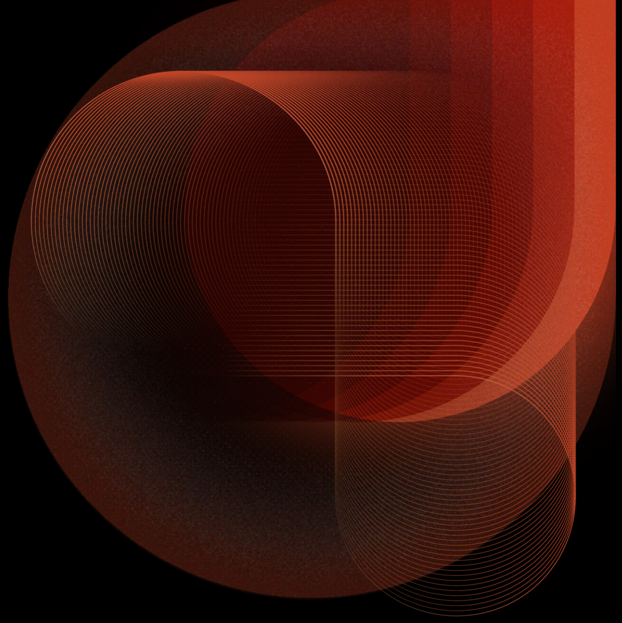
CYBERSECURITY CHECKLIST

57 Tips to Proactively Prepare

Securing Your Organization Is a Journey, Not a Destination



It's up to you to determine where to focus your defense efforts. It may not be possible to prevent breaches, but it is possible to be well-prepared for breaches before they occur. By taking action now, you can ensure that your organization isn't an easy target for threat actors, and you'll minimize damage in the event of a cyberattack by limiting an attacker's ability to spread through your networks. You'll need to work out ahead of time what your organization must do to remove threats, restore normal operations, and recover.

The following recommendations are based on real-time incident response cases and summarized from our 2022 Unit 42 Incident Response Report. They're divided into sections to help you focus your efforts and build more resiliency into your security program.

Comprehensive Recommendations to Make Your Organization More Secure

Identity and Access Management (IAM)

- Use single sign-on (SSO) platforms for web applications and multifactor authentication (MFA) wherever possible.
- Regularly review Active Directory for newly created accounts, mailboxes, and unrecognized group policy objects.
- Configure servers to prevent unauthorized access and directory listings. Enforce strong access controls.
- Should an employee be terminated, act quickly to revoke their access (e.g., active sessions, tokens, accounts, MFA devices, and rotating credentials), and then verify that access has been revoked. Ensure you preserve their system and data in case an investigation is needed.
- Limit the use of privileged accounts to when there is a valid business need, or a user requires a privileged account to complete their job task, and do not reuse local administrator account passwords.
- Disable administrative interfaces and access to debugging tools for anyone whose job role does not require them.

The **seven most targeted industries** were finance, professional and legal services, manufacturing, healthcare, high tech, and wholesale and retail.

Risk, Vulnerability, and Patch Management

- Identify your organization's critical and most valuable assets. This should include conducting an inventory of critical assets to understand where your highest-value targets are and if they require any additional protection.
- When implementing open source code, research it to understand whether it has any published vulnerabilities; only use code that is vetted and patched.
- Conduct regular web application/code reviews and annual penetration testing for all public-facing infrastructure to search for vulnerabilities; follow remediation recommendations.
- Configure security settings in your development environment according to best practices.
- Run periodic scans that include configuration checks and perform regular system audits to detect misconfigurations.
- Implement change control protocols that require review and sign-off on configuration changes.
- Patch management is critical for operating systems and on-premises applications; APT actors will move very quickly to capitalize on vulnerabilities. Address newly published vulnerabilities as quickly as due diligence allows.

Data and Software Security

- Understand where sensitive data lives and implement strong access controls to protect that data; monitor and audit access regularly. Limit sensitive data access to only those who need it within your organization and with third parties.
- Implement full-disk encryption for laptops and removable devices. Have a contingency plan to disable lost or stolen devices.
- Implement and utilize mobile device management applications that have the capability to locate and/or remotely wipe devices.
- Establish a DLP program responsible for classifying and tagging data and providing alerts when sensitive or other company-identified relevant information is leaving the organization.

Threat Detection and Response

- Consider a credential breach detection service and or attack surface management solution to help track vulnerable systems and potential breaches.
- Leverage EDR or XDR solutions, and ensure your security operations team understands how to utilize this technology to maintain full visibility across the network.
- Have an incident response and remediation plan. Incidents may occur despite best efforts, so have a tested, comprehensive plan to ensure fast action should an incident occur. If you have cyber insurance (recommended), be sure to integrate the policy's key processes and contacts into the plan.

Additional Tips

- Maintain a log retention repository and regularly review all logs and login attempts for unusual behavioral patterns. Ensure that logs are stored for the appropriate amount of time to fulfill any legal or regulatory obligations. Unit 42 consultants recommend a year or more, and if that is not possible, a bare minimum of 90 days.

- Leverage log aggregation systems, such as a security information and event management (SIEM) system, to increase log retention, integrity, and availability.
- Conduct regular security awareness training for all users, including contractors, on a yearly basis. Consider utilizing a trusted training platform that allows you to incorporate custom goals and objectives into the training curriculum.
- Avoid utilizing a flat network. Segregate networks and Active Directories, segment sensitive data, and leverage secure virtual local area networks (VLANs).
- Follow a defense-in-depth approach, implementing safeguards at each layer of the web application stack. This can include web application firewalls, operating system hardening, application input controls, file integrity monitoring, and least-privileged user accounts for database access and industry-standard encryption.
- Give your employees a way to conduct their business legitimately; simply blocking certain vectors will result in creative workarounds that you'll likely miss.
- Consider purchasing domains based on common spelling errors or variations of your organization's name. This can make it harder for threat actors to impersonate your organization.

77% of intrusions are suspected to be caused by three initial access vectors: phishing, exploitation of known software vulnerabilities, and brute-force credential attacks—focused primarily on remote desktop protocol.

Recommendations to Prevent Phishing Attacks

□ Create a "security awareness culture." It is essential that company leaders buy into the importance of cybersecurity and support, promote richer cyber training programs, and emphasize security in company communications.

□ Utilize trusted training vendors or platforms that allow for custom curricula tailored to the organization and employee roles and that take into account the fast-evolving nature of threat actor methodologies.

□ Make it easy for users to report suspected phishing emails; ensure reports are promptly reviewed and actions are taken on such messages.

□ Visually alert users concerning attachments from external senders. This may help identify spoofed domains that appear similar to the company's domain.

□ Develop comprehensive training that includes—and goes beyond—phishing and spear phishing. Include other social engineering concerns that involve physical security, industry best practices against device loss, insider threat indicators, etc.

□ Tailor web-based modules to individual groups that are pertinent to their roles and how they may be specifically targeted so employees can better spot and avoid tactics that may be used against them.

□ Hold across-the-board training annually and a mid-year "refresh" that builds on specific areas of emphasis, such as advanced techniques, for all employees.

□ Gamify security training to better engage employees by setting goals, rules for reaching the goals, rewards or incentives, feedback mechanisms, and leaderboards. Organizations can compete against each other.

□ Track leading performance indicators for your phishing tests so you can adjust phishing content and difficulty based on the needs of the organization.

□ Encourage users to store sensitive information via a file share with role-based access controls rather than in email.

- □ Leverage email security solutions that scan attachments and message contents as well as assess sender reputation.
- □ Use anti-spoofing and email authentication techniques, such as Sender Policy Framework (SPF).
- □ Consider blocking account logins based on geographic regions if not needed for normal business operations.
- □ Adopt advanced phishing protection/machine learning solutions or other third-party solutions to detect and deter sophisticated phishing campaigns. Consider automating your phishing response activity to reduce the human touch required.

Patching Recommendations to Keep Your Organization's Systems up to Date

- □ Inventory all IT assets (including storage, switches, laptops, etc.) across the entire distributed organization through automated discovery tools to get a clear picture of what you have to manage.
- □ Prioritize your patching needs. Determine which vulnerabilities represent high, medium, or low risk and their level of priority for the business according to your organizational risk tolerance.
- □ Have a schedule for deploying patches regularly. Consider a minimum cadence of once a month, with the option to deploy high-priority patches out of cycle when necessary.
- □ Test your patches in a development QA environment to ensure they won't "break the system" once deployed into production.
- □ Once patches are deployed, monitor them for stability. This may also include monitoring your network for stability.
- □ Remove systems that are running on operating systems that are no longer supported.

65% of known cloud security incidents were due to misconfigurations.

Recommendations to Secure Your Cloud Environment

- □ Periodically evaluate what data is accessible or exposed on the public-facing internet.
- □ Consider an attack surface management solution to help track vulnerable systems and unmanaged cloud assets.
- □ Leverage expertise in cloud security per platform. Managing security in the cloud requires expertise catered to the nuances of each platform. The more complex the platform, the more plentiful the opportunities for errors that can inadvertently disclose data.
- □ Ensure users with cloud control access are fully trained in each cloud environment.
- □ Evaluate your options for managed security services if you don't have the in-house expertise or if your cloud estate is particularly complex and in a continual state of change.
- □ Control access to the cloud environment. Access to cloud controls such as CSP consoles, APIs, and CLIs in the cloud should be restricted to only those who need it. Such RBAC is essential to minimizing the risks of configuration and other security errors.

□ Separate administrative and user credentials, and limit everyday users to production environments.

□ Implement allow listing where possible to further limit access to known and trusted endpoints.

□ Regularly audit your cloud data to know what sensitive data you have and where it's located.

□ Encrypt sensitive data (at a minimum), segment it, provide access using RBAC, and rotate keys regularly. Evaluate whether maintaining keys with the cloud provider or within your organization is the best option for you, but ensure you have a key security policy that limits key access and exposure to risk.

Shore up Security Operations with Cortex

As we know, security operations run on a finely tuned balance of people, processes, and technologies. To that end, we want to introduce you to a complete suite of security solutions designed for the SOC.

The Cortex portfolio offers an end-to-end security solution that helps you improve detection and operational efficiencies across your security operations. These technologies power our Palo Alto Networks SOC and thousands of SecOps worldwide.

Cortex XDR helps keep your organization safe from attack by delivering leading endpoint protection and enterprise-wide threat detection and response across network, cloud, endpoint, and virtually any data source. Patented behavioral and machine learning-based analytics pinpoint evasive threats and provide the intelligence you need to respond before a breach can occur. Don't wait to connect the dots after an attack happens; shut it down *before* a breach happens.

Cortex XSOAR provides a single platform for your SOC to manage incidents and automate workflows for maximum operational efficiency. Any of the processes listed in the checklist that are manual and repetitive can be a candidate for automation. And with over 900+ prebuilt automation packs for key processes such as user access control, phishing response, vulnerability management, cloud security, etc., XSOAR can serve as your virtual partner in the SOC to speed up incident response and ease daily analyst workloads.

Cortex Xpanse knows your cloud is always changing and exposing security gaps. All it takes is one gap for an attacker to compromise your network. Xpanse constantly monitors your attack surface to give you an up-to-date inventory of your internet-facing cloud assets and misconfigurations. Discover shadow IT before an attacker does.

With end-to-end native integration and interoperability, SOC teams can close the loop on threats with continual synergies across the Cortex ecosystem. All three products work in concert to monitor the threat landscape and provide the most robust detection, response, and investigation capabilities:

- Cortex XDR and Xpanse provide ultimate visibility and detections across the internet attack surface, endpoints, cloud, and network, including remote workers.
- Cortex XDR can leverage XSOAR to automate malware investigation and response.
- Cortex Xpanse and XSOAR work together to automatically enrich incidents using Xpanse asset information and automate the remediation of newly discovered assets.
- Cortex XSOAR ingests alerts and threat intel from all Palo Alto Networks products and hundreds of other security tools to facilitate incident investigation and drive automated incident response.

Detect and Respond to Cyberattacks 24/7 with Unit 42 MDR

Unit 42 security experts apply their years of experience protecting organizations to monitor your environment and look for suspicious activity. Our analysts leverage Cortex XDR to aggregate security telemetry from endpoint, network, cloud, and identify sources and apply high-fidelity threat intelligence and AI-powered analytics to prevent, detect, and respond to the most advanced threats.

The Unit 42 MDR team uses a mix of proprietary processes, infrastructure, and enrichment to swiftly stop the malicious activity that might impact your organization by accelerating detection, response, and threat hunting.

Initiate Your Response Within Minutes with a Unit 42 Retainer

The clock starts immediately when you've identified a breach. If you don't contain the breach right away and determine the root cause, your adversary will be back in your environment again.

With a Unit 42 Retainer, our experts become an extension of your team on speed dial, helping you respond faster so you can minimize the impact of an attack and get back to business sooner.

What's Next? Future-Forward with XSIAM

While Cortex products address key SOC requirements for visibility, protection, and automation, most organizations still depend on SIEM as a core component of SecOps. But SIEM products have failed to deliver on the promise of effective centralized threat detection and response, burdening analysts with endless alerts and manual processes. Security teams need a central platform that incorporates and automates multiple security functions into a single foundational solution with visibility into enterprise-wide security data.

Extended security intelligence and automation management (XSIAM) is purpose-built to address this need, harnessing the power of AI-driven automation to radically improve security outcomes and transform the manual SecOps model. By building an intelligent data foundation and automating unified SOC functions, XSIAM accelerates response, outpaces threats, and dramatically streamlines analyst activities.

For more information on how the Cortex suite of products can deliver best-in-class threat detection, prevention, attack surface management, and security automation capabilities, download our whitepapers:

Building a Virtual SOC Platform with Cortex

How to Plan for Tomorrow's SOC, Today

Check out the Unit 42 2022 Incident Response report for a more in-depth look at today's cyberthreat landscape, as well as favorite tactics that threat actors like to use.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com