CUSTOMER SUCCESS STORY

adlumin™

Shedding Light on the Unknown: A Security Operations Platform

Challenges

- Previous solution failed to detect malicious activity or provide any alerting on lateral movement.
- Cybercriminals work outside of working hours, so the firm needed 24x7 security.
- Needed a security analytics platform to discover threats, malfunctions and IT operation failures.
- Looking for a platform that could visualize usage, web, and project execution metrics from their system.

Results

- User & Entity Behavior Analytics (UEBA) helped determine and account for system's normal behavior pattern, and identify anomalies.
- Complete security and analytics provided for the firm's large enterprise networks.
- 24x7 Managed Detection and Response services supported the firm during their investigations.

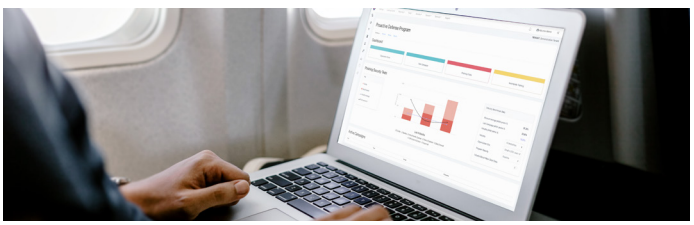
An International Cybersecurity Incident-Response Firm Detects Unauthorized Activity

The firm, a well-established U.S.-based international cybersecurity incident-response organization, is based in Washington, DC, and has nearly 2,000 employees and 100 IT experts. The firm responds to a call when a breach is discovered, bringing many years of investigative experience and tools to the situation. It sought an investigative tool that would help them detect and scope unauthorized activity in a client's network, be easy to deploy and operate, and help them rapidly contain and deny cyber threat actor activity. With those non-negotiables in mind, in 2018, Adlumin's Security Operations Platform became the primary investigative tool for the incident response firm's cyber investigations practice.

Looking for More Than a SIEM

In 2020, the Federal Bureau of Investigation (FBI) notified the firm's client that a threat actor may have acquired unauthorized access to their network. The the firm's client relied on a high-ranking Gartner Upper Right Magic Quadrant "highly rated" Security Information and Event Management (SIEM) platform. Unfortunately, that platform did not detect the activity nor provide any alerting on lateral movement. After being notified, the company engaged the firm to investigate.

FBI brought the issue to light, and the investigation followed. While the deployed SIEM had some form of artificial intelligence, the SIEM didn't adequately detect and alert the client that there were abnormal lateral movements in the network or even an intrusion in progress.



Adlumin Detected Threats When Firm's Previous Solution Failed

Based on Adlumin's User & Entity Behavior Analytics (UEBA) and Adlumin's Adlumin's Security Operations Platform, the firm found a persistent threat with administrative-level access to the client's Active Directory (AD) environment; Adlumin's platform even provided graphics showing exactly how the intruder entered the network after the breach.

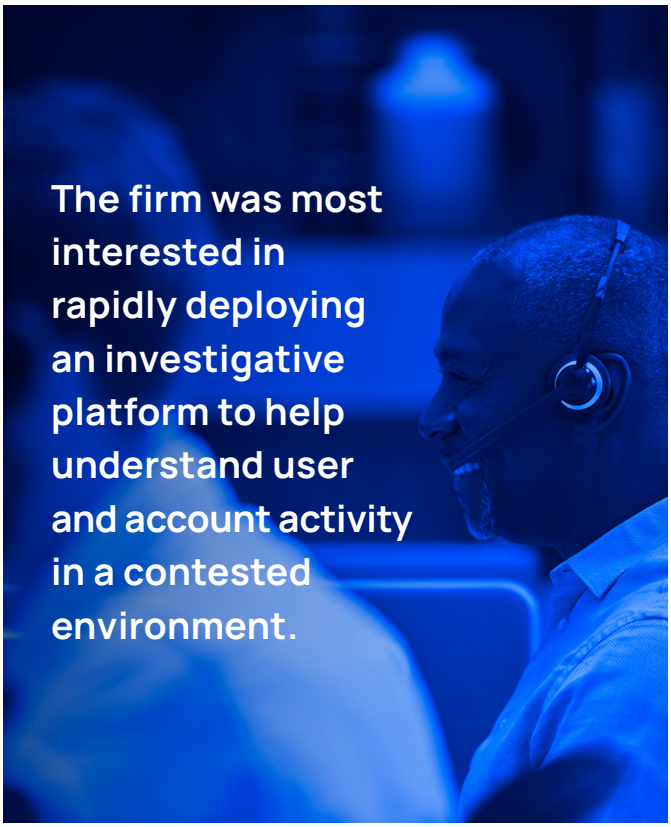
Within a short time, the platform mapped out the environment, triggered on-account anomalies, and guided the investigation to uncover Kerberos forgery issues. Adlumin then assisted the team with scoping unauthorized access, containing the threat activity, and denying further exploitation of the environment. As a result, the unauthorized activity was eradicated, and the response and investigative process introduced the client to the MDR tool—precisely how it handles windows security events and identifies abnormal activity. As a direct result, the client purchased the Adlumin's Security Operations Platform..

> "With Adlumin, we can understand which users are leveraging certain devices, installed and shared applications, and gaining a holistic view of the global environment, which is a force multiplier."
>
> - -- Senior Director of IT at Cybersecurity Incident-Response Firm

Provided Support Outside of Working Hours

The firm is often asked to help with nation-state exploitation and long-term investigations into cybercriminal exploitation activity and with such tasks comes big responsibility. The firm searched to find a Security Operations Platform and Managed Detection and Response (MDR) Services that could could handle a rapid response to an extended enterprise network with thousands of systems, defend its global environment, and prevent potentially ongoing data breaches during the investigation.

The firm also needed a solution that included User & Entity Behavior Analytics (UEBA), allowing each artifact discovery to become more intuitive. The firm was most interested in rapidly deploying a solution to help understand user and account activity in a contested environment. The old-school-traditional way of pulling logs and analyzing account activity was not quick or efficient enough for an incident response use case. The firm needed a platform that would provide intuitive and efficient visibility into user and account behavior in environments where unauthorized activity was suspected.



Adlumin is An Extended Part of Your Security Team

The firm and Adlumin's journey together is now spanning over three years. The firm explored and evaluated the platform's main features and beneficial capabilities, leading them to go to Adlumin when user/account behavior visibility was needed. Adlumin's platform core features like UEBA and Integrated Threat Intelligence gave cyber investigators rapid visibility into enterprise network intrusion activity that they were investigating for their clients.

Adlumin's One-Touch Compliance Reporting tools often serve as a pivotal differentiator, allowing analysts to customize reports and detection alerts for potential threats, breaches, or other anomalous activities on their network.

Adlumin's Security Operations Platform, UEBA, Integrated Threat Intelligence, and MDR Services also automates processes that investigators would have previously done manually (e.g., securing and understanding access/event logs across large numbers of accounts). The most valuable use case is when investigators encounter an extensive active directory user footprint. Adlumin's platform is a quick way to understand account, application, and activity risk.

Next Steps: Illuminate threats. Eliminate Risk. Command Authority

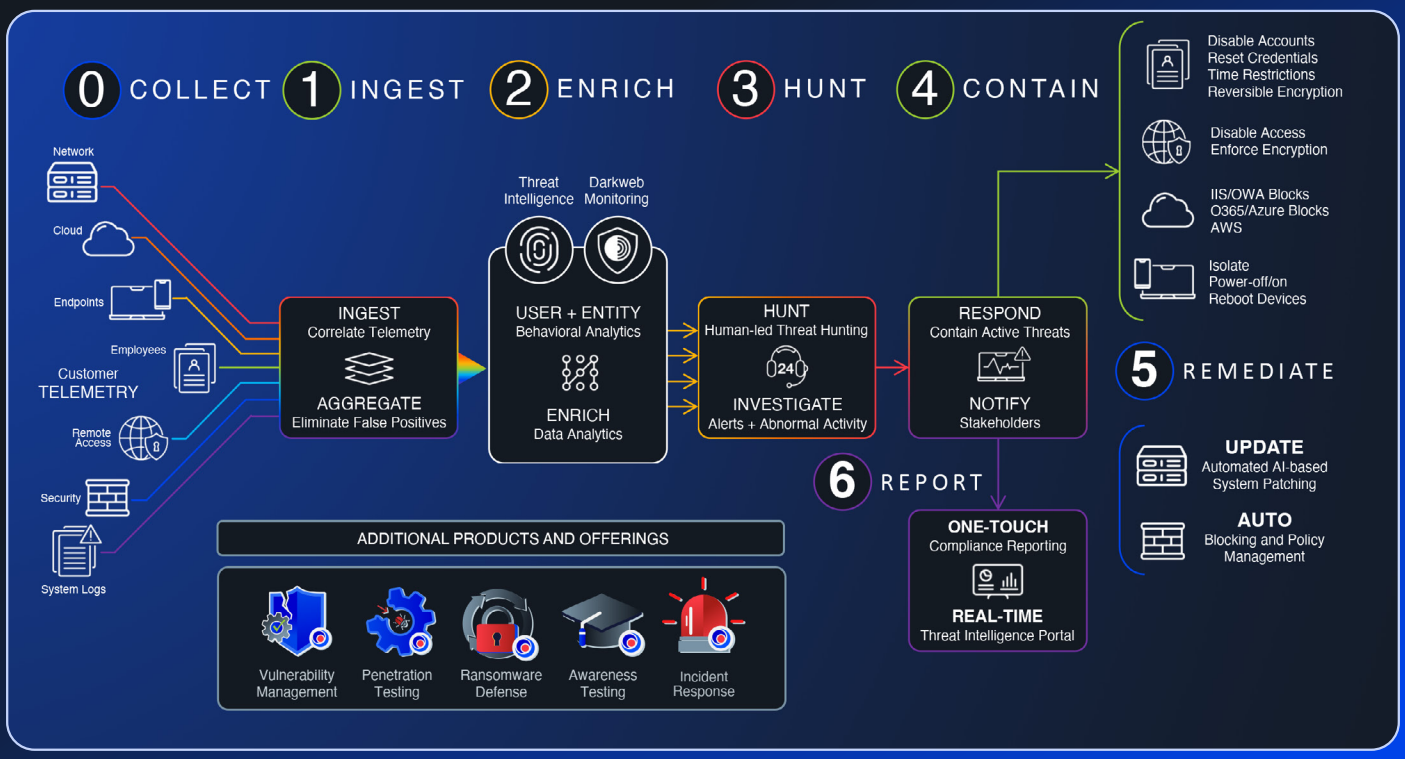
Adlumin's Security Operations Platform deployed in minutes and analytics began working and analyzing data immediately. This provided the firm with complete security and analytics coverage for their breached client's extensive enterprise network.

Adlumin's response to network exploitation events allowed the firm to deploy instant monitoring, detection, and visualization tools. This helped them serve clients more efficiently while ensuring advanced actors and persistence mechanisms were identified and contained.

The platform's UEBA data science also helped determine normal account and system behavior patterns. It then looked for all anomalies of that norm. Lastly, Adlumin's 24x7 MDR Services Team supported the firm's team during their investigations.

Adlumin Security Operations Platform

Adlumin's Platform plus MDR Services.
Your Command Center for Security Operations.



About Adlumin

Adlumin Inc. provides the enterprise-grade security operations platform and managed detection and response (MDR) services that keep mid-market organizations secure. With one license and one platform, its patented technology gives organizations and solution providers everything they need for effective threat hunting, incident response, vulnerability management, darknet exposure monitoring, compliance support and much more.

The Adlumin platform is feature-rich enough for organizations to operate on their own yet built specifically to amplify the skills and capabilities of managed service providers who use it to deliver cutting-edge security that can scale to meet the needs of any operating environment. With full access to the platform regardless of whether they are running it themselves or relying on Adlumin's MDR services or expert partners, Adlumin gives organizations unparalleled visibility into their security posture through access to alerts, investigation data, threat intelligence, compliance reporting and everything else – all in real time. www.adlumin.com