Customer Case Study | Ankura

Ankura is a well-established U.S. based international cybersecurity incident-response firm. When a breach is discovered and Ankura responds to a call, it brings many years of investigative experience and tools to the situation. Ankura 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, the Adlumin Security and Compliance Automation Platform became the primary investigative tool for Ankura's cyber investigations practice.

The Power of Partnership: A Short Story

In 2020, an Ankura client was notified by the Federal Bureau of Investigation (FBI) that a threat actor may have acquired unauthorized access to the client's network. At the time the 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 Ankura to investigate. Based on Adlumin's User & Entity Behavior Analytics (UEBA), Ankura found a persistent threat with administrative level access to the client's active directory environment; Adlumin even provided graphics showing exactly how the intruder entered the network after the breach.

The response and investigative process introduced the client to the Adlumin tool—specifically how it handles windows security events and the identification of anomalous activity. As a direct result, the client purchased the Adlumin platform, its second SIEM, and continues to be a valued Adlumin customer.

Key Points

WHY ADLUMIN?

- AI / Machine Learning
- Cost-Efficient
- Easy-to-Use
- Deploys in Less than 90 Minutes
- Simple & Complete Log Collection

RESULTS

- Adlumin's User & Entity Behavior Analytics (UEBA) helped determine an account or system's normal behavior pattern, and then it looked for all anomalies from that norm.
- Adlumin provided complete security and analytics coverage for Ankura's very large enterprise networks.
- Adlumin's 24/7 Security Operations Center (SOC) supported Ankura's team during their investigations.

Learning Point

During a recent breach response, Ankura discovered the breached customer was using one of the SIEM Platforms in the Gartner Upper Right Magic Quadrant and that the customer did not receive an alert that their network was breached. 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 customer that there were anomalous lateral movements in the network or even, an intrusion in progress.

Using the Adlumin platform, Ankura's investigation confirmed unauthorized access. The Adlumin SIEM was deployed in the customer's enterprise network to determine how the breach occurred by integrating with Active Directory (AD) and capturing lateral movement. Within a short time, the Adlumin SIEM mapped out the environment, triggered on account anomalies, and guided the investigation to uncovering 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 customer purchased the Adlumin SIEM despite having already owning another SIEM platform.

The Challenge

Ankura is based in Washington, DC, and has nearly 2,000 employees and 100 IT experts. The organization is often asked to help with nation-state exploitation and long-term investigations into cybercriminal exploitation activity. With such tasks comes big responsibility. The company searched to find a Security Information and Event Management (SIEM) platform that could handle a rapid response to an extensive enterprise network with thousands of systems, defend its global environment, and prevent potentially ongoing data breaches during the investigation.

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

Ankura was most interested in rapidly deploying an investigative tool that would help understand user and account activity in a contested environment.

The Solution

Ankura and Adlumin's journey together has spanned over three years. Since the beginning, the two companies have identified the evident value of their partnership. Ankura 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 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 as it allows analysts to customize reports and detection alerts for potential threats, breaches, or other anomalous activities on their network.

Adlumin's platform 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.

> *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."*
>
> ---- *Brandon Catalan, Senior Director*

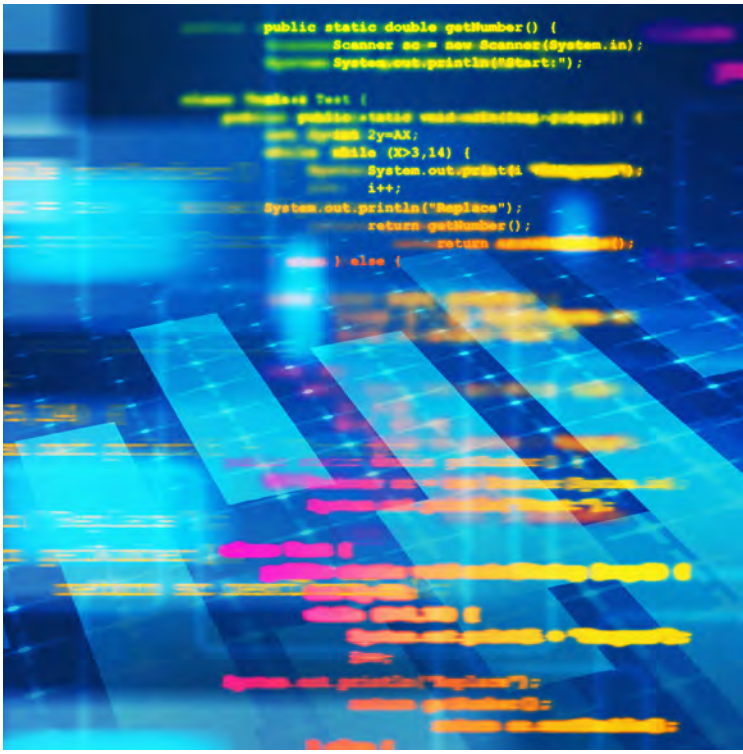
The Results

The Adlumin SIEM platform deployed quickly (within 90 minutes) and analytics began working and analyzing data immediately. This provided Ankura with complete security and analytics coverage for their breached client's extensive enterprise network.

The use of Adlumin's SIEM in responses to network exploitation events allowed Ankura to deploy instant monitoring, detection, and visualization tools. This helped them serve clients more efficiently while ensuring advanced actors and persistence mechanisms are identified and contained.

Additionally, the platform's UEBA data science helped determine normal account and system behavior patterns. It then looked for all anomalies of that norm.

Lastly, Adlumin's 24/7 Security Operations Center (SOC) supported Ankura's team during their investigations.



About Adlumin

Adlumin Inc. is a patented security and compliance automation platform built for corporate organizations that demand commercial bank-grade innovative cybersecurity solutions and easy-to-use, comprehensive reporting tools. The Adlumin team has a passion for technology and solving the most challenging problems through the targeted application of data science and compliance integration. Our mission is to "add luminosity" or visibility to every customer's network process through real-time threat detection, analysis, and response to ensure sensitive data remains secure.

About Ankura

Ankura Consulting Group, LLC is a global provider of a broad range of consulting services in the areas of strategy and performance; transactions, finance, and governance; data and technology; risk, forensics and compliance; disputes and economics; and turnaround and restructuring. We help clients protect, create, and recover value. Ankura has over 1,500 employees and more than 30 offices worldwide.