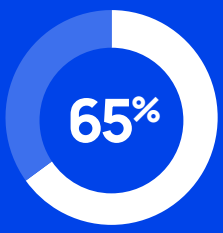
adlumin

INDUSTRY

Government

Challenge

Unnecessary alerts were being produced daily and the behavior was flagged as abnormal.



Solution

Adlumin's MDR team reduced the client's alerts by 65%.

ADLUMIN SUCCESS STORY

How Adlumin's Managed Detection and Response Services Reduced Government Client's Notifications by 65%

Unnecessary Alerts Were Being Produced

Adlumin's Managed Detection and Response (MDR) team escalated and alert that had been consistently triggered. An excessive number of alerts were being created per day for the client. Immediately, the MDR team flagged this as abnormal behavior and were on the hunt to find the root cause.

It became known that the account in question had triggered alerts in the decommissioned server and the newly upgraded server. Additionally, the account was already deleted from the decommissioned server before the handoff to the new system. Now, the team is tasked with determining why these alerts were going off and if there was a malicious threat actor in the environment.

The Phantom Account Discovered

Adlumin's MDR team immediately contacted the client via a two-way communication tracking ticket to inquire about the account firing off unnecessary alerts. The client indicated that the account was previously deleted and questioned how a 'nonexistent' account was still triggering alerts.

The team reached out to the customer via a virtual 'war room' to assist with the 'phantom' account that was still creating alerts. While sharing their local computer screen, Adlumin's MDR team and the client took a deep dive into their system(s) and were on the hunt to identify and eliminate all avenues of where the 'phantom' account was coming from.

About Adlumin

What you can't see poses the greatest risk to your organization. Your exposures lurk in the cloud, hybrid environments, and the darknet. There are countless gaps where threats can hide before they lead to business disrupting events like ransomware shutdowns or massive data breaches.

Adlumin Inc. is a patented, cloud-native Security Operations Platform plus Managed Detection and Response Services. The platform focuses on advanced cyber threats, system vulnerabilities, and sprawling IT operations to command greater visibility, stop threats, reduce business risk, and automate compliance. The command center for security operations, Adlumin leverages powerful machine learning, identifies critical threats, orchestrates auto-remediation system updates, and provides live continuous compliance reporting. Don't let your IT organization be caught in the dark.

Illuminate Threats, Eliminate Risks, and Command Authority with Adlumin.

www.adlumin.com
(202) 352-8001

COM-0036. Rev 3 , 05/2023

Shortly after, the account was identified as a task account to the local machine and utilized as a service account. After further review, Adlumin's MDR team recognized an additional source to the trigger as an alert created by a previous team. The alert was triggered due to an artifact that both the old and the new servers contained. The client deemed this non-threatening during the 'war room' call.

The newly identified 'phantom' account was disruptive and triggered many unnecessary notifications to the local government entity. Adlumin's MDR team and the customer agreed to remove the detection since it was identified within the systems as non-malicious, reducing their alerts by 65%.

Adlumin's MDR Team Keeps Customers Protected

Adlumin Security Operations Platform and Managed Detection and Response (MDR) Services brings light to threats within any organization by taking a proactive approach. The MDR team detects abnormal activity, including when there is an abnormal alert. They provide complete visibility so that anyone can understand what threats are inside and outside their IT landscape. With full-enterprise data integration and visibility, local government entities can report on their security maturity by demonstrating compliance with industry standards and legal requirements.

Adlumin's MDR team works as an extension of any client's security team, 24x7. Everything is included in Adlumin's Security Operations Platform to build a security operations command center out of the box.

No matter the time, Adlumin discovers and scans new assets for known and unknown vulnerabilities and threat-prioritizes any vulnerabilities. This government client took control of their IT environment and let Adlumin assist them with improving their overall operations and cybersecurity posture.

Next Steps:

- How Adlumin's Managed Detection and Response Services Reduced Government Client's Notifications by 65% is included in our series of customer success stories. For more information about how Adlumin's MDR Team works as an extension of our client's team, browse more here.
- Request a demo with an Adlumin cybersecurity expert if you are ready to get started.