



How Ogden City Extended Their Security Operations to 24x7 with Adlumin's Security Operations Platform plus Managed Detection and Response Services

Challenges

- Seeking an extended security team to monitor 24x7 with alerting capabilities.
- Looking for a platform with higher security to protect against the rising ransomware attacks within its [industry](#).
- Seeking a cloud-native solution to fit their security plan and strategy better.

Results

- Signed with Adlumin for the next five years and deployed the Security Operations Platform plus extended risk management and security tools.
- Out-of-the-box cloud-native setup in 30 minutes, providing full-time visibility for Ogden City's network team.
- 100% [Extended Detection and Response \(XDR\)](#) capabilities and modules available to shed light on Ogden City's security journey.
- External view added to security program with [24x7 darknet monitoring](#) and automatic alerts to affected users or those responsible.





Ogden City Secures 1,000 Endpoints

Ogden City is a local government entity headquartered in Ogden City, Utah housing 700-1,000 employees, depending on seasonal hires. Ogden City's network team is responsible for securing civilians' data and every internal department, including engineering, accounting, law enforcement, and beyond. The organization primarily works as gatekeepers for highly personal and sensitive data. Its main goal is to secure all data from a technical standpoint while making it easily accessible for users. Additionally, they are tasked with maintaining regulatory compliance by providing a level of transparency that government entities require.

The Search for Consistent Alerts Lead to a 5-Year Contract

Before Adlumin, Ogden City worked with a Security Information and Event Management (SIEM) platform for several years. They soon discovered that they were looking for a platform and service to build the foundation of a [Managed Detection and Response \(MDR\) Center](#). Specifically, a platform that streamlines data ingestion, analysis, and compliance workflows throughout their enterprise. Their previous solution was bare bones and did not include all the features and products they have now, including their MDR services backed by experts and trained professionals, Snapshot 365, and SIEM platform.

As cyber threats change daily, Ogden City knew it had to get ahead of protecting its organization around the clock. Previously, Ogden City conducted an internal study to evaluate its security posture and noticed quite a bit missing. They looked to Adlumin to take their knowledge regarding their network environment and expand on it, providing its team with expert advice. After experiencing a [demo](#) and a [14-day free trial](#), they signed a 5-year contract with Adlumin.

Security Operations Deployed in 30 Minutes: A Cloud Vision Brought to Life

Ogden City describes its network as a hybrid with a cloud-native vision. The organization has over 1,000 devices and needed a solution that could start collecting data immediately and ingest environmental telemetry in real-time. When looking for a [Security Operations Platform](#), they highly considered moving onto a full-time cloud environment, as this is a significant factor when choosing any type of vendor. Adlumin offers a cloud-native and serverless solution that deploys in minutes, no matter the architecture or technology, without relying on hardware or software integrations.

Adlumin's [Security Operations Platform](#) is like no other. Everything is in one place, and an external view of their security landscape is within reach. The platform's [One-Touch Compliance Reporting](#) was a critical feature for Ogden City due to the standards and government regulations they are responsible for upholding. The module provides Ogden City's network team with compliance reporting based on live, accurate, and contextualized data. This allows them to instantly know where there are deviations from policy or misconfigurations that threaten their security posture.



“

“Something that stood out with Adlumin was how easy it was to implement and grab logs, whether it was on-prem or in the cloud, and then on everybody's desktops. We knew that it was going to be a chore or task, and it turned out that it wasn't. And that was a huge feature for us. It was set up in 30 minutes.”

— Brian Martinson, Networking Operations Manager at Ogden City



“

“Every vendor always says that they will do whatever we want, but Adlumin had an answer for when we asked, ‘what should we be doing?’ and they had some best practices [within our industry] we should start with. That helped us realize what the industry is seeing, not just Ogden City.”

- Brian Martinson, Networking/Operations Manager at Ogden City

Employees are 9-5, and Cybercriminals are not: A Security Team Extension

Municipalities must think from a proactive security mindset, especially when ransomware threats are growing. Cybercriminals do not work the regular 9-5; they are searching for the perfect entry point around the clock. Subsequently, Ogden City was looking for a security operations center that would be an extension of their network team. This was essential for Ogden City because they needed support outside regular work hours. Adlumin's MDR team monitors, anticipates, detects, and reports threats for them.

From a security standpoint, Ogden City's network team is in a much safer position. Adlumin's MDR offers 24x7 darknet exposure monitoring extending from internal to external, seeing the entire threat landscape. With automatic alerting included, exposed credentials are quickly identified and cleaned up with notifications to affected users or those responsible. This eliminates the need for Ogden City's team to darknet monitor and allows Adlumin to act as a proxy, empowering them to operate securely.

“

“We have dedicated full-time employees, but we are not 24/7, and our network is. So, that was a driving factor. Cybersecurity experience is great, and we welcome any that we can get. We feel we have a good handle on that, but we always love talking to the pros [Adlumin].”

- Brian Martinson, Networking/Operations Manager at Ogden City

Visibility in Action: Out of Country Logon Alerts

Adlumin's features changed how Ogden City's network team tackles incidents by bringing threats to light through its customizable alerts. Ogden City trusts that Adlumin will discover threats and alert them on and off working hours. When the network team comes to work, they have much more visibility into what is happening inside and outside their IT landscape.

For example, after Adlumin's [Security Operations Platform](#) was deployed within Ogden City's network, the network team experienced an incident where there was a logon from outside the United States. Individuals within the network team were immediately alerted by Adlumin's team to block the out-of-country logon. All source information and transparent insights were provided so the team could act quickly and confidently.

“

“It's not just alerting us. There is a team investigating behind it as well. It is accurate, and there are trained professionals that know what they are doing and are knowledgeable on cybersecurity and keep up in the field. Those were huge wins for us.”

- Brian Martinson, Networking/Operations Manager at Ogden City

Eliminate Risks. Exceed Expectations.

Municipalities should consider an [Security Operations Platform](#) that offers a 24x7 first-response MDR team in addition to 360-degree visibility bringing maximum illumination to security operations. Anti-virus programs or SIEMs are not enough to protect organizations when constant monitoring is necessary. Regardless of size or location, government cybersecurity is essential to mitigate the level of destruction ransomware and other cyberthreats can cause.

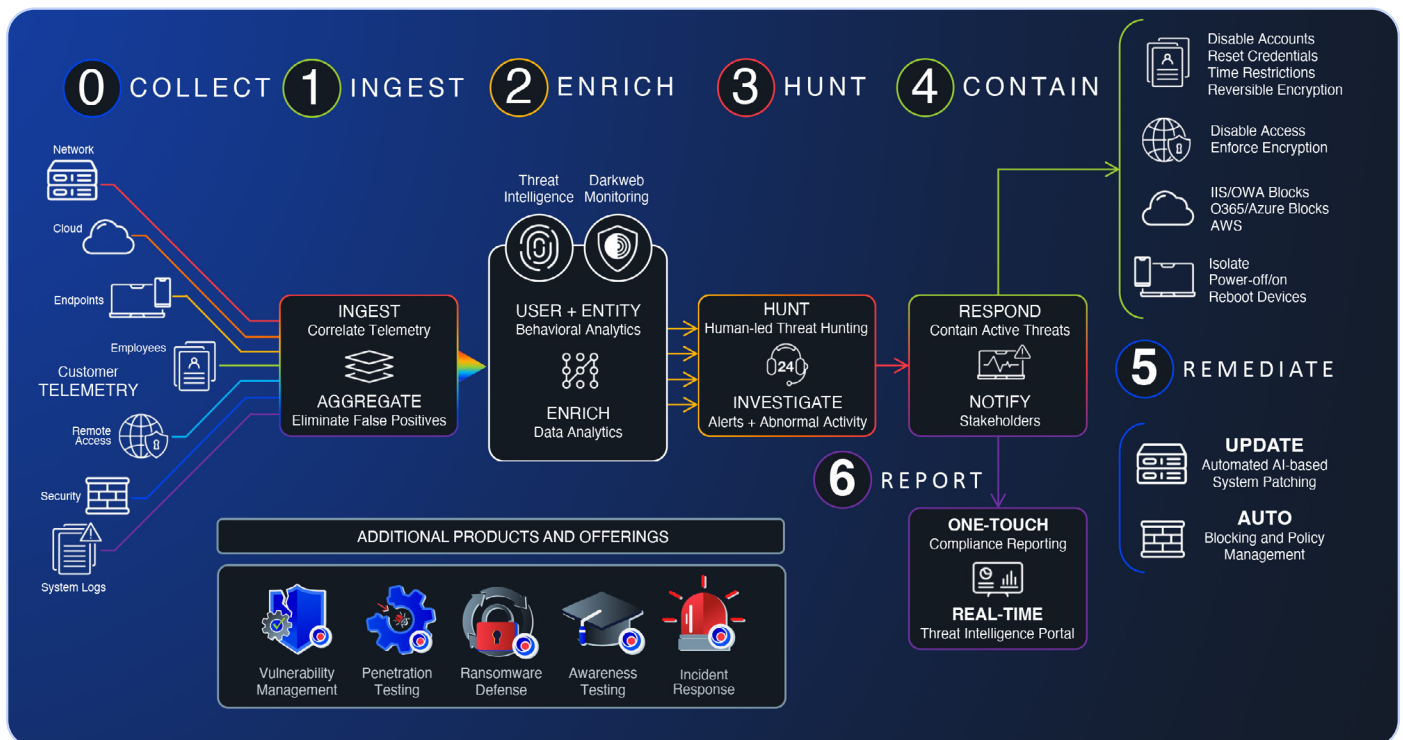


Ogden City's network team enhanced its IT environment and implemented a proactive security strategy. They found a platform tailored to combat threats within their industry. Specifically, they found a solution with advanced alerting that allowed them to command more visibility, authority, and options with Adlumin to stay informed about what was happening on their network.

Austin Knudsen, Network Admin at Ogden City, says, "We have more visibility into more aspects of our network than before. We are receiving alerts for Office 365 events, failed login attempts, and many others we never had. Adlumin has given us a better idea of what is happening behind the scenes and insight into what we need to start controlling and changing." Ogden City took control of its network and IT landscape by trusting Adlumin as its extended security team.

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