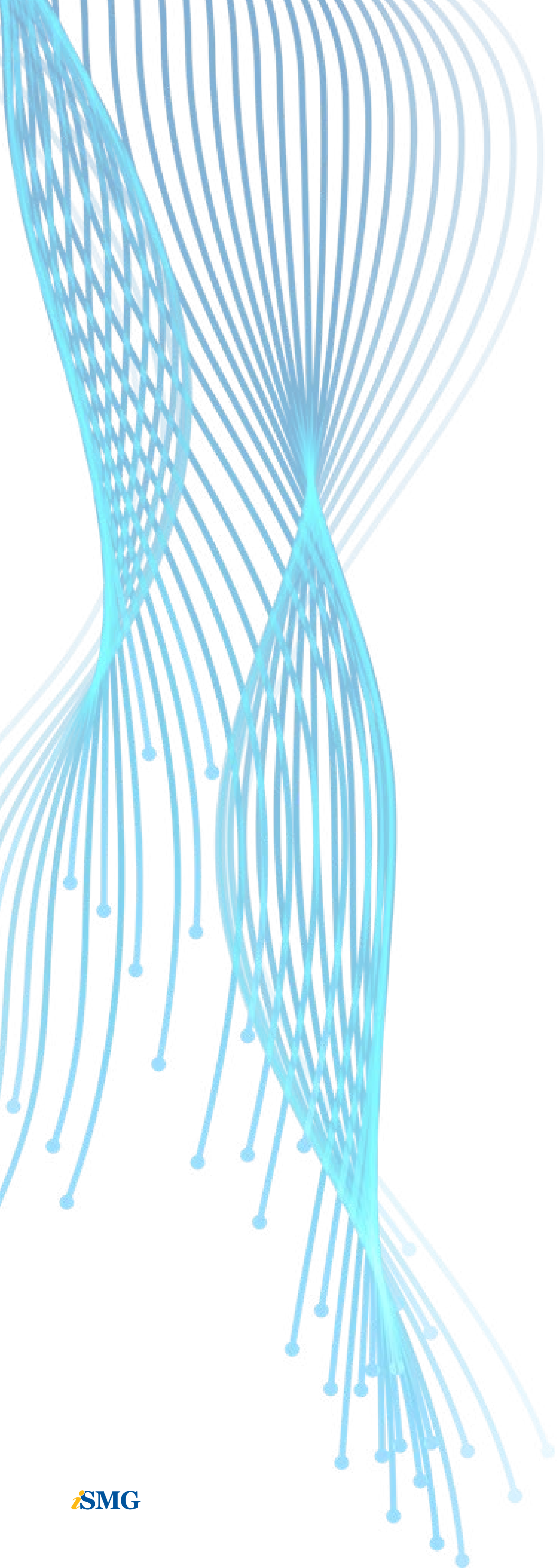
The current global economic uncertainty is having a significant impact on the cybersecurity sector, influencing investment decisions and market trends. Alberto Yépez, Co-Founder and Managing Director of Forgepoint Capital, discussed how mixed economic signals are affecting the cybersecurity industry. “I think there’s uncertainty because we’re seeing some signs of recession. We’re seeing some of the indicators from the Fed,” he said.

Yépez also highlighted the increasing recognition of cybersecurity as a critical business risk, leading to greater willingness among companies to invest in security. This is particularly important as the cybersecurity industry experiences consolidation and companies become more selective in their partnerships.

“The biggest existential threat to their well-being is a cyber attack or a cyber breach. Good news is now boards of directors are recognizing the importance and they are more willing to make investments,” Yépez said. “There’s so much noise in the market… they’re going to have to be very selective in who they partner with.”

Alberto Yépez, Co-Founder and Managing Director of Forgepoint Capital. View the full interview here.

> The biggest existential threat to their well-being is a cyber attack or a cyber breach. Good news is now boards of directors are recognizing the importance and they are more willing to make investments.
>
> **Alberto Yépez**
> Co-Founder and Managing Director of Forgepoint Capital

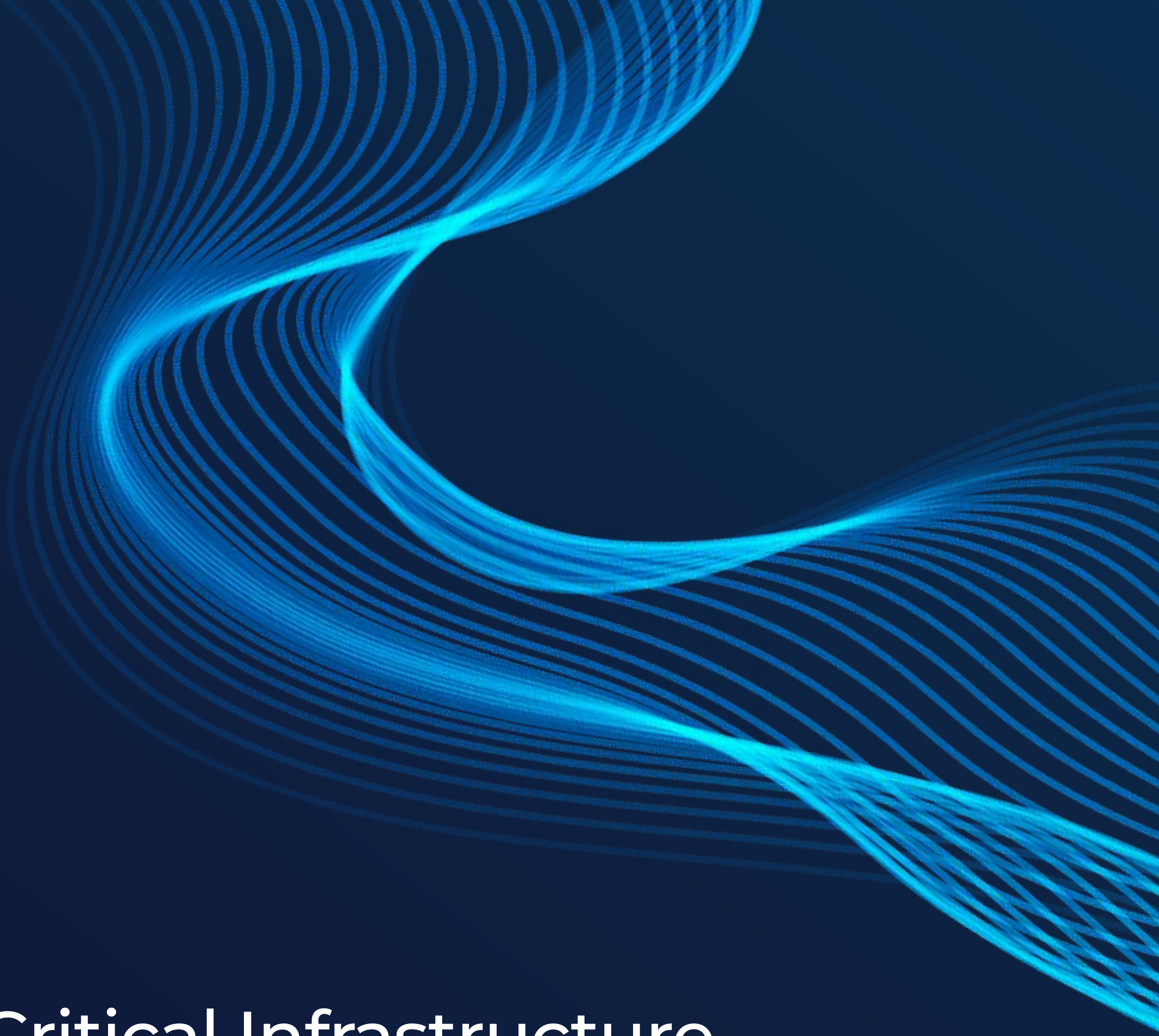


Conclusion

The landscape of enterprise cybersecurity is rapidly evolving, driven by technological advancements and changing business practices. Key takeaways from this chapter include:

1. Securing and monitoring non-human identities has become critical, as they often outnumber human users in modern enterprises.
2. Artificial intelligence and large language models present both significant security risks and opportunities, making them a double-edged sword.
3. Ensuring robust browser security is essential, especially in an era where browsers operate like de facto operating systems.
4. Advanced network detection and response are necessary for achieving comprehensive visibility into threats across the network.
5. Cloud environments continue to pose challenges for security, with traditional tools frequently proving inadequate.
6. Economic uncertainty is impacting both cybersecurity investments and strategies, influencing the direction of enterprise security planning.

As cyber threats grow in sophistication, enterprises must adopt a proactive, holistic approach to security. This involves not only implementing advanced technologies but also fostering a culture of security awareness and continuous adaptation. The future of enterprise cybersecurity lies in the ability to anticipate and respond to emerging threats while balancing security needs with business objectives.



Critical Infrastructure and Ransomware

This chapter explores the escalating threats to critical infrastructure and the evolving landscape of ransomware attacks. Experts highlight the grave dangers faced by power grids and essential services, particularly in conflict zones like Ukraine. The discussion reveals how ransomware groups often surpass Fortune 100 companies in cybersecurity measures. The chapter examines the geopolitical dimensions of these threats, including state-actor involvement, and the shifting tactics of ransomware groups toward multi-layered extortion. It concludes by emphasizing the crucial need for resilient defense strategies and international cooperation to protect vital systems underpinning modern society.

Critical Infrastructure and Ransomware

Critical infrastructure, which underpins modern society, faces significant threats from adversarial nations. Joe Marshall, Senior Security Strategist at Cisco Talos, underscored the grave threat that ransomware poses to critical infrastructure, particularly in the context of the ongoing conflict in Ukraine. Marshall highlighted how adversaries, notably in the Ukrainian conflict, are increasingly targeting essential services like power grids, amplifying the dangers these attacks pose.

"Power grid work at its best is incredibly dangerous. Now do all of that while you're being shot at and you can see how the danger just goes through the roof because in this particular case we know that the Russian adversary is specifically targeting critical infrastructure," Marshall said, emphasizing the heightened risks when critical infrastructure is under direct attack.

Joe Marshall, Senior Security Strategist at Cisco Talos. View the full interview here.

Marshall's insights are grounded in his experience with Project Power Up, an initiative aimed at maintaining power in Ukraine during the war. This project revealed not only the direct physical dangers but also the broader strategic risks associated with the disruption of critical infrastructure through cyberattacks. The power grid, as a vital component of national security and public safety, becomes a prime target for ransomware and other forms of cyber aggression, making it essential for innovative and resilient defense strategies.

Marshall also noted the broader implications of these threats, stressing the importance of learning from global security challenges, particularly from regions that face constant threats to their infrastructure. "If you want the straight ground truth you don't go to the most secure; you go to the least secure who struggle to keep the power on," he said. "You can learn so much and bring so many of those lessons back to where you are," he said, indicating that lessons learned in high-risk environments can be invaluable in strengthening defenses elsewhere.

> If you want the straight ground truth you don't go to the most secure; you go to the least secure who struggle to keep the power on.
>
> **Joe Marshall**
> Senior security strategist, Cisco Talos

Comparison of Ransomware Panels and Fortune 100 Companies

Ransomware groups have become increasingly sophisticated in securing their operations, often surpassing the security measures of even the largest enterprises. A ransomware panel typically refers to an online platform or dashboard used by cybercriminals to manage and monitor their ransomware campaigns. These panels are part of the infrastructure that supports ransomware activities, providing a centralized interface for the attackers to control and coordinate their malicious operations.

Vangelis Stykas, CTO of Atropos, noted that ransomware panels often have fewer vulnerabilities than those found in the web presence of Fortune 100 companies. "The web presence of Fortune 100 companies is way worse than that of the ransomware panels that I checked on," Stykas said. He attributes this to the significant investment ransomware groups make in their security, which allows them to operate with a high degree of protection against counterattacks.

Stykas also discussed the ethical dilemmas associated with targeting these ransomware groups. He views his role as similar to that of a "Socratic fly," aiming to disrupt the status quo imposed by these malicious actors without overstepping legal boundaries. "I always wanted to be what in Greece we call the Socratic fly... I wanted to give those people a taste of their own medicine," Stykas said.

Vangelis Stykas, CTO of Atropos. View the full interview here.

> The web presence of Fortune 100 companies is way worse than that of the ransomware panels that I checked on.
>
> **Vangelis Stykas**
> CTO of Atropos

Impact and Vulnerability of Critical Infrastructure

The vulnerability of critical infrastructure to cyberattacks is a growing concern, particularly as state actors like China and Russia become more aggressive in their tactics. Bryson Bort, Founder and CEO of SCYTHE, emphasized that critical infrastructure, while resilient by design, was not built to withstand modern cyber threats. "This critical infrastructure is what underpins our modern society... and it is not something that we should take for granted," Bort said.

Bort discussed the longstanding presence of adversarial nations within U.S. critical infrastructure, noting that these intrusions are part of broader geopolitical strategies. He warned that cyberattacks could be used to weaken U.S. military responses in conflicts, such as those involving Taiwan. "Cyber is just a means to an end. It is one where I can wake up in Beijing and do something to some place in Dallas," Bort said.

Bort mentioned that while these cyber operations may not always directly involve critical infrastructure, they could exploit other vulnerabilities. "My belief is that what we do see may not necessarily require critical infrastructure, but is more likely that there are other weak points in US military force projection," he said.

Bryson Bort, Founder and CEO of SCYTHE. View the full interview here.

> "We've had adversarial nations inside of our critical infrastructure... That's been the Chinese, that's been the Russians."
>
> **Bryson Bort**
> Founder and CEO of SCYTHE

Ransomware Group Stability

Rob Boyce, Global Cyber Resilience Lead at Accenture, provided insights into the stability and tactics of ransomware groups, emphasizing the critical importance of assessing these factors when organizations face ransomware threats. Boyce explained that evaluating the credibility and reliability of ransomware groups is complex but crucial for decision-making, particularly when considering whether to pay a ransom. “There’s always a lot of determining factors to be able to make a legitimate assessment on whether you can trust the threat actor, whether they’re going to be able to follow through with what they promised you,” Boyce noted. To assist with this, Accenture has developed a maturity matrix designed to assess these aspects of ransomware groups.

He also discussed the evolving nature of ransomware tactics, “We’re now seeing a shift from this totally focused on extorting the victim organization to going to now extort C-level executives. We’ve also seen evidence and trends of even going further downstream to say extort the victims of say healthcare breaches,” Boyce explained, illustrating the increasingly personalized and aggressive approaches taken by these groups.

Regarding the longevity of ransomware groups, Boyce pointed out that the financial motivations and pressures from law enforcement often lead these groups to seek exit strategies, such as large payoffs followed by dissolution or rebranding. “As they become more in the spotlight, it’s easier for them to think, ‘Okay, we need to now think of an exit strategy so that we can just get law enforcement off our backs,’” Boyce said, highlighting the pragmatic and strategic decisions these groups make in response to increasing scrutiny.

Additionally, Boyce touched on the dynamics within Ransomware-as-a-Service (RaaS) groups, noting that they are now offering more support and incentives to their affiliates, which could contribute to greater stability and longevity of these operations. “Now they’re giving them the majority [of the ransom] right? So they’re building more trust and more confidence within their affiliate groups. Maybe we might start seeing some of these groups stay around longer because there’ll be less concerns from the affiliates,” Boyce said.

Finally, Boyce emphasized the role of nation-state support, particularly from Russia, in bolstering the stability of ransomware groups. He pointed out that operating within a nation that offers protection from prosecution allows these groups to act more boldly and aggressively.

“The fact that they can operate within a construct or within a nation that allows them to do that with very limited concerns from prosecution and law enforcement…is just giving them the platform to be more successful in some ways or at least more bold in their attacking,” Boyce said, underscoring the geopolitical factors that influence ransomware group stability.

Conclusion

The convergence of ransomware and critical infrastructure attacks presents a formidable challenge to global cybersecurity. Key insights from this chapter include:

1. The increasing sophistication of ransomware groups, often surpassing the security measures of major corporations.
2. The vulnerability of critical infrastructure to cyber threats, despite its inherent resilience to physical challenges.
3. The evolution of extortion techniques, moving beyond data encryption to multi-layered pressure tactics.
4. The geopolitical dimensions of these threats, with state actors leveraging cyber capabilities for strategic advantage.
5. The importance of assessing ransomware group stability and credibility in response strategies.

As these threats continue to evolve, a proactive, multi-faceted approach to cybersecurity becomes crucial. This involves not only technological solutions but also strategic preparedness, international cooperation, and a deeper understanding of adversary tactics. The future of protecting critical infrastructure lies in our ability to anticipate, adapt to, and counteract these ever-changing threats, ensuring the resilience of the systems that underpin modern society.

Legal and Regulatory Challenges

This chapter examines the evolving legal landscape in cybersecurity, focusing on unprecedented legal risks for CISOs. It analyzes the groundbreaking SolarWinds case, setting a precedent for CISO liability in securities fraud. The discussion covers new SEC disclosure regulations and their implications for cybersecurity professionals. Experts explore the shifting U.S. cybersecurity strategy, emphasizing private sector responsibility and global policy alignment. The chapter concludes by highlighting the critical need for enhanced state-level cyber capabilities and closer collaboration between legal and security teams in this new regulatory environment.

Legal and Regulatory Challenges

The cybersecurity industry is undergoing a seismic shift, not just technologically, but also from a legal and regulatory perspective. This chapter explores the emerging legal challenges facing Chief Information Security Officers (CISOs) and cybersecurity professionals. We examine the groundbreaking implications of recent legal cases, particularly the Solar Winds case, which sets a precedent for CISO liability.

Additionally, we delve into the risks associated with new SEC disclosure regulations and the evolving U.S. cybersecurity strategy. Through expert insights, this chapter illuminates the complex interplay between cybersecurity practices and legal accountability, highlighting the need for a new approach to risk management in the digital age.

> It's the first time ever that a federal court has blessed the theory of intentional securities fraud liability under Securities and Exchange Act 10b- 5 against a CISO.
>
> **Jess Nall**
> Partner, Baker McKenzie LLP

Impact of SEC Legal Theory Validation on CISOs

The validation of the SEC's legal theory in the ongoing SolarWinds case marks a pivotal moment for CISOs across the industry. Jess Nall, a Partner specializing in Cyber and AI at Baker McKenzie LLP, emphasized that this case is the first time a federal court has supported a theory of securities fraud liability against a CISO.

"It's the first time ever that a federal court has blessed the theory of intentional securities fraud liability under Securities and Exchange Act 10b-5 against a CISO," Nall said. This decision has significant implications for the cybersecurity community, potentially emboldening the SEC to pursue similar charges in future cases.

For Tim Brown, the CISO of SolarWinds, this development worsens the risk profile of his case. Nall explained that with the court allowing the SEC's theory to proceed, defending the case becomes more challenging, and the possibility of facing a jury trial increases the risks for Brown. "Now that the court has essentially allowed this theory of intentional securities fraud to go forward against him, it's going to make it more difficult to defend the case overall," Nall said.

Legal Risks Associated with SEC Disclosures

The introduction of new SEC disclosure regulations poses additional legal risks for CISOs, particularly under Regulation S-K, Rule 105. These regulations require public companies to disclose detailed cybersecurity information in their filings, with much of the information coming from the information security team. Nall warned that CISOs could be held liable if any inaccuracies in these disclosures are later uncovered, even if they were not directly responsible for the final filings. “If a problem happens… that’s going to bounce back on the CISO for the most part,” Nall said, highlighting the increased accountability placed on cybersecurity professionals under these new regulations.

To protect themselves, Nall advises CISOs to secure indemnity agreements and ensure robust coverage under Directors & Officers (D&O) insurance. She also stresses the importance of maintaining vigilant internal communications and documentation to safeguard against potential legal issues in the future. “Making sure that you take a note to self sometimes in an appropriate case… so that later on down the line if the government does launch an investigation… you’ll be able to show that the CISO is not the person at fault,” Nall recommended.

Jess Nall, a Partner specializing in Cyber and AI at Baker McKenzie LLP. View the full interview here.

> If a problem happens… that’s going to bounce back on the CISO for the most part.
>
> **Jess Nall**
> Partner specializing in Cyber and AI at Baker McKenzie LLP

US Cybersecurity Strategy

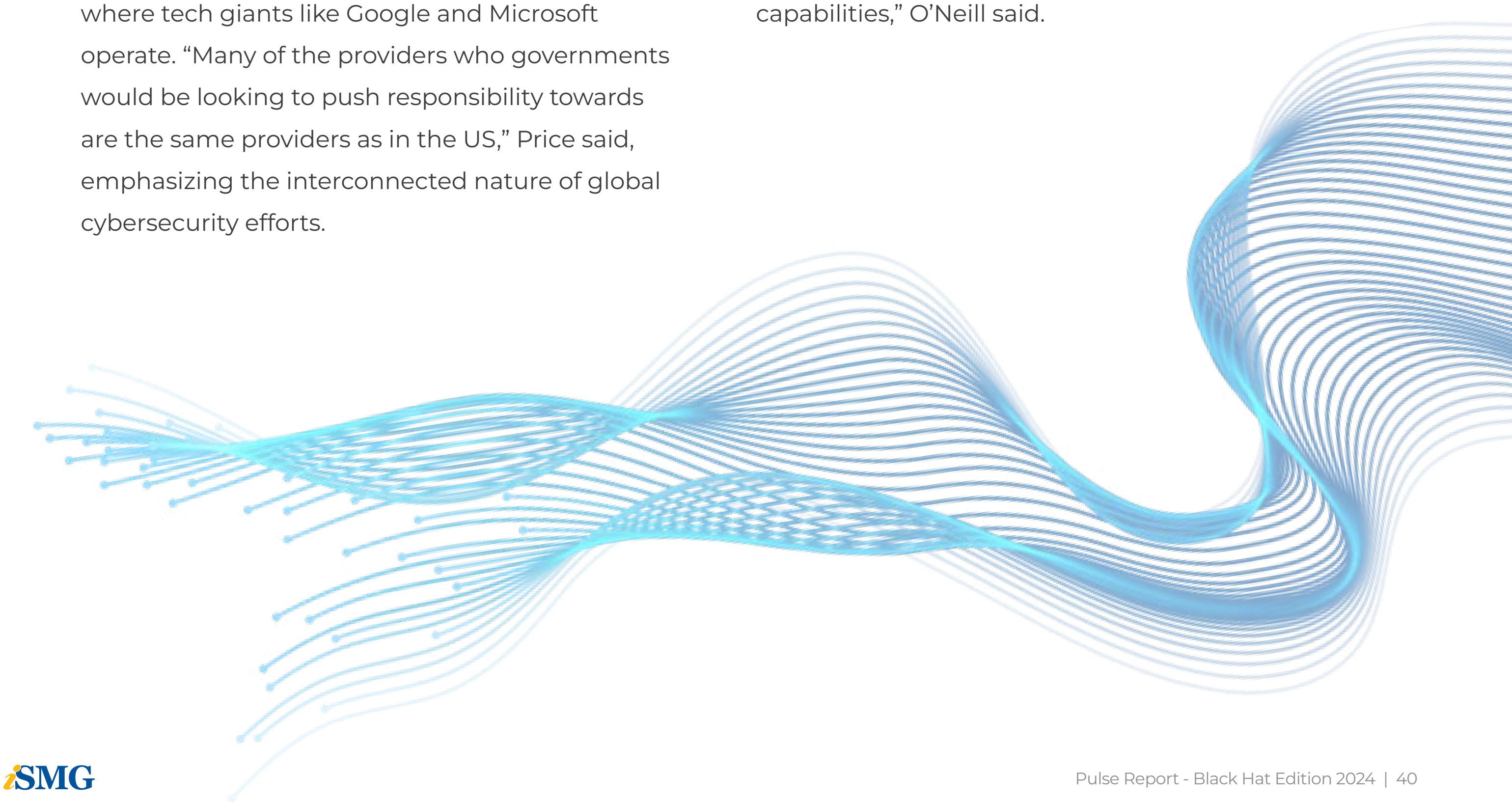
The U.S. cybersecurity strategy has increasingly focused on shifting the responsibility for cybersecurity to entities with the most capability, particularly large corporations. Alex O'Neill, a National Security Researcher formerly with Harvard's Belfer Center, explained that this approach is central to the 2023 U.S. cybersecurity strategy, which aims to incentivize private sector investment in cybersecurity through economic measures such as tax incentives and workforce development. "One of the key themes of the 2023 US strategy… is shifting the narrative and policy around who should be responsible and accountable for cybersecurity," O'Neill said.

In a global context, the U.S. approach contrasts with strategies adopted by other countries, which often rely on partnerships with the U.S., especially where major tech companies are involved. Lachlan Price, a student at Harvard Kennedy School and MIT Sloan School of Management, noted that many international cybersecurity strategies are closely aligned with the U.S., particularly in countries where tech giants like Google and Microsoft operate. "Many of the providers who governments would be looking to push responsibility towards are the same providers as in the US," Price said, emphasizing the interconnected nature of global cybersecurity efforts.

Critical Infrastructure Protection

Critical infrastructure protection remains a central focus of national cybersecurity strategies, with varying approaches taken by different countries. In Australia, for example, the Security of Critical Infrastructure Act places all critical infrastructure regulations into a single framework, although this approach has its limitations. "In Australia, there's the security of critical infrastructure Act which effectively harmonizes all critical infrastructure regulations into this one act. However, the downside is those protections are not tailored to the sector," Price said.

In the U.S., the strategy includes building stronger cyber capabilities at the state and local levels, recognizing that incidents often first emerge at these levels and that quick responses are crucial. O'Neill emphasized that while the U.S. has invested heavily in federal cyber capabilities, there has been underinvestment in state, local, tribal, and territorial capabilities. "The US does an amazing job of investing in its cyber capabilities at the top level federally. We think there's been a little bit of underinvestment in building out those state, local, tribal, territorial capabilities," O'Neill said.



Conclusion

The legal and regulatory landscape of cybersecurity is rapidly evolving, presenting new challenges and responsibilities for cybersecurity professionals. Key takeaways from this chapter include:

1. The Solar Winds case sets a significant precedent, potentially increasing legal liability for Chief Information Security Officers.
2. New SEC disclosure regulations heighten risks, requiring cybersecurity professionals to maintain thorough documentation and communication.
3. The U.S. cybersecurity strategy is shifting toward holding the private sector more responsible and accountable for security measures.
4. U.S. cybersecurity policies have global ramifications, especially in the protection of critical infrastructure.
5. Strengthening cyber capabilities at state and local levels is crucial to supporting federal cybersecurity efforts.

As the legal framework continues to develop, cybersecurity professionals must adapt their practices to mitigate legal risks while maintaining effective security measures. This evolving landscape demands not only technical expertise but also a deep understanding of legal and regulatory requirements. Moving forward, close collaboration between legal and cybersecurity teams will be crucial in navigating this complex terrain, ensuring both robust security and legal compliance in an increasingly scrutinized digital environment.

Emerging Threats and Red Teaming

This chapter delves into cutting-edge cyber threats, focusing on real-time deepfakes and sophisticated social engineering tactics. Experts discuss the alarming rise of AI-driven impersonation in financial fraud and network compromise. The chapter explores SIM swapping as a growing threat to multi-factor authentication, particularly targeting IT help desks and executives. It examines the broader implications of these emerging threats for organizational security and debates the effectiveness of deepfakes in misinformation campaigns. The chapter concludes by emphasizing the need for both advanced technological solutions and robust, process-based security measures.

Emerging Threats and Red Teaming

The cybersecurity threat environment is evolving at an unprecedented pace, with emerging threats pushing the boundaries of traditional defense mechanisms. This chapter delves into the cutting-edge challenges faced by organizations, focusing on real-time deepfakes, SIM swapping, and sophisticated social engineering tactics.

Advancement and Impact of Real-Time DeepFakes

Real-time deepfakes have significantly elevated the threat level in social engineering attacks. Brandon Kovacs, Senior Red Team Consultant at Bishop Fox, explained that these AI-driven deep fakes enable attackers to convincingly impersonate trusted figures within organizations, leading to serious security breaches.

“Back in June, someone cloned the chief financial officer of a multinational bank and instructed [the victim] to send a $25 million wire transfer on a live video call. Turns out it wasn’t actually the CFO, it was a real-time deepfake,” Kovacs said, highlighting the alarming authenticity these technologies can achieve.

The security implications for organizations are profound. Real-time deepfakes can be used not only for financial theft but also to compromise IT networks by impersonating key personnel. “It’s not just about stealing money. People could use this to compromise networks,” Kovacs noted. Attackers could clone IT help desk employees to disable accounts or reset passwords, he said.

Brandon Kovacs, Senior Red Team Consultant at Bishop Fox. View the full interview here.

> It’s not just about stealing money. People could use this to compromise networks.
>
> **Brandon Kovacs**
> Senior Red Team Consultant at Bishop Fox, on the implications of deepfake attacks.

SIM Swapping and Social Engineering

SIM swapping has emerged as a popular tactic among sophisticated crimeware groups, allowing them to bypass multi-factor authentication (MFA) and gain unauthorized access to sensitive accounts. Sherrod DeGrippo, Director of Threat Intelligence Strategy at Microsoft, explained that this technique is particularly effective against IT help desks and executives.

"SIM swapping has become a really popular method for... operationalized crimeware groups. They can then get those password codes and log in as that particular user... it's a significant problem primarily because there aren't a lot of good ways to protect from it," DeGrippo said, emphasizing the challenge of defending against this tactic.

She further explained that SIM swapping is often used in conjunction with social engineering, where attackers exploit human psychology—such as urgency, habit, and emotion—to deceive victims into divulging information or performing actions that compromise security. This combination makes SIM swapping a particularly potent and difficult-to-defend threat, especially as it targets not just individuals, but also IT help desks and executives who have access to critical systems.

DeGrippo's insights underline the need for stronger, hardware-based authentication methods, as traditional SMS-based MFA can be easily undermined by SIM swapping. The threat posed by SIM swapping reflects broader vulnerabilities in how organizations implement and manage authentication, making it a significant focus area for improving cybersecurity defenses.

Security Implications for Organizations

Emerging threats like deepfakes extend beyond financial fraud to the broader security of corporate environments. Kovacs highlighted that the impersonation of CEOs, CFOs, and other public figures can lead to significant security breaches if not properly mitigated. He stressed the importance of process-based controls, such as call-back verification, to counteract deepfake attacks. "Look up in your corporate directory that person's phone number and place a call back... that alone is a very effective process that mitigates these types of incidents," Kovacs said.

While technological solutions for deepfake detection are still in development, Kovacs said AI-driven tools will be crucial in the future. However, he noted that this will require continuous advancements in AI to keep pace with evolving deepfake technologies. "It really comes down to fighting AI with AI. You have to create a ton of deepfakes and then train models against those deepfakes. Then be able to detect them. I know companies are working on it but we're not there yet," Kovacs said.

Challenges with Deepfakes and Misinformation

Deepfakes and misinformation pose a complex challenge for organizations and society as a whole. Nathan Hamiel, Senior Director of Research at Kudelski Security, offers a contrarian view on the threat of deepfakes, arguing that while they are often discussed as tools for misinformation, their real-world impact on significant decisions is limited. "I've never really thought that was overly effective because of the way that people process information," Hamiel said, suggesting that deepfakes are more commonly used for creating memes rather than convincingly altering perceptions.

Hamiel also critiqued the tendency to "throw away the rule book" when new technologies like AI emerge, advocating instead for the application of established security principles. He underscored the importance of integrating AI security with traditional application security to ensure comprehensive protection. "If we take what we already know, we can get most of the way there and then we can look at the gap and say, 'Okay, what's left?'" Hamiel said.

Nathan Hamiel, Senior Director of Research at Kudelski Security. View the full interview here.

> If we take what we already know, we can get most of the way there and then we can look at the gap and say, 'Okay, what's left?'.
>
> **Nathan Hamiel**
> Senior Director of Research at Kudelski Security, speaking on the tendency to "throw away the rule book" when new technologies like AI emerge.

Conclusion

The landscape of emerging threats presents a complex challenge for cybersecurity professionals, necessitating a multifaceted approach to defense. Key takeaways from this chapter include:

1. The alarming authenticity and potential impact of real-time deepfakes in social engineering attacks.
2. The growing threat of SIM swapping as a means to bypass multi-factor authentication.
3. The importance of process-based controls and advanced authentication methods in mitigating these risks.
4. The potential role of AI in both perpetrating and defending against sophisticated attacks.
5. The need to balance new technological solutions with established security principles.

As these threats continue to evolve, organizations must adapt their security strategies to stay ahead. This involves not only implementing cutting-edge technologies but also fostering a culture of awareness and critical thinking. The future of cybersecurity lies in the ability to anticipate, detect, and respond to these emerging threats while maintaining a foundation of robust, time-tested security practices. As the digital landscape becomes more complex, the integration of advanced AI-driven tools with human expertise and traditional security measures will be crucial in building resilient defense systems against the ever-changing threat environment.

Security Testing and Resilience

This chapter explores innovative approaches to security testing and building cyber resilience. It analyzes lessons from the CrowdStrike outage, emphasizing the importance of staged rollouts and comprehensive code analysis. Experts advocate for advanced testing methods like fuzzing and symbolic execution to uncover hidden vulnerabilities. The discussion extends to the limitations of Software Bills of Materials (SBOMs) and the critical role of “shifting security left” in development. The chapter concludes by highlighting the growing importance of cyber resilience as a holistic, organization-wide strategy beyond mere prevention.

Security Testing and Resilience

Organizations are increasingly focused on improving security testing and resilience to better protect against emerging threats. This chapter examines critical insights from industry experts on fortifying defenses against sophisticated attacks.

The recent CrowdStrike outage offers valuable lessons on the importance of thorough testing and staged rollouts in preventing vulnerabilities from reaching production. David Brumley, CEO of Mayhem Security, emphasized that the root cause of the outage was a “ticking timebomb” bug that could have been caught with better code analysis practices.

“The root problem there was insufficient code analysis,” he said. This underscores the critical need for organizations to integrate more sophisticated testing methods, such as fuzzing and symbolic execution, to uncover bugs that standard testing might miss.

David Brumley emphasized three key lessons that CISOs should take away from the CrowdStrike outage:

1. The Importance of Staged Rollouts: Brumley stressed that rollouts should be done gradually over an extended period, rather than all at once. This helps in identifying and mitigating potential issues before they affect the entire system. He also advised against scheduling major rollouts during times of high activity, such as a Friday over a heavy travel weekend.
2. Thorough Testing: He highlighted the need for comprehensive testing, including dynamic analysis techniques like fuzzing, to catch vulnerabilities before they reach production. Insufficient testing was identified as a core issue in the CrowdStrike outage.
3. Robust Code Analysis: Brumley emphasized that the root cause of the problem was insufficient code analysis. He recommended that organizations invest in their developers to enhance security, as this would lead to better outcomes by identifying and fixing vulnerabilities earlier in the development process.

Brumley also discussed the limitations of relying solely on a Software Bill of Materials (SBOM) for security. While SBOMs are useful for identifying software components, they fall short in providing a comprehensive understanding of the attack surface or the vulnerabilities present. “What a software bill of materials says is here are the ingredients. It doesn’t say anything about the vulnerabilities. It doesn’t say which ones are on the attack surface,” Brumley said, advocating for continuous updates with the latest vulnerability data to enhance security effectiveness.

Brumley also emphasized the importance of “shifting security left” in the development process, which involves addressing vulnerabilities during development rather than after deployment.

Dynamic Analysis and Stress Testing for Software Security

Dynamic analysis and stress testing play critical roles in identifying vulnerabilities that may not be uncovered through standard testing methods. Brumley advocates for the use of techniques like fuzzing and symbolic execution to explore untested parts of the code, particularly those susceptible to issues like buffer overflows. "What I'm talking about is using fuzzing and symbolic execution and behavior analysis to stress test and explore parts of the program that really have not been touched before," Brumley said.

These methods are essential for finding and fixing vulnerabilities before they can be exploited, helping organizations to build more secure and resilient software systems. "So when you have a buffer overflow... it's in many cases zero clicks simply by putting a file on disk you can exploit these sort of things," Brumley said.

David Brumley, CEO of Mayhem Security. View the full interview here.

> What I'm talking about is using fuzzing and symbolic execution and behavior analysis to stress test and explore parts of the program that really have not been touched before.
>
> **David Brumley**
> CEO of Mayhem Security

Theresa Lanowitz, Chief Evangelist at LevelBlue, emphasized that cyber resilience involves the broader ability of an organization to continue operations during and after a cyber event rather than just focusing on prevention.

> Cyber resilience needs to be a whole organization issue. The CIO, CTO, and CISO need to work together to form a united front. It's not just a security issue.
>
> **Theresa Lanowitz**
> Chief Evangelist at LevelBlue

Cyber Resilience in 2024

Cyber resilience is increasingly recognized as a critical component of an organization's overall security strategy. Theresa Lanowitz, Chief Evangelist at LevelBlue, emphasized that cyber resilience involves the broader ability of an organization to continue operations during and after a cyber event, rather than just focusing on prevention.

"Seventy-two percent of governance teams do not understand what cyber resilience is. People will conflate cyber resilience with cybersecurity... but cyber resilience is not just a security issue; it's about getting the whole IT estate back up and functioning," Lanowitz said.

Lanowitz stresses that achieving true cyber resilience requires a whole-organization approach, with collaboration among the CIO, CTO, and CISO to ensure that business operations can be maintained even during disruptions.

"Cyber resilience needs to be a whole organization issue. The CIO, CTO, and CISO need to work together to form a united front. It's not just a security issue; it's about keeping the business running during and after a disruption," she said.

Conclusion

The insights gathered in this chapter underscore a fundamental shift in cybersecurity practices:

1. Thorough testing, including dynamic analysis and stress testing, is crucial for uncovering hidden vulnerabilities.
2. The CrowdStrike incident highlights the need for staged rollouts and comprehensive code analysis.
3. Ethical considerations complicate efforts to disrupt ransomware operations, requiring careful navigation of legal and moral boundaries.
4. Cyber resilience emerges as a critical organizational priority, demanding collaboration across IT, security, and business leadership.
5. A holistic approach to security, integrating testing and resilience strategies throughout the development lifecycle, is essential.

As digital threats continue to evolve, organizations must adapt their security strategies accordingly. This adaptation requires not just technological solutions, but also a shift in organizational culture and practices. By embracing comprehensive testing methodologies, ethical security practices, and organization-wide resilience strategies, businesses can better prepare for and withstand the challenges of an increasingly complex digital environment. The future of effective cybersecurity lies in this integrated, proactive approach to identifying vulnerabilities, mitigating risks, and ensuring operational continuity in the face of inevitable disruptions.

Innovations in Cybersecurity Tools

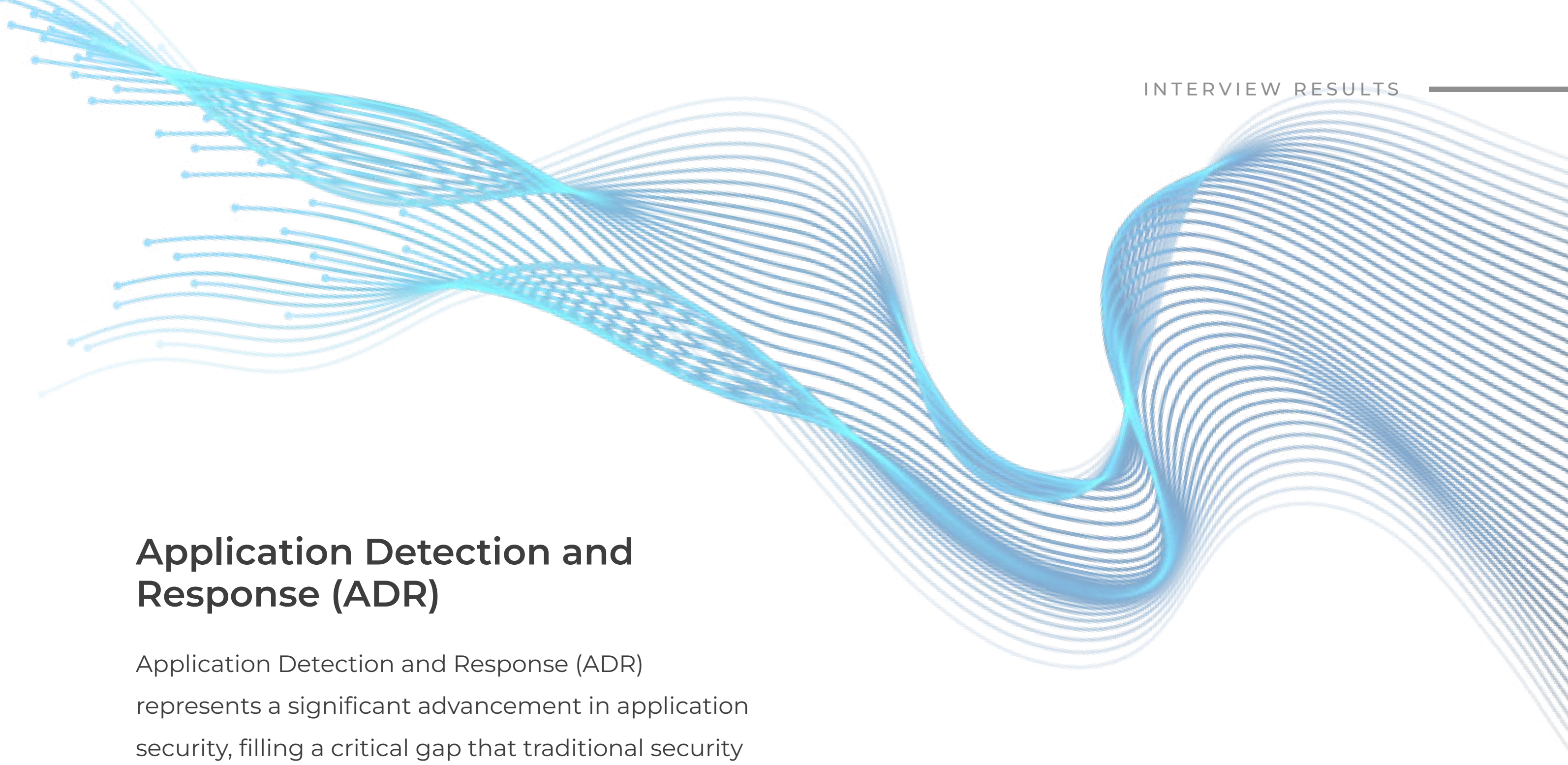
This chapter examines cutting-edge developments in cybersecurity technology. It introduces Application Detection and Response (ADR) as a crucial tool for protecting the often-overlooked application layer. The discussion covers the exploitation of Emergency Data Requests (EDRs) by cybercriminals and the emerging role of process mining in enhancing security operations. Experts highlight the growing importance of dynamic analysis and automated security testing in the era of AI-generated code. The chapter concludes by emphasizing the need for organizations to integrate these innovative tools into their security frameworks for comprehensive, responsive defense against evolving digital risks.

Innovations in Cybersecurity Tools

As digital threats grow in sophistication, the tools to combat them must evolve in tandem. This chapter examines cutting-edge developments in cybersecurity technology, focusing on four key areas: Application Detection and Response (ADR), the exploitation of Emergency Data Requests (EDRs), process mining in security operations, and advancements in dynamic analysis and testing automation. These tools represent the frontline of defense against an increasingly complex array of digital risks.

> Security operations really don't have very good visibility into the application layer. Unfortunately, that's where a lot of the risk is.
>
> **Jeff Williams**
> Founder and CTO of Contrast Security

Jeff Williams, Founder and CTO of Contrast Security. View the full interview here.



Application Detection and Response (ADR)

Application Detection and Response (ADR) represents a significant advancement in application security, filling a critical gap that traditional security tools often overlook. Jeff Williams, Founder and CTO of Contrast Security, introduces ADR as a new solution specifically designed to protect the application layer. "We're going to introduce a new acronym to the conversation: ADR—Application Detection and Response."

He emphasized that while traditional tools are designed to protect endpoints, servers, and clouds, ADR is specifically developed to detect and respond to unwanted behaviors within applications and APIs.

Williams also addressed the issue of visibility in application security, noting that most security operations currently lack insight into what occurs within applications. This gap leaves many risks unmanaged, as traditional security tools often do not cover the application layer adequately.

"Security operations really don't have very good visibility into the application layer. Unfortunately, that's where a lot of the risk is," he said, stressing the importance of enhancing visibility to manage these risks effectively.

> "ADR focuses down on that one percent. It's the ones that reach the vulnerabilities that we are targeting."
>
> **Jeff Williams**
> Founder and CTO of Contrast Security

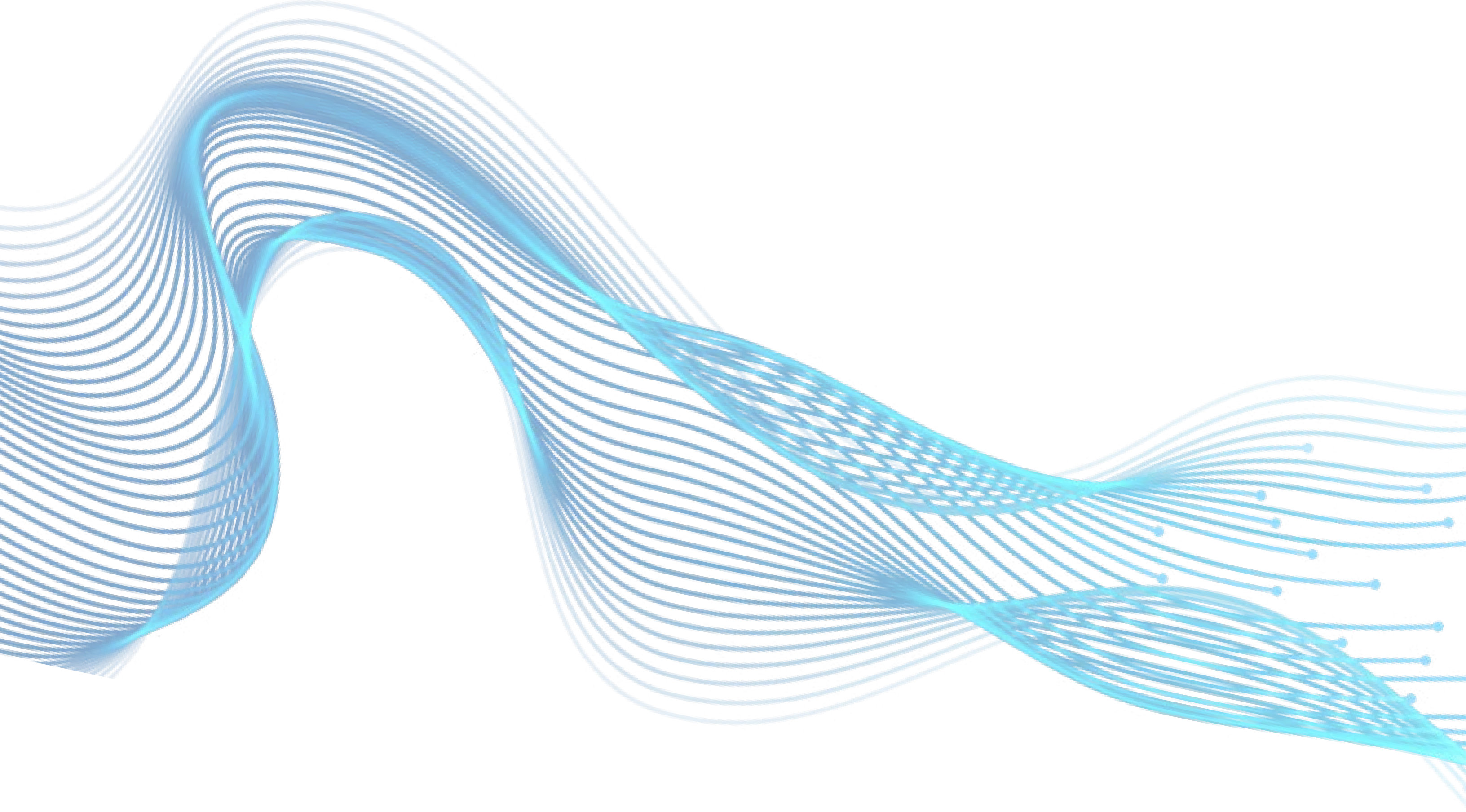
As applications have become more complex, so too have the attacks targeting them. Williams described how traditional vulnerabilities, such as SQL injection, now appear in more sophisticated and less visible parts of applications, like APIs and multi-tier systems, making detection and defense more challenging.

"The underlying vulnerabilities are fairly similar. But now they're in APIs or more complex applications... And the attackers have figured this out," Williams said, pointing to the evolving nature of application threats.

According to Williams, ADR involves creating detailed security blueprints for applications. These blueprints offer a comprehensive view of an application's attack surface, existing defenses, risky operations, and backend connections, providing actionable insights for security teams. "With our instrumentation-based approach we can generate a security blueprint of every application. It shows the full attack surface, the security defenses in place, the dangerous stuff each route does, and the backend connections," he said.

Integration with existing security tools is another key feature of ADR, ensuring that it can work seamlessly within an organization's broader security strategy. Williams highlighted successful integrations, such as with Splunk, to demonstrate how ADR can complement traditional security operations. "ADR generates telemetry about events and incidents," Williams said.

Finally, Williams emphasized that ADR differs from traditional security tools like Web Application Firewalls (WAFs) by focusing on identifying and responding to genuine incidents rather than overwhelming users with excessive event data. "Unlike a WAF where it's anything that looks like an attack... ADR focuses down on that one percent. It's the ones that reach the vulnerabilities that we are targeting," he said, underscoring ADR's effectiveness in managing the most critical security threats.



Exploitation of Emergency Data Requests (EDRs)

Emergency Data Requests (EDRs) are a legitimate tool used by law enforcement to obtain critical information during emergencies, but cybercriminals have found ways to exploit this process. Jacob Larson, Team Lead for Security Testing and Assurance at CyberCX, described how attackers compromise government email accounts to submit fraudulent EDRs, bypassing legal procedures and gaining unauthorized access to sensitive user data. “The process is called an emergency data request or an EDR… if a hacker can compromise a government email they can use that to verify themselves and then receive that information,” Larson said.

Larson also discussed the broader implications of these exploits, including the black market for government email accounts and the need for service providers to implement stronger verification processes. “I’ve seen threat actors sell government email addresses for as low as 70 dollars. I also found examples of U.S. Department of Justice and FBI email accounts that were compromised and were being used to submit fraudulent requests,” Larson said.

> The process is called an emergency data request or an EDR… if a hacker can compromise a government email they can use that to verify themselves and then receive that information.
>
> **Jacob Larson**
> Team Lead for Security Testing and Assurance at CyberCX

Role of Process Mining in Cybersecurity Operations

Process mining has emerged as a powerful tool for improving cybersecurity operations by providing detailed insights into the processes involved in vulnerability management. John Morello, Co-Founder and CTO of Gutsy, described how process mining helps organizations understand where delays occur in their security processes and how these delays impact the overall effectiveness of their vulnerability management efforts. “Process mining is really just a technique… to help organizations understand… what are the biggest vulnerabilities… and then… correlate what all the steps are in that process even as those steps go through a lot of dissimilar different technologies and teams,” Morello said.

Morello introduced the concept of a security process fabric, which integrates and normalizes data from various detection tools to provide a comprehensive view of an organization’s risk. This approach allows security teams to visualize and address the specific factors that delay remediation efforts, ultimately improving security outcomes.

Dynamic Analysis and Security Testing Automation

Chris Wysopal, Co-Founder and CTO of Veracode. View the full interview here.

> Around 30 to 40 percent of the code that's generated will have a vulnerability in it. It was trained on human generated code.
>
> **Chris Wysopal**
> Co-Founder and CTO of Veracode

Dynamic analysis and automated security testing are crucial for identifying and addressing vulnerabilities in software, especially as the pace of development accelerates. Chris Wysopal, Co-Founder and CTO of Veracode, underscored the importance of automation in both testing and remediation to keep up with the increased volume of code generated by AI tools. "You're going to get higher code velocity… so it makes automation even more of a requirement. So shifting left, building security testing into your repo pull request or into the IDE when you're cutting and pasting code, test it right there," Wysopal said.

Wysopal also highlighted the security risks associated with AI-generated code, noting that it often contains vulnerabilities similar to those found in human-generated code. He advocates for using specialized AI models trained on secure coding practices and stresses the need for continuous security testing throughout the development process.

Conclusion

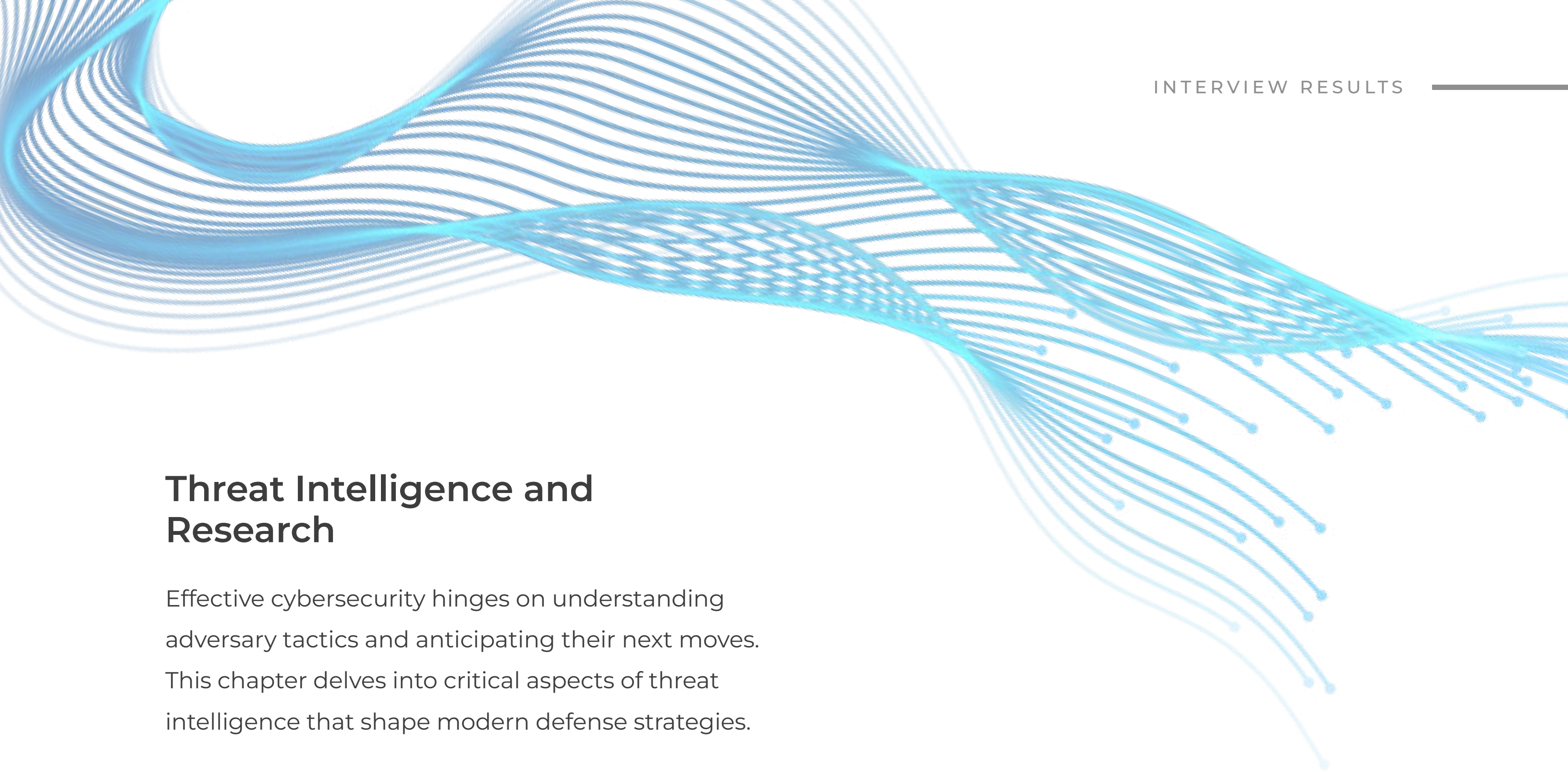
The innovations explored in this chapter signify a pivotal shift in cybersecurity practices:

1. Application Detection and Response (ADR) emerges as a crucial tool for protecting the often-overlooked application layer.
2. The exploitation of Emergency Data Requests (EDRs) highlights the need for robust verification processes in sensitive data handling.
3. Process mining offers valuable insights into vulnerability management, enabling more efficient security operations.
4. Dynamic analysis and automated testing become indispensable as AI-driven development accelerates code production.
5. The integration of these tools promises enhanced visibility, improved response times, and more comprehensive security coverage.

As technology continues to advance, the integration of these innovative tools into existing security frameworks will be crucial. Organizations must adapt their strategies to leverage these new capabilities, focusing on enhanced visibility, streamlined processes, and automated, continuous security testing. The future of effective cybersecurity lies in the intelligent application of these tools, combined with a proactive, integrated approach to identifying and mitigating digital risks. By embracing these innovations, organizations can build more resilient, responsive, and comprehensive defense systems capable of meeting the challenges of an ever-evolving threat environment.

Threat Intelligence and Research

This chapter delves into critical aspects of threat intelligence shaping modern defense strategies. It examines the role of intel brokers in breach forums and their impact on enterprise security. Experts discuss how cybercriminals exploit shell companies and jurisdictional differences to evade detection. The chapter highlights the importance of infrastructure intelligence in tracking resilient threat groups like Scattered Spider. It also explores the crucial role of Network Detection and Response (NDR) in providing visibility into complex attacks. The chapter concludes by emphasizing the need for a multifaceted approach to threat intelligence, combining network monitoring, infrastructure analysis, and proactive vulnerability management.



Threat Intelligence and Research

Effective cybersecurity hinges on understanding adversary tactics and anticipating their next moves. This chapter delves into critical aspects of threat intelligence that shape modern defense strategies.

Intel Brokers in Breach Forums

Intel brokers operating in breach forums have become a significant focus in the cybersecurity community due to their ability to sell highly sensitive information about large enterprises. Etay Maor, Chief Security Strategist at Cato Networks, explained that the credibility of these brokers is often bolstered by their status as moderators in these forums, which indicates a high level of trust within the criminal community.

“I think the reason for the focus on Intel brokers is the fact that he, assuming it’s a he, is a moderator in breach forums so he does have the reputation. You don’t get to a level of moderator if you haven’t performed good deals, if you haven’t shared information, if you are not trusted by that community,” Maor said.

Maor also highlighted the persistent challenge of organizations failing to patch known vulnerabilities like Log4j, which Intel brokers continue to exploit. “You have a whole number of these older vulnerabilities which threat actors are still taking advantage of. It really shows that number one, if they’re doing it, it means it works,” Maor said, underscoring the ongoing risks posed by unpatched systems.

> You have a whole number of these older vulnerabilities which threat actors are still taking advantage of. It really shows that number one, if they’re doing it, it means it works.
>
> **Etay Maor**
> Chief Security Strategist at Cato Networks

Role of Shell Companies and Jurisdictional Exploitation

Cybercriminals frequently use shell companies in jurisdictions with lax regulatory oversight to conceal their illegal activities, making it difficult for law enforcement to trace the true ownership and financial flows. Renée Burton, Vice President of Threat Intelligence at Infoblox, discussed how these shell companies are employed to sustain operations while complicating efforts to disrupt them.

“If your company is incorporated in specific countries… the company registry is going to be closed so you have no information of who’s owning a company. Trying to trace back the money… [is] almost impossible,” Burton said.

Burton also elaborated on the connection between cybercrime and human trafficking, noting that trafficked individuals are often coerced into working in illegal gambling operations and other online scams. This exploitation adds another layer of complexity to law enforcement’s efforts to dismantle these criminal networks.

Importance of Infrastructure Intelligence in Tracking Cyber Threats

Malachi Walker, a Security Advisor at DomainTools, emphasized the critical role of infrastructure intelligence in tracking and disrupting cyber threats, particularly in the context of dealing with resilient threat groups like Scattered Spider. Despite several high-profile arrests within the group, Scattered Spider has continued its operations, adapting its tactics to evade detection. Walker noted that the group's decentralized structure allows its members to operate in silos, making it challenging for law enforcement to dismantle the entire network.

"A lot of these Scattered Spider members are a little bit more decentralized. It's harder to connect one arrest to another individual who's also part of the campaign," Walker said, highlighting the difficulties posed by this lack of central leadership.

Walker pointed out that infrastructure intelligence, such as DNS data and domain registration patterns, is crucial in tracking these cyber threats. He explained that law enforcement can leverage these patterns to identify and disrupt threat actors, especially when they make operational security mistakes. "With Scattered Spider there's a lot of young kids who are going after it for financial motivations... and are slipping up a little bit more," Walker said, emphasizing how even small errors can be exploited to trace and mitigate cyber threats.

Furthermore, Walker underscored how understanding the history and context of domain registrations can significantly aid in incident response and remediation efforts. By analyzing domain creation dates and associated infrastructure, security teams can narrow down the time frame of an attack, allowing for more focused and effective responses. "If we can know when this domain was spun up then that narrows our window of when we were compromised," he said, underscoring the importance of timely and accurate infrastructure intelligence in defending against cyber threats.

Overall, Walker's insights underscore the importance of infrastructure intelligence in not only tracking and identifying cyber threats but also in informing proactive defense strategies that can prevent future incidents.

> If we can know when this domain was spun up then that narrows our window of when we were compromised.
>
> **Malachi Walker**
> Security Advisor at DomainTools

Conclusion

The exploration of threat intelligence and research in this chapter reveals several critical insights for cybersecurity professionals:

1. Intel brokers in breach forums pose a significant threat, leveraging their credibility to sell sensitive enterprise information.
2. Shell companies in lax jurisdictions complicate efforts to trace and disrupt cybercriminal operations.
3. Infrastructure intelligence, particularly DNS analysis, proves crucial in identifying and mitigating evolving threats.
4. The persistence of known vulnerabilities, like Log4j, underscores the ongoing challenge of basic security hygiene.

As cyber threats continue to evolve, the role of comprehensive threat intelligence becomes increasingly vital. Organizations must adopt a multifaceted approach, combining robust network monitoring, infrastructure analysis, and proactive vulnerability management. The future of effective cybersecurity lies in the ability to anticipate and adapt to emerging threats, leveraging advanced intelligence techniques to stay ahead of adversaries. By integrating these insights into their security strategies, organizations can build more resilient defenses, better equipped to navigate the complex and ever-changing threat environment.

Privacy, Data Leakage, and API Vulnerabilities

This chapter examines critical vulnerabilities threatening individual and organizational security. It explores the dangers of location data leakage in dating apps and widespread API vulnerabilities, highlighting the tension between user privacy and app functionality. Experts discuss the persistent threat of resilient cybercriminal groups and the challenges in disrupting their operations.

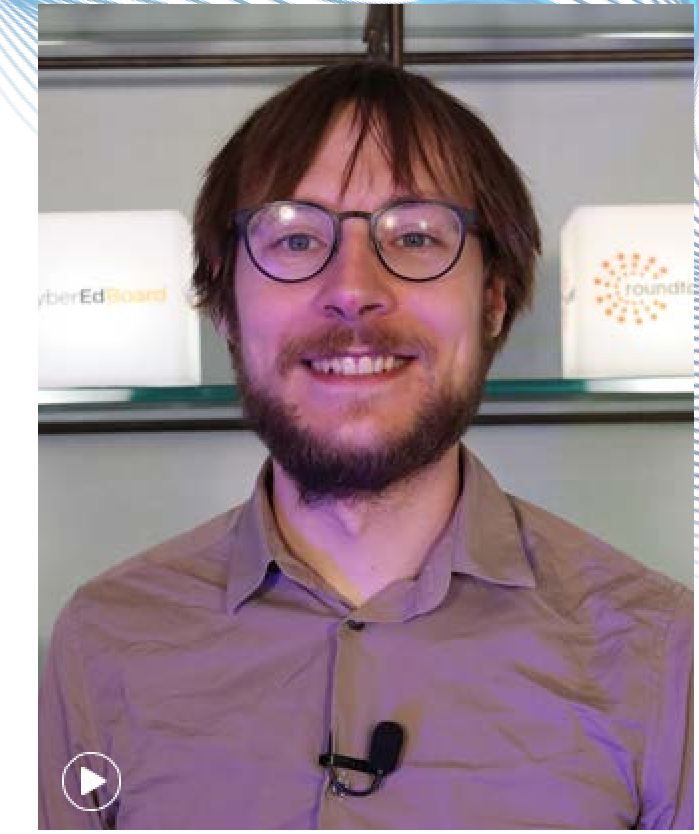
The chapter also addresses the ongoing struggles with responsible disclosure practices in the cybersecurity community. It concludes by emphasizing the need for a multifaceted approach to digital privacy and security, balancing technical solutions with regulatory frameworks and increased user awareness.

Privacy, Data Leakage, and API Vulnerabilities

In an era of pervasive digital connectivity, the boundaries between personal privacy and public exposure are increasingly blurred. This chapter examines critical vulnerabilities that threaten individual and organizational security. We explore the dangers of location data leakage in dating apps, the widespread issue of API vulnerabilities, the persistent threat posed by resilient cybercriminal groups, and the ongoing struggle with responsible disclosure practices.

Location Data Leakage

Victor Le Pochat, a Postdoctoral Researcher at KU Leuven, highlighted the severe risks associated with location data leakage from dating apps, stressing that such vulnerabilities can have dangerous real-world consequences. He emphasized that when users' precise locations are leaked, it can transform online threats into serious physical dangers, including stalking and harassment.



Victor Le Pochat, a Postdoctoral Researcher at KU Leuven, highlighted the risks associated with location data leakage from dating apps.

"When people's exact locations are being leaked, you run into issues where threats in the online world are being translated to the real world. That can really cause these kinds of physical harms that really threaten people's personal safety," Le Pochat said, underscoring the critical nature of this issue.

Le Pochat also discussed the economic incentives driving dating apps to collect and potentially leak this sensitive location data. He pointed out that selling this data is central to the business model of many apps, which are designed to connect users based on proximity. "I think that's an economic question. They are selling this data to other parties... this is basically their business model to collect this data," he said, indicating the financial motivations behind the continued collection of precise location data despite the associated risks.

Additionally, Le Pochat addressed the widespread issue of API vulnerabilities in dating apps, which can lead to the leakage of sensitive user information, even when such data isn't visible in the app's interface. "Out of the 15 most popular dating apps that we looked at, we saw that all of the apps leaked data. And we found the staggering amount of 99 data leaks."

In terms of solutions, Le Pochat advocated for strategies such as data minimization, which involves reducing the amount of data collected to limit what could potentially be leaked. “Data minimization essentially means the data that you don’t have and you don’t collect you can’t leak this data,” he said, acknowledging the tension between these security measures and the economic motives of the apps. These insights underline the critical need for improved data protection practices in the development and operation of dating apps.

API Vulnerabilities

API vulnerabilities represent another critical concern, particularly in the realm of dating apps where poorly protected APIs can lead to significant data breaches.

Karel Dhondt, a PhD Researcher at KU Leuven, emphasized the ongoing and pervasive issue of API vulnerabilities in dating apps, highlighting how these weaknesses can lead to significant data leaks. Dhondt noted that despite some progress, many apps remain vulnerable, with some repeating the same mistakes made years ago.

“Some apps like Tinder learned lessons from the past. So these were not vulnerable anymore,” Dhondt said. “But other ones like Bumble... have the same vulnerabilities that Tinder had 10 years ago.” This statement underscores the persistence of these issues and the failure of certain platforms to address and rectify long-standing security flaws in their APIs.

Karel Dhondt, a PhD Researcher at KU Leuven. View the full interview here.

> “Some apps like Tinder learned lessons from the past. So these were not vulnerable anymore. But other ones like Bumble... have the same vulnerabilities that Tinder had 10 years ago.”
>
> **Karel Dhondt**
> PhD Researcher at KU Leuven

Eduard Agavriloae, an AWS Offensive Security Expert, and Matei Josephs, Senior Security Researcher and Founder at HiveHack.

> We received only 10 responses for over 70 responsible disclosure emails. We also had to do some weird things like scheduling sales calls with companies just to tell them about the vulnerability.
>
> **Eduard Agavriloae**
> on the lack of responsiveness from organizations to vulnerability disclosures.

Challenges in Responsible Disclosure

Responsible disclosure remains a significant challenge in the cybersecurity community, with many organizations failing to respond adequately to reported vulnerabilities. Matei Josephs, Senior Security Researcher and Founder at HiveHack, and Eduard Agavriloae, an AWS Offensive Security Expert, expressed frustration with the current state of responsible disclosure. Josephs recounted an incident where a company initially ignored a reported vulnerability until further proof of its impact was provided. “We reported this Stripe API key and we didn’t get any response. We did get a response within a few hours from the CEO just CCing the CTO of the company as well,” Josephs said.

The lack of responsiveness from organizations not only delays the resolution of security issues but also increases the risk of these vulnerabilities being exploited. Agavriloae highlighted the broader problem.

“We received only 10 responses for over 70 responsible disclosure emails,” he said. “We also had to do some weird things like scheduling sales calls with companies just to tell them about the vulnerability.”

Conclusion

The examination of privacy issues, data leakage, and API vulnerabilities in this chapter unveils several critical insights:

1. Location data leakage in dating apps poses severe risks to personal safety, highlighting the tension between user privacy and app functionality.
2. Widespread API vulnerabilities across popular platforms underscore the persistent gap between security awareness and implementation.
3. The resilience of cybercriminal groups like Scattered Spider demonstrates the evolving nature of threats and the challenges in disrupting decentralized networks.
4. Inadequate responses to responsible disclosure efforts reveal a concerning lack of prioritization for cybersecurity in many organizations.
5. Economic incentives often conflict with privacy protection, complicating efforts to secure user data.

Addressing these challenges requires a multifaceted approach that goes beyond technical solutions. Organizations must prioritize security in their development processes, implement robust API protections, and foster a culture of responsiveness to security disclosures. Regulatory frameworks need to evolve to better balance innovation with privacy protection. Additionally, raising user awareness about the risks associated with data sharing is crucial.

Lessons Learned

AI as a Double-Edged Sword in Cybersecurity: The integration of AI and machine learning in cybersecurity presents both opportunities and significant risks. While AI enhances threat detection and defense capabilities, it also enables more sophisticated attacks, including the creation of convincing deep fakes for social engineering. Organizations must invest in AI-driven security solutions while also preparing for AI-enhanced threats.

Persistence of Traditional Vulnerabilities: Despite advancements in cybersecurity, long-standing vulnerabilities like SQL injection remain prevalent. This persistence highlights the need for continued vigilance in basic security practices and thorough code analysis. Organizations should not overlook these “classic” vulnerabilities while focusing on emerging threats.

Critical Infrastructure Vulnerability: The targeting of critical infrastructure by state actors and cybercriminals poses a severe threat to national security. The vulnerability of systems like power grids to cyberattacks emphasizes the need for enhanced protection measures and international cooperation to safeguard essential services.

Evolving Legal Landscape for CISOs: Recent legal cases, particularly the SolarWinds case, set new precedents for CISO liability. This shift in the legal landscape necessitates that CISOs secure robust indemnity agreements and maintain meticulous documentation of their security practices to protect themselves from potential legal action.

Importance of Comprehensive Security Testing: The CrowdStrike outage highlighted the critical need for thorough security testing, including dynamic analysis and stress testing. Organizations should implement comprehensive testing strategies that go beyond standard methods to uncover hidden vulnerabilities before they reach production.

Rising Threat of Non-Human Identities: The proliferation of non-human identities in cloud environments creates a vast, often overlooked attack surface. Security teams must extend their focus beyond human identities to effectively monitor and manage these machine-to-machine communications, which are increasingly targeted by attackers.

Vulnerabilities in Emerging Technologies: New technologies, from electric vehicle chargers to AI-driven development tools, introduce novel security risks. Organizations must adopt a security-first approach when developing and implementing these technologies, considering potential vulnerabilities from the outset.

Ransomware Evolution and Geopolitical Factors: Ransomware groups are becoming more sophisticated and stable, often operating with implicit state support. Understanding the stability and tactics of these groups is crucial for developing effective response strategies. The geopolitical dimension of cybercrime complicates efforts to combat these threats.

Privacy Risks in Consumer Applications: Location data leakage and API vulnerabilities in popular apps, particularly dating apps, pose significant privacy and safety risks. This underscores the need for stricter data protection practices, including data minimization and robust API security, to safeguard user information.

Challenges in Responsible Disclosure: The cybersecurity community continues to face challenges with responsible disclosure, as many organizations fail to respond adequately to reported vulnerabilities. This highlights the need for improved communication channels between security researchers and organizations, as well as a cultural shift towards prioritizing cybersecurity concerns.

These lessons underscore the complex and evolving nature of the cybersecurity landscape, emphasizing the need for a multifaceted approach that combines technological solutions, legal preparedness, continuous education, and collaborative efforts across industries and nations to effectively combat emerging cyber threats.

Contributors

List of Interviews Contributing to This Report

Chapter 1: AI and Machine Learning in Cybersecurity

Sam Curry - Vice President and Chief Information Security Officer (CISO) at Zscaler.

Michael Sikorski - Vice President of Threat Intelligence and Chief Technology Officer (CTO) at Unit 42, Palo Alto Networks.

Shachar Menashe - Senior Director of Security Research at JFrog.

Michael Brown - Principal Security Engineer at Trail of Bits.

Sherrod DeGrippo - Director of Threat Intelligence Strategy at Microsoft.

Chris Wysopal - Co-Founder and CTO of Veracode.

Alberto Yépez - Co-Founder and Managing Director of Forgepoint Capital.

Chapter 2: Vulnerabilities and Exploits

Paul Gerste - Vulnerability Researcher at Sonar.

Thijs Alkemade - Security Researcher at Computest Sector 7.

Robert Herrera - Researcher at NCC Group.

Alexander Plasket - Researcher at NCC Group.

Matei Josephs - Senior Security Researcher and Founder of HiveHack.

Eduard Agavriloae - AWS Offensive Security Expert.

Michael Bargury - Chief Technology Officer at Zenity.

Alon Leviev - Security Researcher at SafeBreach.

Chapter 3: Cybersecurity in Enterprises

Adam Cheriki - CTO and Co-Founder of Entro Security.

Ravi Ithal - Co-Founder and CTO of Normalyze.

John Wrobel - Chief Revenue Officer at Menlo Security.

Brian Dye - CEO of Corelight.

Alberto Yépez - Co-Founder and Managing Director of Forgepoint Capital.

Chapter 4: Critical Infrastructure and Ransomware

Joe Marshall - Senior Security Strategist at Cisco Talos.

Vangelis Stykas - CTO of Atropos.

Bryson Bort - Founder and CEO of SCYTHE.

Rob Boyce - Global Cyber Resilience Lead at Accenture.

Chapter 5: Legal and Regulatory Challenges

Tim Brown - CISO of SolarWinds.

Jess Nall - Partner specializing in Cyber and AI at Baker McKenzie LLP.

Alex O'Neill - National Security Researcher, formerly with Harvard's Belfer Center.

Lachlan Price - Student at Harvard Kennedy School and MIT Sloan School of Management.

Chapter 6: Emerging Threats and Red Teaming

Brandon Kovacs - Senior Red Team Consultant at Bishop Fox.

Sherrod DeGrippo - Director of Threat Intelligence Strategy at Microsoft.

Malachi Walker - Security Advisor at DomainTools.

Nathan Hamiel - Senior Director of Research at Kudelski Security.

Chapter 7: Security Testing and Resilience

David Brumley - CEO of Mayhem Security.

Vangelis Stykas - CTO of Atropos.

Theresa Lanowitz - Chief Evangelist at LevelBlue.

Chapter 8: Innovations in Cybersecurity Tools

Jeff Williams - Founder and CTO of Contrast Security.

Jacob Larson - Team Lead for Security Testing and Assurance at CyberCX.

John Morello - Co-Founder and CTO of Gutsy.

Chris Wysopal - Co-Founder and CTO of Veracode.

Chapter 9: Threat Intelligence and Research

Etay Maor - Chief Security Strategist at Cato Networks.

Renée Burton - Vice President of Threat Intelligence at Infoblox.

Malachi Walker - Security Advisor at DomainTools.

Brian Dye - CEO of Corelight.

Chapter 10: Privacy, Data Leakage, and API Vulnerabilities

Victor Le Pochat - Postdoctoral Researcher at KU Leuven.

Karel Dhondt - PhD Researcher at KU Leuven.

Malachi Walker - Security Advisor at DomainTools.

Matei Josephs - Senior Security Researcher and Founder at HiveHack.

Eduard Agavriloae - AWS Offensive Security Expert.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANKINFO SECURITY® CAREERSINFO SECURITY® GOVINFO SECURITY® HEALTHCAREINFO SECURITY®

CUINFO SECURITY® Just for Credit Unions Data Breach® TODAY Prevention. Response. Notification. infoRisk® TODAY AIToday.io CIO.inc

CyberEd.io CyberEdBoard DeviceSecurity.io FraudToday.io PaymentSecurity.io

CYBER THEORY GREYHEAD AN ISMG COMPANY Xtra mile LIFECYCLE MARKETING QG MEDIA

iSMG