merlin

May 2020

If Tools Could Talk...

Come clean with your cyber hygiene

Security tools tell a cyber hygiene story

INTRODUCTION

Large corporations typically work with more than 70 cybersecurity vendors. Enterprises have added tool after tool to secure their data, systems, and users from increasingly sophisticated cyberattacks. As a result, organizations have tools that are misconfigured, repetitive, or siloed – in addition to poor visibility and control over their environments. This puts a massive strain on an organization's cyber hygiene, which is often considered the Achilles heel of cybersecurity.

Poor cyber hygiene creates severe security vulnerabilities and requires action, especially as telework surges. But it often takes time, money, and resources to properly maintain cyber hygiene. Already overwhelmed with the complexity and costs of managing their IT infrastructure, security executives must remain vigilant about the cyber posture of their enterprise.

What if all of an organization's cybersecurity tools could talk? What would they say to the security and risk teams managing them? What would they be telling the CISO, CEO, or even the Board of Directors? The tools all have a voice. The challenge, however, is that most security and risk executives simply aren't listening to them. Not because they don't want to. Many just don't have the means to be able to do so. Security teams are overwhelmed with the chaos – the 'fog of more' with tools, alerts, and security incidents. Inevitably, these teams lose context of how their security tools connect to applications that enable the business.

To succeed, cybersecurity leaders need to remember what constitutes proper cyber hygiene and how they can continuously monitor their security posture. Security executives should consider maximizing the ROI on already-purchased tools before adding new ones to their crowded ecosystem. While cyber hygiene encompasses tools, training, and policies, this paper focuses on tools and the critical importance of correctly configuring, maintaining, and monitoring them.

BACK TO THE BASICS

In the ongoing struggle of securing infrastructures against external and internal dangers, organizations should strive to gain full visibility over everything on their network. Those with a clear picture can keep their cyber hygiene 'house in order' and are better equipped to deal with threats. Cyber hygiene involves all the fundamental activities and principles that ensure an organization's IT security is in peak condition, protected from threats, and aligned with the core business. An enterprise practices proper cyber hygiene when it possesses comprehensive visibility of its network, protects its most vital data, sustains its cybersecurity infrastructure, adopts best practices for security controls (e.g., industry-recognized frameworks like NIST or CIS), and follows manufacturers' recommendations for associated security tools configuration.

Cyber hygiene can be divided into five key focus areas, which tend to be aligned with industry-accepted frameworks:

Maintaining these focus areas and ensuring that they remain in good standing can mitigate or eliminate many of the common threats organizations face. A 2018 report from the Online Trust Alliance analyzed that more than 90 percent of all security breaches can be prevented by basic cyber hygiene.[1] Therefore, proper cyber hygiene is an absolute necessity and not a nice-to-have.

Recognizing this need, most organizations align with one or more of the industry-recognized frameworks to guide their cyber posture. NIST CSF and the CIS Controls help enterprises implement their cybersecurity risk guidelines and best practices in areas like incident response, patching, and vulnerability management.

But adherence to a framework is typically only measured during infrequently scheduled audits, if at all. Unfortunately for organizations, changes in tool configuration and controls between audits open them up to vulnerabilities. One recent study found that by following security controls that directly map to a given vulnerability, an organization could expect to completely mitigate the vulnerability two-thirds of the time, with partial mitigation one-third of the time.[2]

While tools are integral to cybersecurity, the focus of cyber hygiene is not to deploy more tools. Instead, it's about concentrating on the tools that are already deployed and making sure they're providing the best possible protection and visibility. At RSA 2019, one CISO said that 80 percent of cybersecurity challenges can be solved by getting the hygiene correct, rather than chasing the latest technology.[3] Misconfigured, unpatched, and unprotected security tools provide more risk than the latest zero-day threat, and gaps with the tools must be addressed immediately.

More than 90% of all security breaches can be prevented by basic cyber hygiene.

SPEAKING OF CHALLENGES

While the concept of getting cyber hygiene 'correct' is simple in its message, the difficulty lies in applying it to the IT environments of today. CISOs are responsible for their organizations' IT operations, security, and risk management. They're expected to effectively manage all of that while also meeting the needs of their C-suite colleagues, complying with regulations, dealing with an increasingly dynamic threat landscape, and executing across hybrid infrastructures. Risk-based decision making in cybersecurity must align with the overall business impact.

As organizations have evolved their IT infrastructures and moved operations partially or completely into the cloud, securing a network's perimeter with a single toolset no longer applies. There is a growing number of quality tools designed for today's complex IT environments and many enterprises take a 'best of breed' approach when purchasing. While this approach allows them to align with the technologies that provide the security and features necessary for their unique needs across on-premises

[1]Retrieved April 23, 2020, from https://www.internetsociety.org/wp-content/uploads/2019/04/2018-cyber-incident-report.pdf
[2]Such, Jose; Ciholas, Pierre; Rashid, Awais; Vidler, John; Seabrook, Timothy, "Basic Cyber Hygiene: Does it work?" (Computer, 2018)
[3]Wing VC – Research Note: RSA Conference 2019

and cloud environments, it also creates a new set of challenges. Organizations are now faced with ecosystems that involve multiple security tools vendors, many of which cannot be managed and scored with a common security platform.

Defense in depth, while a long-standing tenant of security strategies, adds to the complexity and difficulty of maintaining proper cyber hygiene. For example, a multilayered approach to securing email leverages spam protection, attachment sandboxing, and local protection placed on the endpoint. Typically, however, each of those protections is from a different vendor, requiring specific product knowledge to update and maintain.

Adding further complexity, organizations must comply with various industry (HIPAA, PCI-DSS, CIS, etc.) and government regulations (e.g., FedRAMP, GDPR, CCPA) as they arise. Beyond regulations, meeting compliance requirements of external auditors, internal teams, customers, and partners across the same ecosystem can be a time-consuming, manual process that provides only point-in-time assurances of compliance.

These layers of complexity and issues only exacerbate the security industry's ongoing shortage of skilled workers. The current cybersecurity workforce is estimated to be 2.8 million people worldwide, against an estimated need of more than 4 million professionals.[4] Adding more full-time employees to maintain cyber hygiene across different tool vendors is not a viable solution.

Therefore, it's evident that tool fragmentation is an issue in cybersecurity. Average-sized companies have 25-30 security vendors while larger corporations typically utilize more than 70.[5] With a fragmented toolset, the knowledge required to maintain those tools increases. Further difficulties arise when attempting to quantify a risk, failed security control, or poorly configured tool against another tool in a completely different security domain from different vendors. Silos between IT and security operations teams further amplify the complexity. Luckily, there are ways to gain better insights and take back control to improve one's cyber hygiene.

Average-sized companies have 25-30 security vendors while larger corporations typically utilize more than 70.

[4]Retrieved April 28, 2020, from https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

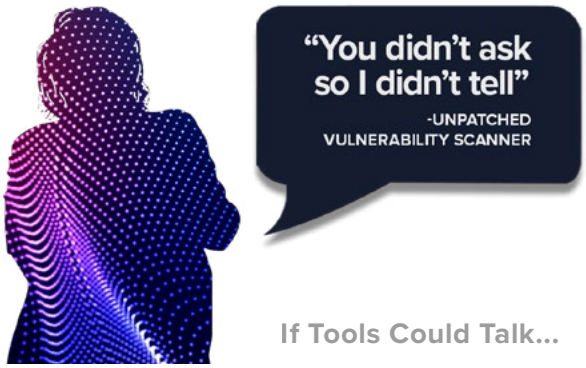
[5]Wing VC – Research Note: RSA Conference 2019

COME CLEAN WITH YOUR TOOLS

Practicing proper cyber hygiene is a lot more than purchasing and implementing security tools. Proper configuration of the tools you have is a fundamental but often overlooked cyber hygiene task. For example, Gartner research found that more than 95 percent of firewall breaches were due to misconfigurations.[6] If this is true for firewalls, what does it say about all the other tools your enterprise uses?

Tool misconfiguration is frequently cited as a cause of breaches. Establishing configuration baselines, along with visibility of assets, is a bedrock of proper cyber hygiene. We need security tools to maintain our hygiene, but it's using those tools correctly that helps solidify our overall cybersecurity posture.

According to a 2019 Ponemon Institute report, more than half of IT experts don't know how well the security tools they've deployed are working.[7] Here's how to ensure your tools are effective and telling you what you need to know about your cybersecurity posture:



If Tools Could Talk...

1) Analyze

Analyze if the tools you're using are engineered properly and doing what you expect them to do. For example, if it's a vulnerability scanner, is it updated and scanning your entire IT landscape? Or, if it's a next-generation firewall, are you using all its features appropriately? Can you identify the impact to your core business applications?

2) Review

Review and rate your current tools with a critical eye. Try to rationalize each tool against your organization's current and future needs. Move past qualitative descriptions and into quantitative analysis by ranking and scoring them with questions like:

- **Does this tool have a niche or special purpose?**
- **Is it more or less secure than other options?**

3) Examine

Finally, examine each tool's actual configuration. Does it have default passwords or other weak controls? Does it use vendor-supplied admin accounts? How easy is it to harden?

[6]Retrieved April 23, 2020, from https://www.firemon.com/misconfigurations-firewalls-greatest-threat/
[7]Retrieved April 24, 2020, from https://www.businesswire.com/news/home/20190730005215/en/Ponemon-Study-53-Percent-Security-Leaders-Don%E2%80%99t

UTILIZE A SIMILAR APPROACH WHEN EVALUATING NEW PRODUCTS AND SERVICES:

1) Determine

Determine what tool your organization needs and how you'll implement it. Each new product brings unforeseen challenges and opportunities, some good and some bad. They also mean new vendors, engineers, and a host of technical expectations and assumptions your organization might be unprepared for. CISOs and CIOs can't be shortsighted when pursuing new solutions since individual decisions have direct implications to business applications and enterprise risk management.

2) Evaluate

Evaluate how and where the tool fits within your ecosystem. What are the integration points? How does it complement existing tools? Or, does it provide additional coverage and capabilities that your organization currently lacks? Focus on multilevel integration with every tool and express this need early and often with vendors. The interoperability they deploy should be standards-driven and utilize the least privilege necessary.

Security tools, and cyber hygiene by extension, are only as effective as an organization's internal process for keeping them in good working order. There are solutions, however, which easily automate this work and provide organizations with comprehensive and continuous oversight of their cybersecurity posture.

WALK THE TALK

Enterprises need a central place where they can continuously monitor their tools and infrastructure, ensure alignment with industry frameworks and best practices, and prioritize critical security controls ((CSC) across their environment while also being able to prioritize based on business impact. With the rise of telework and hybrid infrastructures, organizations also require full visibility into their networks, applications, processes, and endpoints. By gaining such a comprehensive picture of their cybersecurity posture, organizations reduce vulnerabilities and improve cyber hygiene.

Cyber Observer is an agnostic cyber hygiene management platform that gives CISOs and their teams the ability to gauge real-time security posture across all tools and security domains, regardless of manufacturer. The intuitive solution provides clarity to organizations with fragmented security tool ecosystems and continuously monitors their cyber hygiene. Cyber Observer connects to each tool via exposed interfaces (e.g., API access, LDAP queries, SQL queries) and uses

read-only access to gather CSC information. The platform collects all this information and uses it to inform an organization whenever there is a deviation from established thresholds and baselines.

Cyber OBSERVER

Status and scoring on all security tools and configurations

Security views that assess against industry frameworks

Gap analysis to enhance your security environment

Real-time monitoring of security tools and domains

Cyber Observer enhances an enterprise's ability to correctly deploy, implement, and leverage a tool's full capability while lowering the required knowledge capital. The solution sends alerts on configuration anomalies or errors and whenever a tool is not being leveraged fully, directly helping improve an environment's cyber hygiene. Able to also provide gap analysis and security views that assess against industry frameworks, Cyber Observer is an essential tool for proper cyber hygiene.

Turning attention to network security and endpoints, longtime pillars of hygiene like anti-virus and endpoint detection and response (EDR) solutions are no longer enough. New and emerging threats on mice, keyboards, webcams, and other hardware can go undetected by these security solutions. Sepio Systems' purpose-built platform helps address such vulnerabilities.

From a network security standpoint, Sepio provides total visibility into an organization's network using hardware fingerprinting and machine learning algorithms. These features enable the platform to detect invisible attack tools inside a network or pinpoint an organization's most vulnerable network switches.

Sepio is also a leader in rogue device mitigation (RDM) with its ability to discover passive listening devices. The platform provides hardware visibility for all endpoint peripherals in an organization's network through continuous, real-time monitoring and control. Organizations achieve a stronger cybersecurity posture through Sepio's combination of network and endpoint security solutions, which start with visibility and finish with mitigation.

SEPIO SYSTEMS

Hardware fingerprinting and machine learning algorithms provide full network visibility

Continuous, real-time monitoring and control of all hardware assets and behavior

Rogue device mitigation leader

From business process and IT measurement perspectives, Centerity provides the ability to align both security and IT metrics with business impact. Named a Gartner Cool Vendor, Centerity's dynamic service views eliminate 'unknown' IT zones while embracing total visibility into all technological layers to help reduce mean-time-to-repair (MTTR) to minimal levels.

CENTERITY

AIOps platform ensures performance, availability, and security of critical processes

Real-time, consolidated business analytics for on-premises, cloud, and hybrid environments

Identifies performance anomalies and isolates faults across applications, operating systems, infrastructure, and cloud assets

Centerity's AIOps platform provides executive dashboard views highlighting real-time service levels and performance bottlenecks while delivering root-cause analysis. Its holistic visibility helps executives and administrators assess the security and IT impact that incidents have on operational performance.

Centerity's AIOps topology discovery engine enables organizations to identify changes in endpoints, servers, networks, and other elements in a contextual way, allowing for the creation of dedicated executive dashboards and reports for accurate measurement of service-level impact. The Centerity platform can enrich data flow analysis sources such as NetFlow and others to identify unauthorized usage and provide a CyberOps health score using a variety of critical metrics.

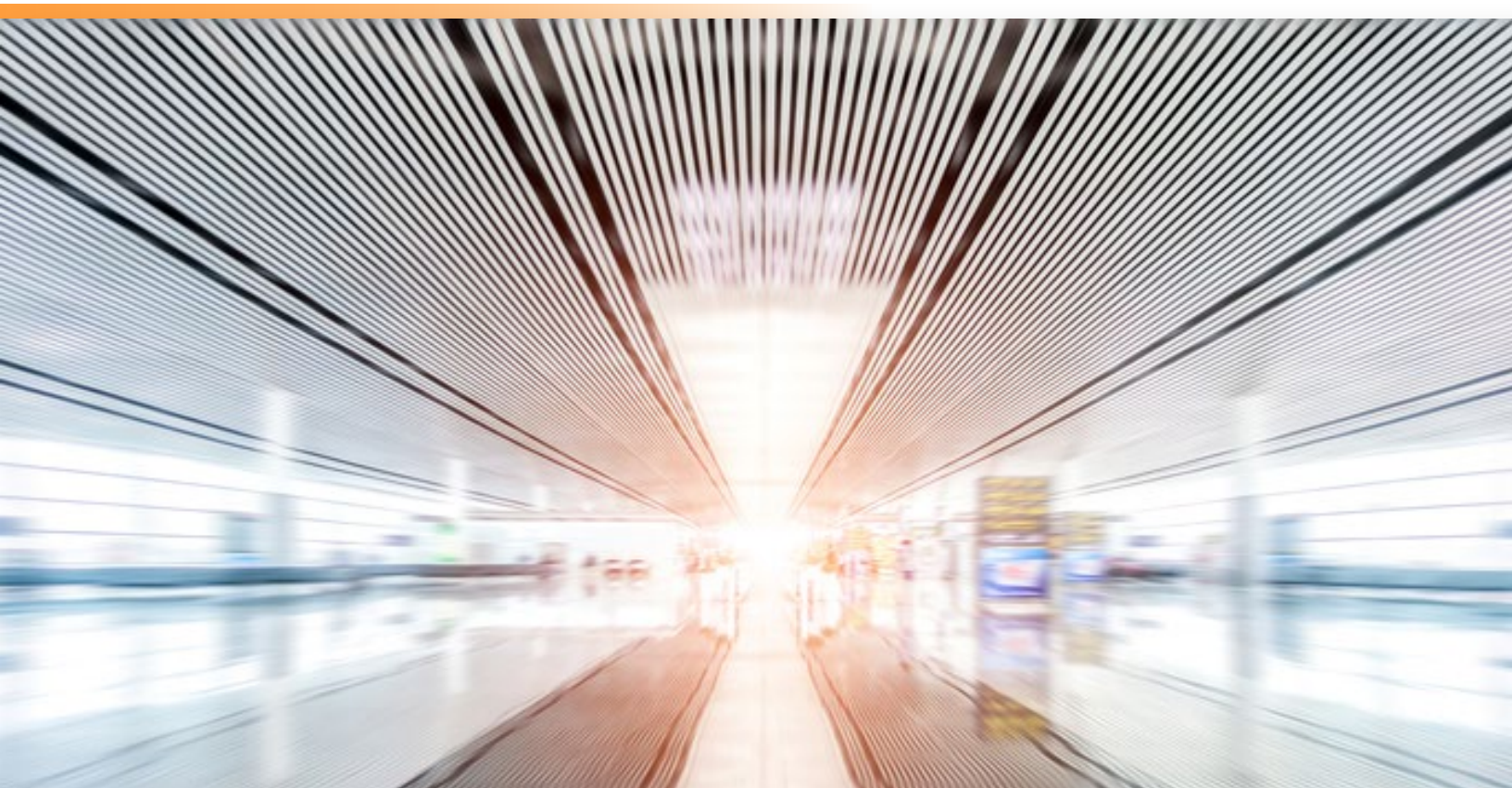
If Tools Could Talk...

CONCLUSION

The complexity of today's IT infrastructures coupled with security tool fragmentation and misconfiguration makes cyber hygiene challenging for companies of all sizes. Cyber Observer helps you continuously monitor and improve your cybersecurity posture, Sepio provides greater visibility and control over hardware assets connecting into your network, and Centerity adds business context and impact analysis. Together, the three platforms provide a comprehensive way for organizations to implement and maintain proper cyber hygiene and business health across the board.

Cyber Observer's continuous monitoring and actionable insights allow organizations to ensure hygiene, compliance to frameworks, and fully optimized tool configuration across their security ecosystems. The customizable platform enables organizations to address fragmented tool ecosystems while providing timely metrics on overall security posture. Centerity's AIOps platform adds auto-discovery engines and collects business metrics to decrease business impact while eliminating 'unknown' IT zones. Sepio adds to your cyber hygiene arsenal by detecting and mitigating rogue devices across the enterprise. Through Sepio's solutions, security teams gain full visibility of their organizations' hardware and how they're behaving.

As emerging technologies, Cyber Observer, Centerity and Sepio can be implemented quickly to produce immediate value and reduce organizational risk cost-effectively. The three solutions can work in tandem to provide a clear overall picture of your organization's cybersecurity posture, reducing your cybersecurity vulnerabilities, and helping ensure proper cyber hygiene with minimal business impact.



ABOUT MERLIN

Merlin is the premier cybersecurity platform with a unique business model that leverages technologies, trusted relationships, and capital to develop and deliver groundbreaking security solutions that help organizations minimize risk and simplify IT operations. Merlin represents prominent cybersecurity brands and invests in visionary, emerging technologies, bringing everything together into its lab where cybersecurity engineers integrate, test, and deliver innovative security solutions. This approach helps organizations save time, money, and other resources while more effectively securing their systems, data, and users no matter how requirements evolve.

Learn more at merlincyber.com.

AUTHORS

R. Casey Turner
is a Cybersecurity Solutions Architect at Merlin. He provides technical leadership in security solutions development and helps formulate scalable and adaptable solutions that meet business and compliance requirements.

Miguel Sian
is Merlin's Director of Solutions Architecture and Engineering. He leads a team of solutions architects and engineers that provide technical cybersecurity consulting for commercial and federal customers.

Daniel McGregor
is Technical Director of Customer Success for Merlin. He is responsible for delivering world-class support while developing customer relationships that promote retention and loyalty.

Arin Karimian
is Merlin's Director of Content.