APRIL 2021

THE MODERN SECURITY BATTLEFIELD:

What 2020 taught us about gaps in vulnerability management

An ICIT Virtual Briefing Primer

Authored By:
Drew Spaniel, Lead Researcher, ICIT

Contributors Include:
Joyce Hunter, Executive Director, ICIT
Jannine A. Mahone, Senior Manager, Product Marketing

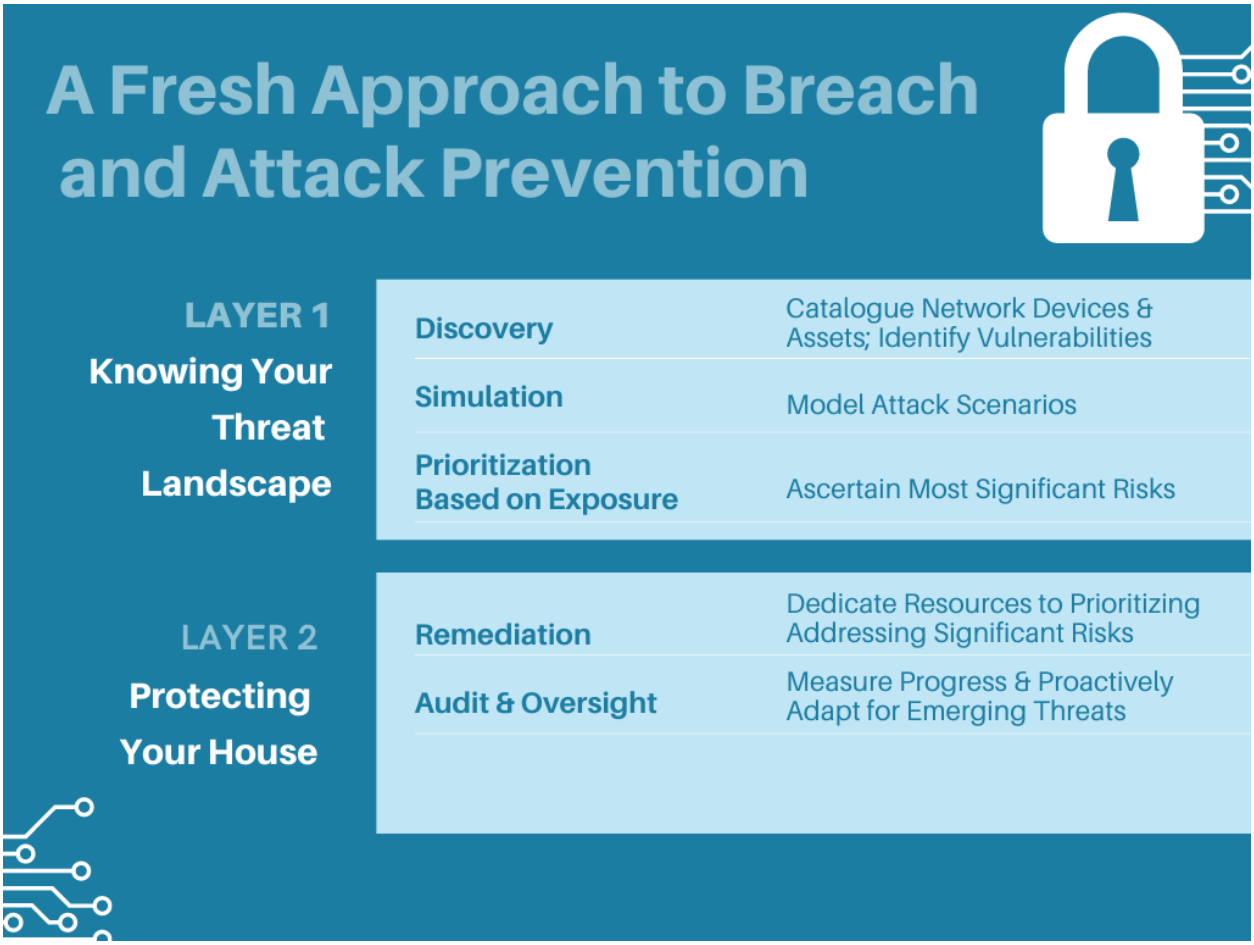
ICIT | Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

With prolific security breaches such as SolarWinds dominating the news, organizations are daunted by the fear that they could be made infamous in the next major breach. Developing a mature and tightly connected security framework that enables the reduction of risk and improves security capabilities is more critical than ever. While 2020 was fraught with tragic outcomes of social and economic proportions, security teams have learned many lessons on resilience and have orchestrated many technical innovations to secure a distributed workforce. An expanded attack surface, defending against sophisticated multi-stage and multi-vector attack campaigns, and a pressing need to improve operational efficiencies have reframed digital transformation priorities. One important element to help address this challenge is having better automation tools that simplify remediation, provide an operational advantage, and improve security. But are these tools primed and ready to deliver the CISO with quick time to value, a comprehensive risk remediation plan to present to the Board, and assurance that the organization will maintain a mature vulnerability and risk management program that averts increasing attacks? A fresh approach to breach and attack prevention is needed to shift defense paradigms towards proactive security.

At the April 8, 2021, ICIT panel discussion, subject matter experts will discuss the gaps that COVID 19 uncovered in current vulnerability management programs and why the combination of trustworthy security policy management and closed-loop vulnerability remediation will become the new citadel for securing large and increasingly complex enterprise networks. **Join us** to learn the importance of integrating automation into full lifecycle vulnerability management:

- Scoping your efforts to target vulnerabilities that matter
- Using the 'ex-factor' of exposure analysis plus exploitability data to focus remediation efforts
- Creating a cohesive web between existing security products to automate and deliver remediation from discovery to resolution
- Developing a mature and tightly connected security framework that enables the reduction of risk and improves security capabilities

Panelists Include:
- John Agnello, Chief, Development Branch at United States Cyber Command
- Renee Wynne - former, CIO NASA
- Steven Pruskowski, Security Test & Evaluation Lead, Cybersecurity and Infrastructure Security Agency (CISA)



Network Vulnerability Management Life Cycle

Discovery

Discovering network vulnerabilities begins with cataloging all physical, cloud, and digital assets and endpoints and identifying details such as operating system, applications, process, access, and function. The network profile can then be used to establish a baseline of expected activity and behavior. Further, the baseline can be combined with aggregated CVE's, advisories, and breach reports to inform the organization about their network attack surface and risk exposure.

Simulation

Solutions like Skybox's network modeling empower organizations to detail their networks, detect vulnerabilities, and simulate potential attack paths. Simulated attacks expose system vulnerabilities, reveal conflicting security controls, and empower the organization to walk the paths of potential attackers. The simulations help the organization develop and practice incident response plans so that if a security incident occurs, the organization maximizes its

potential to forestall a breach and minimizes the potential impact and cascading harms the adversary can inflict.

Prioritization

Using the network model developed in the Discovery phase and the vulnerability insights gleaned during simulation exercises, the organization can focus its resources on mitigating and remediating the vulnerabilities with the highest risk scores. Network and security tools like Skybox can enable organizations to aggregate emerging vulnerability data, device configuration data, and risk advisories across disparate environments, endpoints, and network infrastructure, to better inform risk scores and customize the scores to the risk appetite of the organization.

Remediation

Organizations should begin by identifying and remediating vulnerabilities whose exposure could result in an exfiltration of sensitive data, disruption to mission-critical operations, or afford the adversary the most pervasive foothold in the network. If the prior steps were followed, these would be the vulnerabilities with the greatest risk scores.

Oversight

Establish controls and metrics to measure and verify remediation efforts and demonstrate progress. Verify that vulnerabilities have been remediated and that risk has been mitigated through continuous audits and regular simulations. Clearly assign security responsibilities and expected network activity. Proactively improve the cyber-hygiene of personnel and test their retention of the best practices and their ability to implement the incident response plan.

Effective information security is a cyclical and continuous process. Ensuring that your organization is not made infamous as the victim of the next prolific breach is an active, not passive responsibility. Actionable security strategies require vigilance, proactivity, and innovative tools such as Skybox solutions that automate security operations and risk insights.