ALERT LOGIC™

Cybersecurity Checklist

Part 2:

Mitigating Post-Exploitation Techniques

In our first cybersecurity checklist, we provided a security overview and best practices to help organizations prevent an initial compromise from occurring. In this guide, we will help you understand practical steps you can take to mitigate techniques attackers use once they have penetrated your defenses. Once attackers have access to a machine, they can evade detection by using fileless techniques and legitimate system administration tools to do their dirty work. With this checklist, you will have a guide to help mitigate the impact of an attacker. Lastly, we will hep you understand how partnering with a company like Alert Logic can provide better defenses to stop attackers in their tracks.

This checklist helps to explain how to:

- How to manage and limit PowerShell access
- Securing and utilizing Windows Management Instrumentation (WMI)
- Ways to apply application controls
- Following the principle of least privilege and applying access controls
- What to monitor for to help uncover malicious activity

Lastly, we will cover how partnering with a company like Alert Logic can assist you will implementing a security solution that will advance your capabilities far faster than you can achieve on your own. By partnering with a managed security provider, organizations gain access to a modern, always-advancing set of technology to help secure their business, the intelligence to provide context to security decisions, and expertise and remediation guidance to help secure their business.

Manage And Limit Powershell Access

- [ ] **When PowerShell is not necessary, disable it**
PowerShell is a powerful scripting framework that can provide attackers with a wide variety of dangerous functionality.

- [ ] **When PowerShell is necessary, take the following steps:**

UPDATE TO LATEST VERSION OF POWERSHELL
It provides additional logging and updates to security features that can otherwise be bypassed on older versions (specifically version 2).

BLOCK UNSIGNED POWERSHELL SCRIPTS
While attackers can bypass this and other execution policy, attempts to do so can make attacks more visible.

CONSIDER USING POWERSHELL CONSTRAINED LANGUAGE MODE
Using PowerShell constrained language mode limits PowerShell to basic functionality. This renders many fileless attack techniques unusable.

ENABLE AND MONITOR EXTENDED POWERSHELL LOGGING
Just be prepared for this to generate a lot of events. Tools like PowerShell Method Auditor can help process them.

Secure & Utilize Windows Management Instrumentation (WMI)

- [ ] **Create Defensive Permanent WMI Event Subscriptions**
Its wide range of powerful admin capabilities make WMI a popular target of abuse, but they also make it a great tool for logging and responding to malicious activity.

- [ ] **If There's No Need for Remote WMI**
Consider setting up a fixed port for WMI and blocking it.

Apply Application Controls

- [ ] **Limit the Execution of Executables, DLLs, and Scripts with AppLocker**
  How restrictive you can be with whitelisting will depend on your organization's needs. There is always a balance between security and the needs to run businesses efficiently.

- [ ] **Take Additional Steps to Harden AppLocker**
  As with any security measure, there are ways of bypassing AppLocker. Look for our future blog on how to create rules that mitigate that risk. balance between security and the needs to run businesses efficiently.

Apply Least Privileges & Access Controls

- [ ] **Exercise Least Privilege**
  As best practice, users should be given the bare minimum of access and privileges necessary, limiting the damage they can do if compromised. Microsoft's Just Enough Administration can help.

- [ ] **When Possible, Use Highest UAC Enforcement Level**
  That includes setting UAC to "always notify," which will trigger prompts whenever a program attempts to make changes to Windows settings or the machine (yes, this can be annoying).

- [ ] **Enable Admin Approval Mode**
  It enforces UAC for the built-in Administrator, which can help thwart privilege escalation and lateral movement attempts.

- [ ] **When Possible, Use Highest UAC Enforcement Level**
  That includes setting UAC to "always notify," which will trigger prompts whenever a program attempts to make changes to Windows settings or the machine (yes, this can be annoying).

- [ ] **Remove Users from the Local Administrators Group**
  This can also help prevent privilege escalation attempts.

- [ ] **Disable Credential Caching**
  Don't allow storage of credentials or network authentication. Anytime credentials are stored it presents attackers with an opportunity to grab them.

- [ ] **Avoid Credential Overlap Across systems**
  This can help prevent lateral movement opportunities if valid credentials are obtained.

- [ ] **Avoid Staying Logged In On Remote Systems**
  Otherwise you open yourself up to attackers hijacking your admin access and privileges.

- [ ] **Disable Anonymous Login for Read and Write Access to Network File Shares (NFS)**
  Open shares provide a pivot point or means to further further spread an attack to other users on the network.

- [ ] **Disable Anonymous Login for Read and Write Access to File Transfer Protocol (FTP)**
  For the same reasons stated above for NFS.

- [ ] **Use Strong Passwords**
  Should go without saying, but obviously still a major common problem.

- [ ] **Utilize 2FA When Possible**
  Requiring two factor authentication can help keep attackers out even if they've successfully stolen passwords.

- [ ] **Apply Account Lockout Policies and/or Progressive Delays for Logins**
  This can help thwart brute force attempts.

What To Monitor For...

- [ ] **Changes In The Registry**
  Hiding scripts in the registry is one of the most common ways attackers gain persistence. Using WMI subscription events and/or tools like Sysinternals Autoruns can help.

- [ ] **Suspicious WMI Activity**
  Again, creating defensive WMI subscription events can help.

- [ ] **Scheduled Task Creation**
  Scheduled tasks can be used to achieve persistence and escalate privileges. Track creation with PowerShell scripts.

- [ ] **Suspicious Processes and API Calls**
  Monitoring for specific calls in the PowerShell operational log can provide strong indication of attacks. Using tools like Systernals Process Explorer and Get-InjectedThreads can also help.

- [ ] **Processes Being Spawned with the CREATE_SUSPENDED flag**
  This is a good indication of process hollowing.

ADVANCE YOUR SECURITY PROGRAM

Alert Logic is the only managed detection and response (MDR) provider that delivers comprehensive coverage for public clouds, SaaS, on-premises, and hybrid environments. Since no level of investment prevents or blocks 100% of attacks, you need to continuously identify and address breaches or gaps before they cause real damage. With limited expertise and a cloud-centric strategy, this level of security can seem out of reach. Our cloud-native technology and white-glove team of security experts protect your organization 24/7 and ensure you have the most effective response to resolve whatever threats may come. Founded in 2002, Alert Logic is headquartered in Houston, Texas, with business operations, team members, and channel partners located worldwide, and online at alertlogic.com.

Alert Logic – unrivaled security for your cloud journey.