Abstract

iMedPub Journals
www.imedpub.com

American Journal of Computer Science and Information Technology

2021
Vol.9 No.S1

Network based threat hunting – a critical component for securing the cloud!

Etay Maor
Sr Director Security Strategy, Cato Networks & Cyber security Professor at Boston College,
Email: etay.maor@catonetworks.com

Abstract

Using legacy, "on-prem" security strategies to combat today's threats is like bringing a knife to a gun fight. Threat actors have been perfecting the art of evading security controls for years and we see the results in headlines all the time. In this session we will dive into network based threat hunting and how it can be implemented within an organization's security strategy. A cloud environment requires a cloud security strategy!

Most organizations are going through a digital transformation journey, be it a planned one ore one that was forced upon them due to circumstances. But how many organizations are making sure that this journey also includes security transformation? Most organizations use the same security tools and techniques as the ones we have been using for over a decade, but our infrastructure as well as the threats targeting them have changed and evolved. They are bringing a knife to a gun fight! End point AV?
Sandboxes? Siloed threat intel feeds? Threat actors today have proven over and over they can bypass these strategies.
In this session we will review how today's threats evade security detection and how they evolved over time. We will see how a network based threat hunting program does not necessarily mean changing and buying new products but rather how to better utilize current capabilities to fit today's threats. It's not all about new features but rather how to deploy and use them! We will show use cases as well several of the tactical, practical techniques to help detect and mitigate today's threats. A cloud environment cannot be protected with the tools and techniques of the "on-prem" days, a cloud environment requires a cloud security strategy!

Biography

Dr. Etay Maor is the Sr. Director Security Strategy at Cato Networks and an industry recognized cyber security researcher and key note speaker. Previously, Etay was the Chief Security Officer for IntSights where he lead strategic cybersecurity research and security services . Before that Etay held numerous leadership and research positions as an Executive Security Advisor at IBM where he created and led breach response training and security research and as Head of RSA Security's Cyber Threats Research Labs where he managed malware research and intelligence teams and was part of cutting edge security research and operations. Etay is an adjunct professor at Boston College and holds a BA in Computer Science and a MA in Counter Terrorism and Cyber Terrorism. Etay is a frequent featured speaker at major industry conferences and is part of RSA Conference and QuBits conference committees. Deanna Mulvihill has her expertise in evaluation and passion in improving the health and wellbeing. Her open and contextual evaluation model based on responsive constructivists creates new pathways for improving healthcare. She has built this model after years of experience in research, evaluation, teaching and administration both in hospital and education institutions. The foundation is based on fourth generation evaluation (Guba& Lincoln, 1989) which is a methodology that utilizes the previous generations of evaluation: measurement, description and judgment. It allows for value-pluralism. This approach is responsive to all stakeholders and has a different way of focusing