innovate days - Wichita 2022

Cybersecurity Education Sessions

Why Your Endpoint Strategy is Failing

Speaker: **Adam Gray**

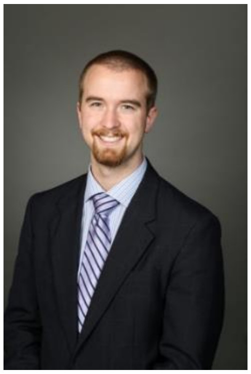
A nationally recognized figure in the cybersecurity industry, **Adam Gray** has been at the forefront of applying security research and innovation for the last 25 years, helping protect some of the world's largest and most vulnerable enterprises against critical threats. A highly sought-after speaker who has lectured at universities and before armed forces security councils, Adam has advised many of the nation's Fortune 1000 corporations as well as the US Army, Navy, and Air Force. With a unique perspective on the emerging threats and the ever-changing landscapes of everything from compliance to intrusion prevention, Adam has an impressive track record of successfully steering strategy for the full spectrum of IT and security disciplines.

Session Abstract

The unspoken truth is that endpoint security misses a significant portion of the malware, adware, riskware, and other problematic themes in your environment. Turning a blind eye to software controls, secure configurations, and a lack of monitoring has led to one of the worst years in history as it relates to cybersecurity. During the course of this talk, we'll outline the risks and issues we are facing, what some strategies are to resolve those and cover market trends that we believe are important. This talk is not meant for security vendors. It is a practitioners talk.

Forging a Secure Software Supply Chain

Speaker: **Alec Harrell**



Alec Harrell is a Director of Security Services at Novacoast specializing in DevSecOps, cloud security, and custom development at the enterprise scale. He regularly advises customers in architecting secure and maintainable custom solutions for all size companies ranging from startups to Fortune 10. Alec has worked with several large enterprise software vendors building additions and extensions to their core platforms to address novel customer requirements. His recent work includes conducting security assessments for application security, custom application architecture, security product implementation, and security advisory in DevSecOps and Cloud.

Session Abstract

This session covers the importance of security as a part of the software supply chain. It introduces the concept of SLSA which ensures the security of the build, validates that the code has not been tampered with, and also provides a framework to security checks including open-source library review and security tooling like SAST, DAST, and secrets management.

Cybersecurity Education Sessions

Re-educating Your Guesses: How to Quantify Risk & Uncertainty

Speaker: **Sara Anstey**

Sara Anstey is a Data Analytics Manager at Novacoast who is passionate about empowering businesses to use everyday data to make strategic business decisions. She believes that the intentional adoption of a data-driven culture can be a key differentiator to companies in today's security climate. Sara has experience in custom web development, artificial intelligence, data analytics, business intelligence, and applied statistics.

Session Abstract

Asking for budget and justifying spend in cybersecurity departments can be a difficult task due to limited data and high uncertainty of future events. This talk will dive into quantitative risk analysis as it relates to cybersecurity - how to model uncertain events and understand financial risk. Attendees will see a first hand demonstration of how quantitative modeling can be used to communicate risk and understand ROI. Attendees will walk away with the tools needed to present cyber risk as a dollar amount that can be easily understood by other business decision makers at their company.

Vulnerability & Patch Management: There are no solutions…only trade-offs

Speaker: **Jon Poon**

Jon Poon has a background in development starting with a degree in Computer Science and spanning 15 years in security and enterprise software. His expertise includes architecting and implementing web (full stack), mobile, and desktop applications. He has worked with developers and engineers across the industry to develop solutions that range from simple services to mission critical processes. His work includes staying actively engaged with senior and board level professionals across industries working both domestically and internationally. In addition to his work with customers, Jon also works heavily with product vendors and has guided product development as a member of several partner advisory councils over the years. Jon is currently the Vice President of Security Services at Novacoast.

Session Abstract

Most organizations make significant investments in Vulnerability, Patch, and Asset Management "solutions." They often divide ownership and responsibility of basic security disciplines such as vulnerability scanning, system patching, and asset inventory among different groups who leverage different tools to execute different processes according to different policies overseen by different decision-makers. Despite each groups' effort to address the challenges specific to their area of responsibility, the organization's goal of basic cyber hygiene generally remains unattained. We'll explore why thinking of these disciplines as separate programs might be the biggest obstacle to an organization's effectively addressing the controls around hardware and software inventory, secure configuration, and continuous vulnerability and patch management to achieve sustainable cyber hygiene.

Insights From a Threat Hunter

Speaker: **Elise Manna-Browne**

Elise Manna is Director of Threat and Intelligence at Novacoast, specializing in threat response, hunting, intel, crimeware analysis, and penetration testing. She participates in the infosec community as a member of the H-ISAC Threat Intelligence Committee, and as a member of FS-ISAC, believing information sharing is an important component to defending against cybercrime. Elise has worked countless cases in organizations ranging from manufacturing, healthcare, financial, retail, and educational sectors, with attacks ranging from insider theft to ransomware outbreaks.

Session Abstract

Hear Ever wonder what goes into a threat hunt? We'll explore the process of planning and executing a threat hunt. Using LockBit ransomware as a case study, this session will cover the workflow and techniques that can be applied during this proactive approach to threat detection.