Three Critical Elements for the Perfect Security Operations Mix

By: Brittany Demendi, Corporate Communications Manager

Introduction

According to Gartner, data breaches broke records in 2021, which is why 88% of executives consider cybersecurity a top threat to their operations rather than a technical IT problem[1]. Organizations must invest in solutions that proactively and continuously protect against threats while offering automated solutions to mitigate the risk of an attack. Technologies and services are often expensive and complex requiring significant management. For this reason, many small-to-medium businesses turn to a Security Operations platform.

First Steps to Building the Foundation of Security Operations Platform

As the threat landscape evolves, compliance regulations follow suit, and the volume of data and emerging technology introduces new obligations and exposures. As a service, a Security Operations platform utilizes organizations' data by tracking and detecting threat trends across a broad base of monitored customers. The assistance from an extended security team is invaluable, as they manage the software and tools in your security stack and provide 24x7 emergency responses for

Table of Contents

A vast majority of organizations have chosen to find a Security Operations platform plus Managed Detection and Response (MDR) services mainly because of expertise, lack of resources, and cost-effectiveness. MDR services deliver benefits scaled for businesses of all sizes. Investing in security operations platform as a service immediately enables access to talented cybersecurity experts around the clock, scalability, lower ongoing costs, and shared threat intelligence.

To conclude our three-part white paper series, this paper explores three critical elements to incorporate into your cybersecurity strategy as your threat profile expands.

Critical Element 1: One-Touch Compliance

Stay Vigilant and Prove Compliance

Cybersecurity compliance is when organizations from all industries are required to uphold regulatory requirements and standards by establishing risk-based controls to protect data and information availability, integrity, and privacy. This can be a significant challenge for some, mainly because requirements and industry standards can overlap, leading to confusion or continuously evolve year-to-year.

However, despite these regulations being challenging, they are a driving force for many organizations' success. Complying with industry standards can be one of the first steps to setting a secure foundation for cybersecurity.

The Benefits

Avoid Fines and Penalties for Being Non-Compliant

Failure to comply with evolving regulations and laws can result in hefty fines and severe penalties. Staying up to date allows organizations to plan for and be proactive against data breaches.

Builds Customer Loyalty and Trust

When data breaches occur within an organization, trust becomes affected, which can and will have a negative impact on the company's reputation. This can create a domino effect causing business disruption, financial loss, and more.

Improves Data Management Capabilities

Organizations must keep track of all the data collected from customers and have a plan for where it is being stored safely. New data protection laws have been implemented where customers can ask organizations to delete data associated with their identities. This is causing many to revamp their data management plans in order to comply with data protection laws, which helps increase operational and management efficiency.

The Adlumin Difference

When an organization's operational and security data is with Adlumin, you receive instant access to ensure or prove compliance against any standard or custom requirement. Additionally, as your security program's command center, Adlumin's reporting module provides one-touch compliance reporting.

For example, **Utah State Bar** knows that the regulations the American Bar Association (ABA) issues provide a minimum standard for their legal industry, which is why they turned to Adlumin for more robust protection and instant access to their compliance reporting

.

Shifting regulations and standards, like PCI DSS, NIST, FFIEC CAT, NCUA ACET, HIPAA, and others, are becoming more than just checkbox or paperwork exercises. More security and risk teams are being asked to use data-driven processes to improve cyber risk maturity or show regulatory compliance.

Adlumin compliance support benefits include:

- Live Environmental Data
- Instant Variance Alerts
- Provable Compliance

Critical Element 2: User & Entity Behavior Analytics (UEBA)

Proactive Threat Detection

User and Entity Behavior Analytics (UEBA) is a cybersecurity process and analytic tool included within Adlumin's security operations that monitors 'normal' activity employees participate in daily. Activity is flagged if any abnormal behavior is detected or if there are deviations from an employee's 'normal' activity patterns.

For example, if a user consistently downloads five megabytes of assets daily but suddenly downloads ten gigabytes, this is considered abnormal, and your team would be alerted immediately. In other words, UEBA complements other security controls that detect implicit indicators of compromise (IoCs) (think antivirus detecting known malware). In contrast, UEBA identifies inferential IoCs before criminals can download malicious payloads.

How UEBA Works in Real-Time

The foundation of UEBA can be very simple. A cybercriminal can easily steal a user's login credentials, but it is much more challenging to convey that user's daily behavior once inside the network. Adlumin's UEBA looks for historical statistical outliers against models and behaviors within a system environment. UEBA maps behavior patterns for every user and entity, such as servers, laptops, and desktops. Once there is a detection of suspicious activity, it is flagged immediately.

For example, Adlumin's MDR team received an alert notification of impossible travel of an end user going from Massachusetts, U.S., to Germany for a financial institution client. The MDR team immediately flagged this alert and began investigating the issue.

Having a dedicated team gave this institution visibility beyond its boundaries by providing continuous monitoring, detection, and response 24x7. Adlumin's platform provided analysis and recommendations for confirmed incidents and proactive security actions by delivering high-confidence alerts. This institution took control of its IT environment and let Adlumin assist them with improving its overall operations and cybersecurity posture.

The Benefits

Traditional security tools, such as perimeter defenses, are easily bypassed by skilled cybercriminals. In simpler days, an organization was considered secure by having intrusion prevention tools, firewalls, and web gateways. However, we now recognize that larger organizations have porous perimeters that are also strenuous to manage.

Preventative measures are no longer sufficient. Firewalls are not foolproof, and cybercriminals will penetrate your system eventually. Detection is equally important so that if they intrude, their presence is immediately alerted to minimize the damage. UEBA is an essential part of security, allowing:

Compromised Account Detection
Human error is the number one reason for data breaches and attacks. Some users may unknowingly download malware, compromising their accounts. UEBA weeds out compromised users before damage is done.

Brute-Force Attack Detection
UEBA detects brute-force attacks when cybercriminals go after cloud-based entities and third-party systems. UEBA blocks access to these entities.

Insider Threat Detection
It may seem far-fetched that a trusted employee, or even a group of employees, could steal confidential data by abusing their own access, but it happens. UEBA detects sabotage, data breaches, policy violations, and privilege abuse.

Changes in Permission Detection and Super User Creation
UEBA allows organizations to detect super user creation or if any employee account was granted permissions without authority.

Breached Data Detection
Passwords are not enough to protect organizational data. UEBA detects when users access sensitive data when they have no reason to access it.

The Adlumin Difference

Adlumin's Security Operations Platform and MDR Services use proprietary artificial intelligence and machine learning algorithms to analyze account-based threats and write an organization's SIEM. **UEBA** is one way within the multi-layer detection approach, a light is shined on all threats stopping attackers before their mission is complete. Adlumin's UEBA data science helps identify, detect, analyze, and prioritize anomalous behavior in real-time.

It is the perfect balance of automation and machine learning paired with cybersecurity experts learning every behavior within a network. This includes analyzing where employees log on, the average times they log on, identifying any abnormal behavior, and alerting the MDR team when an activity needs attention. **Adlumin's UEBA** cranks up the power of an organization's searchlight and security risk.

Critical Element 3: Security Orchestration, Automation, and Response (SOAR)

Automate Manual Tasks

In addition to UEBA, another MDR capability deemed essential is Security Orchestration, Automation, and Response (SOAR). SOAR analyzes gathered data and deploys automated responses for each specific threat brought to light.

As defined by Gartner[2], a SOAR product combines threat intelligence platform capabilities, orchestration and automation, and incident response in one solution. In addition, Gartner continues, these tools are used for the following operation tasks:

- To document and implement processes
- To support security incident management
- To apply machine-based assistance to human security analysts and operators
- To better operationalize the use of threat intelligence

Workflows are typically automated and orchestrated via integrations. This technology helps execute, coordinate, and automate tasks between tools and people within one security operations platform. This allows organizations to be proactive against future attacks and understand future threats to improve their security posture.

The Benefits

SOAR takes the way security teams analyze, respond, and manage alerts and threats to the next level. When teams are tasked with manually handling hundreds, if not thousands, of alerts daily, there is no room for human error. Security teams are challenged with connecting the noise from contrasting systems. This makes it essential that organizations have systems, such as SOAR, that enable them to automate their response and alert processes and systematically orchestrate them.

SOAR allows the following:

Quick Incident Response
Many of the actions with a SOAR tool are automated. Therefore, a vast number of incidents are dealt with automatically and immediately.

Mitigation of Time-Consuming Actions
SOAR capabilities decrease the number of manual processes that analysts complete daily, false positives, and repetitive tasks.

Increased Decision-Making Capability
This process is aimed to be user-friendly and gather insights and data to make it easier for security teams to take the correct actions to evaluate incidents.

Reporting and Communication Improved
When everything is in one place to view, stakeholders can easily access all the requested information, including reports that can assist in making improvements to workflows and reducing incident response times.

Everything in One Place
Security teams can view everything from one platform and are provided with all the information needed to review and analyze any possible incidents.

Integration of Tools
All the different security tools can be connected to achieve a higher level of comprehensive analysis and data collection. There is no need to be flipping between various tools.

The Adlumin Difference

Adlumin's Security Orchestration, Automation, and Response (SOAR) capabilities provide a menu of remediation options to eliminate potential threats within minutes. Adlumin's SOAR can take automated and analyst-driven actions based on alerts to provide machine-time remediation solutions. SOAR functions can initiate and disable accounts in machine time to contain the threat and reduce the amount of damage done.

Impossible travel, suspicious remote access, account takeovers, lateral movement, and defense evasion are examined through the Adlumin patented UEBA engine. They are tied to the SOAR capabilities to automatically respond with an account or device blocks or used during broader investigations to identify compromised accounts or security groups, tampered devices or modified global policies.

Containment occurs at the account, device, system, or cloud service level through automated responses or as part of an orchestrated investigation with more granular actions taken on specific accounts and devices to avoid blackout denial of service or cascade effects across your environments. At the user, group, or systems level, you have the option to make surgical decisions rather than clumsy device resets and power-offs that might stop the adversary but also cripple logging and forensics collection.

Remediation

The Adlumin platform often streamlines tedious and technically challenging system updates and policy roll outs. Following an attack, IoC information is used to update block lists and autogenerate policies and rules that the platform can automatically push to network and security controls such as firewalls and UTMs. Auto-updates reduce management loads and reduce the risk of repeat intrusions through previously attempted vulnerabilities.

The Adlumin Advantage

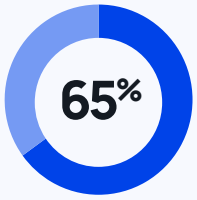
Around-the-Clock Response with Automation

Most technologies or managed services providers give organizations partial visibility or bare-minimum management resources. An Security Operations platform plus managed detection and response services offers differentiated delivery options. Adlumin's Security Operations Platform includes 100% extended detection and response (XDR) capabilities and modules to shed light on your security journey, providing a team with you at every step. Many IT teams are stretched to their limits and find it challenging to manage the ever-changing threat landscape. So, instead of trying to manage it all by themselves, they turn to Security Operations Platform as a service.

The Benefits

Cybercriminals don't work a 9-5 schedule; they work around the clock all year round. Most attacks occur during off hours, either on the weekends or in the late night/early morning, to maximize the probability of a successful attack. One of the main benefits of Security Operations as a service is the 24x7 network monitoring with the ability to respond immediately when any threat is detected.

For example, Adlumin's MDR team escalated an alert that had been consistently triggered. An excessive number of alerts were being created daily for a government entity client. Immediately, the MDR team flagged this as abnormal behavior and was on the hunt to find the root cause. The alert was triggered due to an artifact that both the client's old and new servers contained.



Adlumin's MDR team improves the visibility and action of priority alerts by 65%.

Implementing and utilizing 24x7 services, one-touch compliance reporting, UEBA, and SOAR capabilities is the start to a perfect mix to better your security posture. Adlumin allows customers to choose how they want to stay protected by managing our security operations platform themselves, through a trusted Partner, or engaging our Security Operations Platform 24x7. And no matter what, Adlumin is their Command Center for security operations giving easy access to everything in one place.

Let's continue the conversation.
Visit us at www.adlumin.com.

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

1. https://www.gartner.com/doc/reprints?id=1-29FBE5ZT&ct=220317&st=sb
2. https://www.gartner.com/reviews/market/security-orchestration-automation-and-response-solutions