CYBERARK

CHECKLIST TO ASSESS VULNERABILITIES FROM ADVANCED, SOPHISTICATED ATTACKS

Use this checklist to quickly assess your readiness in the event of an advanced, stealthy attack. For help with risk mitigation, consider CyberArk's PAM Rapid Risk Assessment and Remediation Offer.

	Already There	Medium Effort	A lot of work
To mitigate the risk of credential theft, how easily could you:			
Quickly identify all administrative accounts, including Windows accounts, Databases, Service Accounts, Linux accounts and SSH Keys?	☐	☐	☐
Determine which users have a higher level of privileged credentials then required to do their job?	☐	☐	☐
Do the same for non-human consumers of high privilege secrets like applications, bots, third party security tools, OS services?	☐	☐	☐
Secure privileged access to CI/CD platforms (consoles and CLIs), PaaS admins and other cloud privileged entities?	☐	☐	☐
Reduce the permission and/or manage the associated service account for any embedded OS services that are running as domain admin?	☐	☐	☐
To upgrade protection beyond simple usernames and passwords, how easily could you:			
Implement the kind of Multi-Factor Authentication (MFA) that uses contextual information to choose the authentication factors to apply?	☐	☐	☐
Enforce MFA across cloud and on-premises apps, workstations, VPNs, network devices, servers, etc.?	☐	☐	☐
Provide a choice of authentication methods: passwordless factors, hardware tokens, authenticator apps, etc.?	☐	☐	☐
To sharpen your ability to detect and stop lateral and vertical movement, how easily could you:			
Implement session isolation and monitoring (with credential boundaries where appropriate) to limit an attacker's range of motion	☐	☐	☐
Individualize and randomize credentials to break the attack chain?	☐	☐	☐
Regularly rotate credentials to limit an attacker's window of opportunity?	☐	☐	☐
Protect application credentials by replacing hard-coded credentials with a secure approach, such as an API call to fetch the secret from a digital vault?	☐	☐	☐
Eliminate shared common credentials across endpoints to prevent easy traversal	☐	☐	☐
Record these sessions to be able to later check all the administrative activity carried out before detection of a compromise?	☐	☐	☐

	Already There	Medium Effort	A lot of work
To improve your control over privilege escalation and abuse, how easily could you:			
Implement least-privileged access controls at the OS level in the most widely deployed platforms: Windows, Unix and Mac endpoints?	☐	☐	☐
Move to a Zero Trust model yet encourage adoption by implementing just-in-time security controls?	☐	☐	☐
Eliminate credentials that are no longer needed?	☐	☐	☐
Identify and review all new privileged or administrative accounts?	☐	☐	☐
Temporarily grant access to higher levels of privilege?	☐	☐	☐
To more easily spot privilege-related anomalies, how easily could you:			
Automatically analyze privileged activity, identify suspicious actions and detect attacks in progress?	☐	☐	☐
Analyze data from multiple sources, using advanced algorithms to intelligently establish baselines, evaluate threats and prioritize risks?	☐	☐	☐
Analyze privileged account behavioral data at the individual user level against specific criteria?	☐	☐	☐
Generate alerts of incidents that may lead to a breach, assigning a risk score to for each incident?	☐	☐	☐
Automatically require stronger authentication when anomalies are detected?	☐	☐	☐
Monitor for managed credential use outside the PAM solution?	☐	☐	☐
Implement bidirectional feeds that provide privileged threat anomalies, and ingest detections from other monitoring solutions?	☐	☐	☐
Use a canary in the system or implement other deception technologies to help expose the presence of attackers.	☐	☐	☐

SO HOW MUCH WORK WILL IT BE TO ASSESS AND REMEDIATE RISK FROM AN ADVANCED ATTACK?

If the majority of your tick marks fall in the "A lot of work" column, consider these services from CyberArk:

CyberArk Privileged Access Management (PAM) Rapid Risk Assessment: CyberArk offers a no cost assessment that includes the CyberArk Discovery and Audit (DNA) tool run against a representative sample of their Windows IT and/or Unix infrastructure. Based on the scan, customers will receive curated remediation recommendations with several 'sprint' tactics for short-term success.

CyberArk Privileged Access Management (PAM) Rapid Risk Remediation: CyberArk and our certified partners can assist customers to prioritize PAM controls including credential management, multi-factor authentication, session isolation, and least privilege on servers and workstations to prioritize servers for rapid risk reduction.

Such measures will be based on findings from the organization's incident response readiness and in alignment with the CyberArk Blueprint for PAM Success.

For more resources on how to mediate risk, visit CyberArk's Identity Defense-in-Depth webpage.