ANNUAL THREAT REPORT

2024 Cybersecurity Enhanced Resilience Checklist

Actionable steps to enhance your 2024 cybersecurity strategy

The new year is here, and so is our Annual Threat Report. To make sure you get the most out of what we've learned, we've translated the full report into a high-level checklist your security operators can act on.

We recommend reading the full report first and using this list to guide your security strategy for the upcoming year. While this list isn't exhaustive, it's a great starting point to make sure your cybersecurity strategy is playing offense *and* defense.

Feeling overwhelmed? We can help with that. Contact us here to learn more.

A refresher on general cybersecurity best practices

Odds are, none of these are unfamiliar to you. You know as well as we do that this upfront work can save your team (and company) future headaches. In the coming year:

- □ ***Actually* test your security tools and policies–just having them in place isn't enough.**
- □ **Provide regular *and* timely security training to your employees.** Do they know how to spot a malicious QR code? Are they familiar with role-specific phishing attempts?
- □ **Regularly review events marked as suspicious by your end users.** This feedback can help confirm and supplement detections of suspicious activity.
- □ **Understand that *someone* will always forget to change a default password.** Plan accordingly, and maintain an up-to-date inventory of internet-facing assets.

PRO-TIP: A real-life attack isn't the best time to test your incident response plan. Stress test your plan regularly—we recommend once a quarter—to make sure everyone knows what to do when a bad thing happens. And, to make your plan the most effective it can be, include roles and responsibilities, communication, reporting, how to handle data, and how to prepare for the emotions your team will experience.

Protecting against identity-based threats

Okta and Microsoft accounts are common targets for password abuse, and adversary-in-the-middle (AiTM) techniques are trending up as well. To protect against these common identity threats:

- □ **Reset user passwords, terminate sessions, and monitor for new multifactor authentication (MFA) device registration after a successful account compromise.** Don't forget that session termination!
- □ **Utilize Fast Identity Online 2 (FIDO2) and certificate-based authentication to stop AiTM attacks.** Or at minimum, keep these tools on your radar for the next budget meeting.

□ **Alert when a user simultaneously logs in from two locations.** This is a telltale sign of a successful AiTM login, since the attacker needs to intercept the user's session cookie.

□ **Alert for new Outlook inbox rules with suspicious names.** Look for keywords such as "invoice," "payment," "w2," or "deposit" in the filter parameters, or rules that automatically delete emails.

□ **Require admin approval for personal information updates.** This is an extra step but employees will thank you if someone attempts to edit their direct deposit info.

□ **Treat *any* evidence of password compromise as an identity incident.** Attackers blocked by one security mechanism may make additional attempts to access an account, and it's better to be vigilant than surprised.

□ **Block and track previously unseen or abnormal login attempts, *and* analyze them.** Logs aren't of much use until their data is scrutinized to reveal patterns, and if you're doing that during an incident, it's too late.

> **"Identity has been and will continue to be the frontier for risk.** With location and infrastructure control no longer core places where security controls are added, access and identity controls are the new firewall."
>
> —Greg Notch, Chief Information Security Officer at Expel

Protecting against cloud threats

As Amazon Web Services (AWS) and cloud tools (like Amazon Cognito) rise in popularity, the targets on the organizations using them also grow. And once bad actors can access your cloud—regardless of vendor—they can persistently access your infrastructure, too. To protect your cloud:

□ **Review configurations to ensure they align with best practices.** Build detections for configuration changes. This can identify unauthorized changes and misconfigurations when they occur.

□ **Monitor cloud platform auditing tools regularly for changes in your attack surface.** More tools = more access points for bad actors.

□ **Set up alerts for *any* sign of suspicious activity, such as attempted connections to unauthorized regions, VPNs, hosting providers, data centers, and large numbers of failed or unique API calls.** And to avoid alert fatigue, make sure you have a prioritization process in place—it only takes one missed alert to cause a problem.

□ **Enforce MFA for cloud consoles, and regularly remove and rotate access keys.** Simple key hygiene can go a long way!

□ **Perform regular audits of your cloud tools.** And include them in third-party audits, too.

> DID YOU KNOW?
>
> **96% of the cloud infrastructure incidents we detected and responded to occurred in AWS**, and the remaining 4% were split evenly between GCP and Azure.

Protecting against computer-based threats

These threats come in all shapes and sizes, from ransomware to malware to vulnerabilities and everything in between. To protect against computer-based threats:

□ **Have a defined (and timely) process where users can request tool or software downloads.** Be sure this also includes your IT team or other roles with unique needs.

□ **Use robust alerts for PowerShell.** Be sure to log alerts for a variety of potentially suspicious activities, such as encrypted commands, network connections, or high volumes of requests for internal host names from the same source.

□ **Check default settings for Windows programs and opening files.** Ensure your default settings do *not* automatically open files with a double click, and configure .JS, .JSE, .WSF, .WSH, and .HTA files to open in Notepad.

DID YOU KNOW?

Among the industries we serve, **financial services (19%) and hospitality (17%) experienced the greatest volume** of high-risk malware.

Protecting against phishing attacks

Phishing will remain a cybersecurity issue so planning for human error isn't optional. To protect against phishing:

□ **Avoid using QR codes.** But if you do need them, educate your internal and external users on how and when they can expect them to reduce risk.

□ **Educate employees on how to identify suspicious QR codes.** They can also use tools like zxing.org to view the link before opening it.

□ **For Microsoft users, enable the strictest QR code settings possible.** These are newer, so make sure you regularly check for additional security features Microsoft rolls out.

□ **Keep your security tech stack updated.** Consider adding tools like secure email gateways (SEG), anti-email spoofing controls like DMARC, SPF, and DKIM, or phish-resistant FIDO security keys.

"Adversarial use of AI will supercharge social engineering and a new generation of spear-phishing attacks. The election cycle and emotive geopolitical situations provide a particularly rich breeding ground for disinformation."

—Daniel Clayton, VP Security Operations at Expel