Security Forum Presentation and Presenter Bio

'**Visualyze 2022_Deep Observability**' by Gigamon Scott Hamilton, Senior Solutions Engineer for Gigamon.

Metrics that Matter. According to a recent survey of over 900 global IT leaders across North America, APAC and EMEA, that affirmed that network-derived intelligence is critical to the security and performance of multi-cloud workloads. In this research, 75 percent of enterprises consider DEEP OBSERVABILITY as critical to mitigating threats quickly and effectively.

To quote analyst Mark Leary: "*Networking, cybersecurity and observability are becoming intertwined. IT organizations are looking to leverage an immutable source of truth and more collaborative management efforts to break down siloed technology approaches, position themselves for long term success, and, ultimately, deliver the best possible business outcomes. Deep observability must be prioritized as IT organizations look to fully realize the transformational promise of a resilient and responsive digital infrastructure and continually maintain a strong security posture to meet today's digital business requirements."* – Mark Leary, Research Director with C.

You've carefully planned your network security architecture and purchased the latest, most advanced security tools. But is that enough? Here are a few statistics to ponder:

- Up to 50 percent of traffic never reaches your security tools because of dropped packets or blind spots
- Malware can hide inside encrypted SSL/TLS traffic
- Attackers now use port spoofing to elude perimeter detection

An effective security posture requires seeing all traffic across your network — not just a portion. You also need to know what the threats are, and how best to respond.

Scott Hamilton is a seasoned IT professional with over 35 years' experience in networking, security, and cloud operations. He has spent time at Cisco, Network General, Fortinet, Viavi, and spent the last 5 years with Gigamon designing customer visibility solutions for on-premise, virtual, and hybrid cloud environments.

Security Forum Presentation and Presenter Bio

'**DIY Malware: All my base are belong to me**!' by Mike Salvatore, Lead Developer for Akamai

"If it's not tested, it's broken." How often do you test your network security? How much does it cost you? When pentesting is done right, it's fabulous. If you're not careful, however, the results can be high-cost and low-value. Furthermore, if pentests are performed infrequently, it's hard to know if your team and tools are really up to the challenge of defending your network. In this talk, we'll discuss adversary emulation and how it can augment your red and blue team activities. Then we'll introduce Infection Monkey, an open-source adversary emulation platform that enables security practitioners to quickly design custom malware that's safe for testing in production environments.

Mike Salvatore is a cybersecurity professional and enthusiast from Pennsylvania. He currently works at Akamai, where he is the lead developer of Infection Monkey. Previously, he worked on the Ubuntu security team for Canonical and as a security software engineer at Lockheed Martin. Mike holds a master's degree in cybersecurity from Johns Hopkins University and a bachelor's degree in electrical engineering from Rutgers University. As an active open-source developer and security researcher, Mike loves giving back to the tech community. You can read about Mike's security research at https://salvatoresecurity.com.

Security Forum Presentation and Presenter Bio

'**From Kim Jong-Un to Jinping & Putin…Geopolitical Issues Creating Cyber Threats Against Your Business**' by Steve Stasiukonis, President of Secure Network Technologies

The political tensions between the US and other Nations have led to a growing number of hackers and organizations getting hacked. Organizations around the globe have experienced an exponential number of attacks against their networks, employees, vendors and intellectual property. Join us as we explore the world of cyber criminals and how easy it is to become a cyber-threat actor. With today's threat actors' ability to hide behind a variety of pseudo anonymous crypto currencies, combined with the ease of obtaining hacking resources, you will see what makes the life of cybercrime extremely attractive. As the ransomware threat continues to grow by shutting down businesses, and redirection of funds becomes a common attack. The session will provide you with the roadmap to understand digital criminal, how to protect your entity and what to do in the event you have to deal with an unfortunate incident.

Take aways from this presentation;

THE WHO –"Cyber Threat Actors"… The most sophisticated criminal in the world. Learn what your business is up against.

THE WHY – Breaching Your Business. The Incentive Driving Threat Actors to Hack Your Organization.

THE WHEN – It's NOT "If", but "When" you get breached. Know how to be prepared in the event you get compromised.

Steve serves as President of Secure Network Technologies, focusing on Penetration Testing, Information Security Risk Assessments, Incident Response and Digital Investigations. Steve Stasiukonis has worked in the field of Information Security for over 25 years, specializing in the use of technology to identify information security vulnerabilities, assessing risk and the collection of digital intelligence. As a part of that experience, Steve is an expert in Social Engineering. Steve carries numerous security certifications by various organizations and also serves as a columnist for Information Week magazine and DarkReading.

Pittsburgh Chapter ISSA Information Systems Security Association

Security Forum Presentation and Presenter Bio

'**Defending Azure AD, Office 365 and the Hybrid Cloud**' by Tim Oroszi, Senior Enterprise Engineer at Tenable

Review common attack paths within AzureAD, Office365 and Hybrid environments and discuss defense techniques within each.

Tim is an Enterprise Security Engineer with Tenable supporting North American and Canada Enterprise Accounts. He is a Certified Information System Security Professional and holds his MBA in Executive Leadership from the Ohio University.

Tim has spent over 15 years in IT, focusing in data security and information risk management. Over the course of his tenure Tim has focused his efforts in, helping Fortune 100 companies build and mature their vulnerability management, web application security and identity and access management programs.

Security Forum Presentation and Presenter Bio

'**SOC Modernization - 5 Pillars for Driving Differentiation to Improve Security Operations**' by Brian Magner, Senior Solutions Manager at Deepwatch

Security operations have, like so many things in the security industry, moved into what many consider to be a commoditized, outsourced model in order to combat cost, staffing shortages, and an increased focus on business-driven functions by internal security teams. That said, the basics of content, capability, and prioritized response still matter, but communicating and operating around those topics with partners can be incredibly difficult. Without them, any outsourced programs become one-size-fits-all approaches of dubious value.

In this discussion, we will review the five pillars of crucial capabilities that organizations should pursue to drive differentiation while improving security operations.

Brian has spent the last decade working to help solve security problems and drive security maturity. His career started in GRC and Risk Management consulting where he focused primarily in the healthcare vertical working on implementation and adoption of risk visibly and mitigation practices. From there he shifted into to the Network Security world where he led a team focused on helping customers in the financial, technology, manufacturing and healthcare verticals migrate their security technologies and tooling to better support their cloud transformations. Brian is now a Sr. Solutions Director at Deepwatch where he partners with organizations to help mature their security operations programs.

Security Forum Presentation and Presenter Bio

'**Strengthen your Cyber Insurance Strategy**' by Toni Buhrke, Director Sales Engineering, Mimecast

During this interactive session, Toni Buhrke, Director of Sales Engineering, at Mimecast will highlight key requirements and tools customers have utilized to strengthen their Cybersecurity Insurance Strategy. Specifically, we will review Cyber Insurance basics and touch on four topics important to cyber insurance underwriters:

1. Reducing your attack surface while maximizing your controls
2. Preventing spoofing attacks against your sending email domains
3. Fortifying your resilience through Cyber Awareness and Anti-phishing training
4. Communicating your program effectively to reduce premiums, increase coverage, and manage

Toni Buhrke is a Director of Sales Engineering at Mimecast with more than 25 years of experience in the cybersecurity industry. Together, Toni and her team are responsible for designing customized email security solutions for commercial and SLED customers in the Eastern region of the U.S. Prior to joining Mimecast, she was a Global Director of Systems Engineering at Forescout Technologies. During her 12-year tenure there she led various systems engineering teams focused on helping commercial and public sector organizations and channel partners architect and deploy security solutions to protect complex networking environments. Throughout her career, Toni's focus has always been on bridging the gap between technology and her customers. Toni has an MBA and CISSP certification, and is very active in Women in Technology and Learning initiatives throughout the industry.

Security Forum Presentation and Presenter Bio

'**A Clear Path to NIST & CMMC Compliance**' by Jack Nichelson, CISO for Inversion6

Beginning in 2020, the DoD will use the Cybersecurity Maturity Model Certification (CMMC) to verify contractors of the Defense Industrial Base are operating with effective cyber hygiene. In order to bid on, maintain, and win future DoD contracts, all organizations will need to prove their required level of cyber maturity. If you do business with the DPD, NASA, GSA or another state/federal agency, you need to be prepared for the CMMC framework. In this presentation, we discuss the potential impacts on your business, while introducing an affordable, practical and secure solution for contractors preparing for CMMC certification.

In addition to answering questions from attendees, this presentation will cover the following topics:

- What You Need to Know About CMMC
- CMMC 2.0 Proposed Changes
- The Crawl – Walk – Run of CMMC
- Preliminary Steps for CMMC Success
- How to improve your NIST SP 800-171 Self-Assessment SPRS score

Jack Nichelson is an experienced CISO and technology executive with 25 years of experience in the government, financial, and manufacturing sectors. His roles have included leading transformation and management of information security and IT infrastructure, data management and more for organizations in numerous industries. Jack earned recognition as one of the People Who Made a Difference in Security by the SANS Institute and received the CSO50 award for connecting security initiatives to business value. He's been a CISO for MRK Technologies since September of 2018. Jack holds an MBA from Baldwin-Wallace University, where he is an adviser for its Collegiate Cyber Defense Competition (CCDC) team.

Security Forum Presentation and Presenter Bio

'**Cyber Incident Reporting: Navigating the Latest Federal Requirements**' by Julie Davila, Field CTO Public Sector for Sophos

In this presentation, Julie will summarize the status of federal incident reporting requirements (proposed and implemented), ranging from CIRCIA to the SEC, and the steps an organization can take to be better prepared for what's to come.

Julie is currently the Field CTO Public Sector for Sophos and has worked in private and public sectors with a deeply technical background, having worked in disciplines across software, cloud, big data, DevOps, and cybersecurity. Before Sophos, she led her email cybersecurity startup that primarily served large-scale federal customers. In her free time, Julie enjoys spending time with her children, playing competitive ice hockey, and volunteering with veteran and women-focused nonprofits.