

**AN ICIT
VIRTUAL BRIEFING
TAKE-A-WAY**



AUGUST 2021

LESSONS FROM THE MODERN SECURITY BATTLEFIELD

A Fresh Approach to Breach and Attack Prevention

Author: Drew Spaniel, Lead Researcher, ICIT

Contributors:

- John Agnello, Chief, Development Branch at United States Cyber Command
- Renee Wynne, Former CIO, NASA
- Steven Pruskowski, Security Test & Evaluation Lead, CISA

Contents

Introduction	2
Insights on the 2021 Cyber Threat Landscape	2
The Vulnerability Management Life Cycle - A Fresh Approach to Breach and Attack Prevention.....	2
Discovery	3
Share and Leverage Information on Developing Trends and Emerging Threats	3
Increase Network Visibility.....	3
Prioritization	4
Recognize Early Signals	4
Remediation.....	4
Cybersecurity is More than Scanning and Patching	4
Oversight.....	4
Increase Secure Collaboration	5
Quantify and Prioritize Risk.....	5
Conclusion: Remediate According to Exposure.....	5
Sources	6

Introduction

The COVID-19 pandemic forced a mass migration to a distributed workforce. For many organizations, this exposed the shortcomings, inefficiencies, and vulnerabilities in their networked systems and processes. Many companies tried to plug the gap using automated tools to simplify remediation efforts, improve resiliency, and provide a competitive edge. However, if automated solutions lack the proper scoping and management mechanisms, they may not deliver the essential insights necessary to thwart an emerging attack. At the April 2021 ICIT virtual event, "[The Modern Security Battlefield: What 2020 Taught Us About Gaps in Vulnerability Management](#)," panelists discussed the gaps that the COVID-19 pandemic uncovered in current vulnerability management techniques and why trustworthy security policy management and closed-loop vulnerability remediation are becoming the new citadel for securing complex, large, enterprise networks.

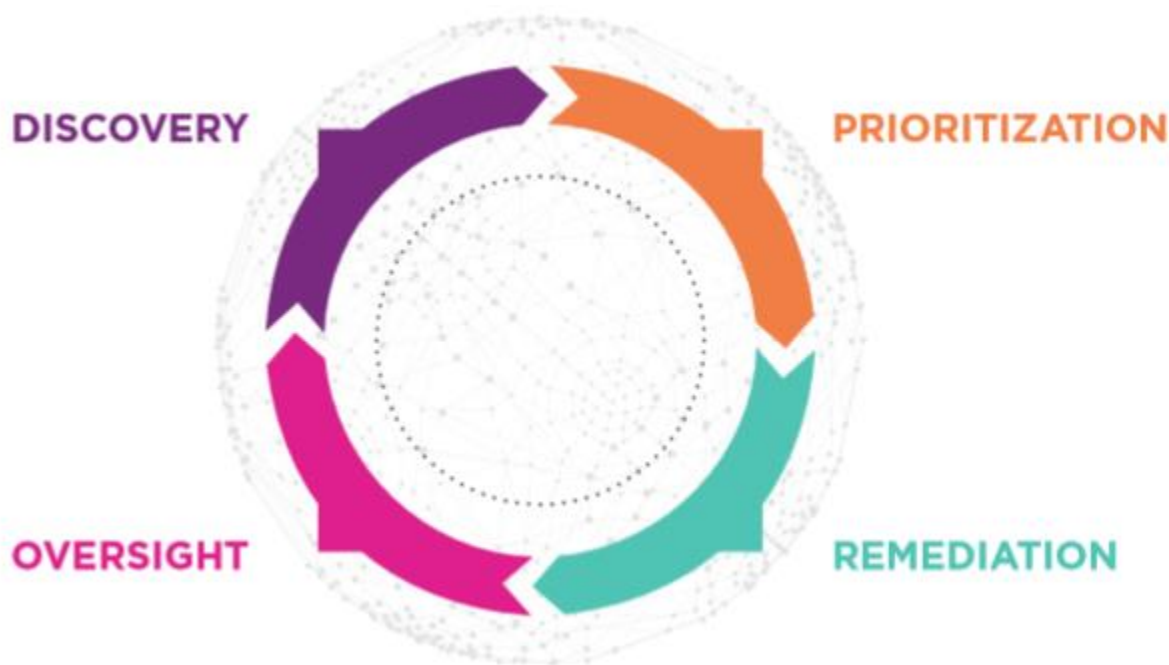
Insights on the 2021 Cyber Threat Landscape

Adversaries capitalized on the chaos and tumult created during the pandemic by exploiting the nascent network ingress and egress points that arose from the rapid migration to a distributed workforce. Furthermore, they may have increased targeted attacks against third-party entities to laterally compromise critical systems, as evidenced by the following statistics:

- Cybercriminals adapted their tools, tactics, and procedures to compromise hybrid working environments. In their publication *Vulnerability and Threat Trends Report 2021: Cybersecurity comes of age*, Skybox found a 106% increase in new ransomware and a 128% increase in new trojans between 2020-2021 [1].
- Between January and April 2020, cloud-based cyberattacks rose by 630% [2].
- The average cost of a breach increased by \$137,000 to ~ \$4 million [3].
- Google claims that by April 2020, it was blocking 18 million COVID-centric phishing emails daily [4]. Around the same time, Symantec estimated that 1 in every 4,200 emails was a phishing attempt [5].
- Between 2020-2021, the FBI measured a 300% increase in reported cybercrimes [6].
- Globally, annual cybercrime is expected to inflict costs exceeding \$6 trillion in 2021 and at least \$10.5 trillion by 2025 [7].

The Vulnerability Management Life Cycle - A Fresh Approach to Breach and Attack Prevention

The ICIT discussion panelists agreed that public and private sector organizations needed to adapt to a more holistic and comprehensive vulnerability management lifecycle. Organizations need to better thwart emerging threats, mitigate novel attacks, and remediate existing vulnerabilities, and the best way to do this is through trustworthy security policy management and closed-loop vulnerability remediation.



Discovery

Discovering network vulnerabilities begins with cataloging all physical, cloud, and digital assets and endpoints. This process must include identifying operating systems, applications, processes, access, and function. Organizations can then use this network profile to establish a baseline of expected activity and behavior. When combined with aggregated common vulnerabilities and exposures (CVEs), advisories, and breach reports, these can inform an organization about its network attack surface and risk exposure.

Share and Leverage Information on Developing Trends and Emerging Threats

One of the most efficient ways to discover indicators of compromise and monitor emerging trends in the threat landscape is to participate in information-sharing efforts with public and private sector stakeholders. John Agnello, Chief of the Development Branch at United States Cyber Command, asserts, “Data is king, so the more information you have and the more you can parse, sort, and use that data, the better your organization will be security-wise.” He recommends increasing information-sharing efforts to help the intelligence community and other critical infrastructures combat emerging adversarial campaigns. He observes:

Increase Network Visibility

It is no longer acceptable for organizations to be unaware of the devices connected to or capable of accessing their networks. As Renee Wynn, former CIO at NASA, provides,

There are two basic questions that you need to be able to answer at all times: who and what is on your network. And when you understand those two pieces for your business, you have a risk characteristic. You apply that model, and then you find out where your highest risks are. While

you can't predict necessarily where the bad guys are going to go, you can predict and identify the highest targets within your enterprise and apply special attention to them.

Network visibility empowers organizations to prioritize resources and optimize their ability to act on data and insights.

Prioritization

Using the network map developed in the Discovery Phase, organizations can focus their resources on mitigating and remediating the vulnerabilities with the highest risk scores. Network and security tools, like Skybox, can enable organizations to aggregate vulnerability disclosures, device configuration data, and risk advisories across disparate environments, endpoints, and networked to generate risk scores customized to tolerances acceptable to the organization.

Recognize Early Signals

Wynn asserts that it is critical to seize information-sharing opportunities and leverage the data while it is relevant. She elaborates,

What really got illuminated in the pandemic is the need to get information into the right people's hands very, very quickly, and then collaborate on how to best use it. We all have to learn how to recognize what is in an early signal and act so that we don't end up with a widespread issue in enterprises or amongst several government agencies. [This is where] information-sharing becomes really critical. It's a reminder that we've got to share, go forward, and try to prevent incidents like Solar Winds.

Remediation

Organizations should begin by identifying and remediating vulnerabilities whose exploitation could expose sensitive data, disruption mission-critical operations, or afford adversaries a pervasive foothold on the network. If an organization has followed the previous steps, these would be the vulnerabilities with the greatest risk scores.

Cybersecurity is More than Scanning and Patching

Agnello observes that too many organizations focus their cybersecurity efforts on scanning for known vulnerabilities and deploying patches. This strategy relies on the erroneous assumption that the organization has received all actionable intelligence and can patch faster than adversaries can exploit. In reality, even with information sharing and collaboration, threat-data sharing still lags behind adversarial momentum. Instead of institutionalizing a culture of security-thru-patching, organizations would be better served by adopting solutions that probe their networks and systems for exploitable vulnerabilities. Once each exploit is assessed according to the latest trends, it would receive a risk score denoting the severity of said exploit.

Oversight

This phase aims to establish controls and metrics to measure and verify remediation efforts and demonstrate progress. Through regular simulations and continuous audits, organizations can verify they have remediated vulnerabilities and mitigated their risks. This involves clearly assigning security

responsibilities to all employees, monitoring expected network activity, proactively improving personnel cyber-hygiene, and testing incident response.

Increase Secure Collaboration

Secure collaboration requires that all personnel understand the information security plan and act per approved processes and procedures. As explained in the Discovery Phase, organizations should audit their networks and processes to establish a secure baseline, at a minimum. Personnel should know how to use secure applications and systems without deviating from the mechanisms and devices approved for daily use. Steven Pruskowski, Security Test and Evaluation Lead at the Cybersecurity and Infrastructure Security Agency (CISA), opines that the challenge of the pandemic partially due to the need to develop collaboration tools that could be implemented without compromising security.

Quantify and Prioritize Risk

Exploitable vulnerabilities and exposed systems are indicative of a failed security policy. Wynn advises “Assume that anything that walks in your door is a potential business risk. However, prioritize based on risk. If the risk is fairly low and an asset is not connected to something critical, you may have to sacrifice it to allocate resources elsewhere.” Solutions, like Skybox, can help organizations discover exposed systems and mitigate exploitable vulnerabilities. Additionally, these solutions can secure often-overlooked network devices, such as routers and legacy systems.

Conclusion: Remediate According to Exposure

The onset of COVID-19 emphasized how organizations managed their security and risk. Adversaries quickly evolved their tactics and exploited the vulnerabilities exposed by the global chaos. Some organizations were quick to adapt their security strategies to an agile vulnerability management lifecycle, while others were less swift to evolve and may have suffered security incidents and breaches. As John Agnello, Renee Wynn, and Steven Pruskowski expressed in their April 2021 ICIT panel discussion, vital lessons can be gleaned from both the successes and failures of the past year. The pandemic united organizations in their shared cybersecurity struggles and how we, as a unified information security community, should continue to promote the adoption and evolution of the vulnerability management lifecycle model that has proven efficient at deterring the adversarial exploitation of critical vulnerabilities. Organizations that have not yet adopted a comprehensive information security framework, such as the aforementioned vulnerability management lifecycle model, should seek the assistance of collaborative cybersecurity partners, such as Skybox, that can assist in the rapid transition to a more secure network model.

Sources

- [1] "Vulnerability and Threat Trends Report 2021", *Skybox Security*, 2021. [Online]. Available: <https://www.skyboxsecurity.com/trends-report/>. [Accessed: 10- Aug- 2021].
- [2] "Cloud Adoption and Risk Report", *Mcafee.com*, 2020. [Online]. Available: <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-cloud-adoption-and-risk-report-work-from-home-edition.pdf>. [Accessed: 10- Aug- 2021].
- [3] "Cost of a Data Breach Report 2021", *ibm.com*, 2021. [Online]. Available: <https://www.ibm.com/security/data-breach>. [Accessed: 10- Aug- 2021].
- [4] N. Kumaran and S. Lugani, "Protecting against cyber threats during COVID-19 and beyond | Google Cloud Blog", *Google Cloud Blog*, 2020. [Online]. Available: <https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond>. [Accessed: 10- Aug- 2021].
- [5] B. Stackpole, "Symantec Security Summary - June 2020", *Symantec-enterprise-blogs.security.com*, 2020. [Online]. Available: <https://symantec-enterprise-blogs.security.com/blogs/feature-stories/symantec-security-summary-june-2020>. [Accessed: 10- Aug- 2021].
- [6] "Internet Crime Report 2020", *ic3.gov*, 2020. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf. [Accessed: 10- Aug- 2021].
- [7] S. Morgan, "Cybercrime To Cost The World \$10.5 Trillion Annually By 2025", *Cybercrime Magazine*, 2020. [Online]. Available: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>. [Accessed: 10- Aug- 2021].