Best practices Security management Microsoft Sentinel
6 min read

How automation is evolving SecOps—and the real cost of cybercrime

By Brooke Lynn Weenig, Senior Product Marketing Manager

June 28, 2023

Multifactor authentication

Security operations

Microsoft Defender

Microsoft Defender for Business

Microsoft Defender Threat Intelligence

Microsoft Incident Response

Microsoft Security Experts

This post is coauthored by Rob May, Founder and Managing Director, ramsac

The security community is continuously changing, growing, and learning from each other to better position the world against cyberthreats. In the latest post of our Community Voices blog series, Microsoft Security Senior Product Marketing Manager Brooke Lynn Weenig talks with ramsac Founder and Managing Director Rob May, who gave a TED Talk called "Your Human Firewall: The Answer to the Cyber Security Problem." The thoughts below reflect Rob's views, not the views of Rob's company or Microsoft, and are not legal advice. In this blog post, Rob talks about security operations (SecOps) challenges and how automation can address them, and shares phishing attack protection strategies.

Brooke: What are the biggest challenges in SecOps?

Rob: SecOps is the team responsible for the security of an organization's IT infrastructure, and for monitoring and responding to security threats and implementing security controls. One challenge for SecOps professionals is keeping up-to-date on the latest trends and tactics used by cyberattackers because threats to security are constantly evolving.

Another challenge is alert fatigue. Security teams are bombarded with alerts from their monitoring tools, and this can make it difficult to identify and respond to real threats. Many of the alerts that security teams receive are false positives that waste time and resources that could be better spent responding to real threats. In the industry, we talk about the utopia of having a single pane of glass that we can look through and get a view of everything. The reality is, in lots of organizations, they are not achieving that.

Balancing security with business needs is always a challenge. Security measures can sometimes conflict with the needs of users in the business, such as usability and accessibility. Professionals have to balance security needs with business needs so that security measures do not get in the way of productivity. Security teams often lack the resources to do their jobs effectively, and that might be budget, staffing, tools, or incident response training.

When a security incident occurs, SecOps professionals have to act quickly to investigate and contain the threat. Organizations are subject to a whole range of regulatory requirements depending on their geography and industry, and that can be complex and time-consuming to maintain. A SecOps professional has to think critically, work under pressure, and stay up-to-date with the latest trends and technologies in order to be successful in their role.

Brooke: **Can automation help address any of these challenges?**

Rob: Definitely. Automation is a powerful tool in SecOps that helps reduce the workload on the team and improve the efficiency and effectiveness of SecOps generally. An automated incident response system can detect unusual activity on the network and take action to contain and remediate that threat. Or it might detect an impossible activity, such as if you spent the day in the office in London and half an hour later, it appears that you are trying to log in in Russia.

Vulnerability management automation can be used to identify vulnerabilities, systems, and applications, prioritize them based on risk, and recommend remediation actions. Threat intelligence can help gather, analyze, and act on threat intelligence data from various sources, including open-source feeds, dark web forums, internal security logs, and compliance monitoring.

We can help ensure compliance with regulatory requirements and internal security policies by continuously monitoring systems and applications for compliance violations and security testing. We can use automation to conduct regular security tests such as penetration testing and vulnerability scanning to identify potential vulnerabilities and weaknesses.

Automation is not a replacement for human expertise and judgment. They go hand in hand. Automation helps improve the efficiency and effectiveness of security operations, and experienced SecOps professionals interpret what it is saying and act on the data provided by the tools.

Brooke: Have you seen a change in sentiment towards automation in the industry?

Rob: If you leave everything to automation, it has more potential to go wrong. For instance, if it detects something and blocks someone out of their account, and there is no human getting involved for a sanity check, all it is going to take is somebody in the C-suite not being able to do their job when they need to for them to think, “Oh, this is rubbish.”

Of course, it is not rubbish. It is an incredibly powerful tool. We just need to be able to interpret that as well. If I look at my own business and how we use something like Microsoft Sentinel, it is a positive thing, but we have used automation to take all the legwork out of it. A very large number of data incidents can be looked at to flush out a much smaller number that then is then investigated. There is no way you could do that without automation. Without a doubt, it is a game-changer.

Brooke: What does it mean to be a “human firewall?”

Rob: The human firewall is the collective efforts, behaviors, and habits of the people within an organization. Many commentators say that when it comes to cybersecurity, people are our weakest link. My view is that it is essential that we also consider the flip side of that coin, which is that people are also our greatest strength. We need to ensure that we give everyone the right training, awareness, tools, and policies to stay as safe as possible. If your people are not cyber-resilient, neither is your business.

Brooke: What is the real cost of cybercrime?

Rob: This question can be answered in a number of different ways. In terms of monetary value, the numbers are huge. I read one report recently that suggested that if the worldwide cost of damages caused by cybercrime was a country (measured in gross domestic product), it would be the third largest economy in the world after the United States and China.

The other way of answering the question is to look at all the associated impacts of cybercrime. This includes the direct costs of responding to an attack, including the investigation, remediation, and repair. Then, there are indirect costs, such as lost business, loss of productivity, reputational damage, emotional harm experienced by the Chief Information Security Officer and company officers, and other things like the resultant increase in insurance premiums (which can be significant).

Brooke: What variants are you seeing with phishing attacks today? How are they getting smarter and how can people and organizations protect themselves from these attacks?

Rob: Phishing attacks come in many different forms, but common variants include:

- **Spear phishing**: This is a targeted attack that is tailored to a specific person or organization. The attacker may use personal information or other details to make the message seem more legitimate.

- **Whaling (chief executive officer phishing)**: This is a type of spear phishing that targets high-level executives (the “big fish”) and other high-profile individuals within an organization.
- **Pharming**: This is an attack that redirects users to a fake website that looks like a legitimate site but is designed to steal their login credentials or other sensitive information.
- **Vishing**: This is a form of phishing that involves voice solicitation, such as phone calls or voicemails, instead of email.
- **QRishing**: This is phishing through QR codes. If you open a QR code on your device, it is no different from clicking on a link in an email.

Cybercriminals are using more sophisticated tactics for their phishing attacks to make their messages seem more legitimate. For example, attackers may use social engineering techniques to create a sense of urgency or to create a false sense of trust. They may also use advanced malware and other tools to bypass security measures and gain access to sensitive information.

To protect against phishing attacks, individuals and organizations should take a number of steps:

- Use strong passwords and multifactor authentication.
- Be wary of emails or other messages that ask for personal information or login credentials.
- Check the URL of any website that asks for login credentials or other sensitive information to make sure it is legitimate.
- Use antivirus and antimalware software to protect against malicious software.
- Educate employees and other members of the organization about the risks of phishing attacks and how to recognize and avoid them.
- Make sure your computer and devices have the latest software and firmware updates.
- Use anti-ransomware detection and recovery and turn on controlled folder access on the desktop.

By taking these steps, people and organizations can protect themselves against the growing threat of phishing attacks.

Learn more

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and Twitter (@MSFTSecurity) for the latest news and updates on cybersecurity.

Connect with us on social

What's new

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Microsoft Copilot

Copilot in Windows

Explore Microsoft products

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy

Sitemap Contact Microsoft Privacy Terms of use Trademarks Safety & eco Recycling About our ads