NONSTOP SECOPS THROUGH REAL-TIME COLLABORATION AND AI-DRIVEN AUTOMATION

Cyber Security Summit Webinar Series

Series June 27th, 2023

Speaker: Gareth Lindahl-Wise, Chief Security Advisor and CISO, Ontinue; speaker at national and international events.
Moderator: Sean Costigan, Director of Cyber Policy; Professor at George C. Marshall European Center for Security Studies
Report Author: Hugo Munoz Reinoso, Cyber Security Summit and UPS intern

Speaker Bio: Gareth Lindahl-Wise is a cybersecurity expert with a wealth of experience in the field. As the Chief Security Advisor and Chief Information Security Officer (CISO) at Ontinue, he is responsible for leading the organization's cybersecurity efforts. Gareth is passionate about leveraging the power of collaboration, automation, and AI to strengthen cybersecurity and defend against emerging threats. He emphasizes the importance of data governance, ethical AI usage, and strategic automation to optimize security operations. Gareth's insights have been instrumental in developing Ontinue ION, AI-powered managed extended detection and response (MXDR) platform, which utilizes Microsoft's technologies and advances in AI to deliver a proactive and efficient cybersecurity defense.

Introduction: In today's digital landscape, cybersecurity has become a top priority for organizations worldwide. The ever-evolving threat landscape demands innovative and proactive approaches to defend against sophisticated cyber-attacks. Traditional cybersecurity methods are no longer sufficient, and security professionals are turning to collaboration, automation, and AI as crucial pillars to enhance their cybersecurity strategies.

This white paper explores the profound significance of collaboration, the power of automation, and the role of AI in cybersecurity. Drawing from insights shared by Gareth Lindahl-Wise, we discuss these three tenets to demonstrate how they reinforce an organization’s cyber resilience.

The Significance of Collaboration in Cybersecurity: Collaboration lies at the heart of effective cybersecurity defense. Cyber threats are complex and dynamic, often requiring the collective knowledge and skills of diverse security professionals. Lindahl-Wise notes there is a need to break down silos and foster a culture of collaboration among security teams.

Collaboration involves seamless communication and information sharing between different teams, such as threat intelligence, incident response, and IT operations. By encouraging collaboration, organizations can ensure that relevant data reaches the right people at the right time. This results in accelerated incident response times, faster decision-making, and improved situational awareness.

Collaborative platforms, like Ontinue ION for Teams, provide a centralized space for security professionals to interact, share insights, and collectively respond to incidents. Adaptive Cards enable teams to gain contextual information and take immediate action, streamlining the incident response process.

The Power of Automation in Cybersecurity: Automation has emerged as a game-changer in cybersecurity. By automating repetitive and manual tasks, security teams can free up valuable resources, allowing them to focus on more strategic and high-impact activities. Lindahl-Wise stresses the importance of approaching automation thoughtfully and strategically.

The foundation of successful automation lies in accurate and well-governed data. The quality of data directly impacts the effectiveness of AI models and automation processes. Organizations must ensure that their data is reliable and properly governed to make informed decisions.

"Managed bravery" is a concept that Lindahl-Wise advocates for in the automation journey. Starting with automation in lower-risk areas allows security professionals to closely monitor outcomes and build confidence over time. This approach ensures that organizations maintain control over AI-driven actions and can intervene, if necessary.

The Role of AI in Enhancing Cybersecurity: AI serves as the backbone of collaboration and automation in cybersecurity. AI models possess the ability to analyze vast amounts of data at incredible speeds, enabling security teams to identify patterns and potential threats that may have gone unnoticed otherwise. Understanding the data better empowers organizations to make informed decisions and take proactive steps to strengthen their cybersecurity posture.

However, Lindahl-Wise emphasizes the importance of challenging AI suppliers and understanding how AI is being used. It’s crucial to strike the right balance between human expertise and AI-driven automation. AI should complement human capabilities and enhance security operations, neither being over-relied upon nor underutilized.

Conclusion: Collaboration, automation, and AI are integral components of a robust cybersecurity strategy. Organizations must prioritize collaboration among security teams to foster seamless communication and information sharing. Thoughtful automation, supported by well-governed data, can significantly enhance operational efficiency and response times.

AI empowers organizations with valuable insights and proactive defensive capabilities. Organizations can build a resilient defense against cyberthreats by adopting a proactive approach, challenging AI suppliers, and combining human expertise with AI-enabled capabilities.

Wholeheartedly embracing collaboration, automation and AI, makes it possible for organizations to out-maneuver their adversaries while safeguarding digital assets and sensitive data. Including these components into cybersecurity strategies empowers organizations to effectively navigate the ever-evolving threat landscape. Together, collaboration, automation and AI fortify defense, enabling organizations to transform to modernize their cybersecurity.