Intelligent Security Week 2022

December 6-8, Virtual Event

December 6 – Critical role of AI & ML in Cybersecurity

9.00am **Optimizing security strategies during an acute talent shortage**
We are all used to seeing data about the rising number of successful cyber-attacks, but even scarier are the number of attacks that go undetected. Bad actors have used malware and vulnerabilities such as Emotet and Log4J to slip malicious code past corporate firewalls, allowing them to roam undetected around co4porate networks for months or even years searching for the most valuable booty. Now, companies are rapidly turning to AI-based technologies tuned to spot even the most subtle anomalies, that were too hard or too expensive to find in the past. Tom Gillis, Senior Vice President and GM of VMware's networking and advanced security group will discuss the rapid evolution of these tools and unlock some of the operational secrets CISOs can use most effectively to put them to work.

Tom Gillis, Sr VP & GM, ***VMware***

9.30am **Why AI is critical for cutting edge, effective cybersecurity**
The most effective tool in any toolbox is the one that gets the job done effectively and efficiently. When it comes to cybersecurity, this is definitely true as well. AI as a component of an effective cybersecurity toolbox is critical: it can transform cyber workflows into streamlines, autonomous, continuous processes that speed remediation and maximize protections. In the process, it offloads menial, manual, and time-consuming security tasks that while important, don't require human supervision. This talk will discuss how AI-powered cybersecurity solutions streamlines the daty-to-day process of maintaining security, maximizes the use of human supervision in the areas that truly need it, and in the process defends brand reputation and trust in an organizations security system and protocols.

10.00am **Machine Learning to automate cybersecurity evaluation and response**
Maintaining a highly functional and effective cybersecurity system for an organization is tricky. Simply having enough time and human power to analyze and assess attacks from zero-day malware or identifying and prioritizing threats (including false positives) quickly becomes overwhelming for any security team, no matter how skilled. This discussion will highlight how Machine Learning can automate these processes as well and free up the relatively limited number of qualified cybersecurity professionals whose expertise should be focused on critical attacks that require human intervention.

December 7 – Identification and Mitigation

9.00am **Identifying and mitigating the most critical security risks:**
The need for cybersecurity solutions is common knowledge, but how do you determine what to secure and how? Do you know where your blind spots are? Is there a successful one-size-fits-all approach to cybersecurity? In this talk you will learn how to assess your organization, identify risks and holes, and what to look for in cybersecurity solutions that can help you proactively recognize risk and effectively respond to attacks.

9.30am **Internal threats that create external attack opportunities and how to combat them**
Having AI-powered cybersecurity solutions automated by robust ML applications is extremely important to an organization's overall security stack, but it still can be circumvented by human actions from the inside. Phishing scams and improperly secured devices can wreak havoc on internal systems that are successful at keeping external threats out, but are vulnerable inside the gates. Learn how educating your work force is an important and ongoing piece of effective cybersecurity solutions.

December 8 – Industry case studies for context

Industry Case Studies: Finance

9.00am **Investing in technologies and people to defend financial institutions**

Stakes for cybersecurity are higher than ever at financial institutions as threat actors are increasingly using more vicious attacks. There has been a serious uptick in destructive cyberattacks that delete or damage the integrity of financial data (records, algorithms, transactions) and generally disrupt or destroy confidence in the integrity of the system. In order to defend against and respond to these attacks, security leaders are doubling down on their investment in cybersecurity solutions. In this talk, you will learn what solutions (both technical and human) CISOs are investing in and why.

Industry Case Studies: Healthcare

9.30am **Best practices and technologies that are the ultimate antidote against healthcare cyberattacks**

The healthcare industry generates a massive amount of data that is extremely vulnerable to data breaches, ransomware, and malware. Attack can be directed at multiple points of vulnerability, which makes it extremely difficult to protect such personal information. Insecure medical devices and equipment, legacy systems, and a lack of documented cybersecurity and governance policies are easy targets for sophisticated cyberattacks – so how do healthcare institutions defend against them? In this talk, you will learn about best practices and technologies employed by members of the healthcare industry to recognize and respond to attacks in real-time as well as protect the data from the inside out.

Industry Case Studies: Manufacturing

10.00am **Building security structure and practice into smart factories**

The rise of digital technologies brought a new level of cyber complexity to manufacturing, but the industry itself hasn't kept up with adequate cybersecurity programs to prepare for the equal rise in risk. The interconnectedness of smart factories has exposed people, technology, physical processes, and intellectual property to threats such as ransomeware and loss of operational systems control. What are the root causes and how do you build cyber resiliency into smart factories? In this talk, you will learn how to invest in proper cyber security technologies, prioritize actions based on risk profiles, and build in security resiliency to create an effective manufacturing cybersecurity program.