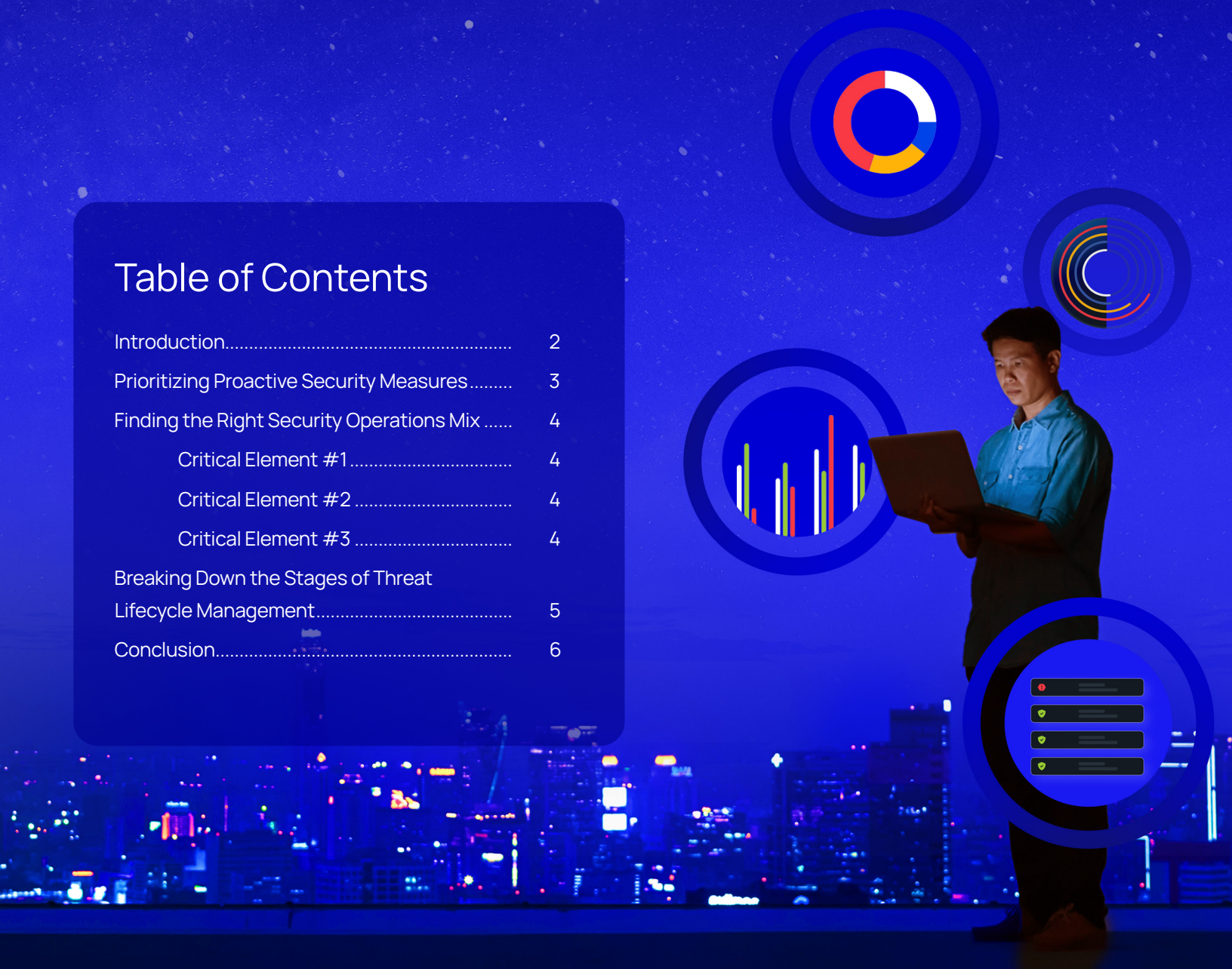
adlumin™

The Executive's Guide to Cybersecurity

Table of Contents



adlumin

Introduction

Ignorance is not bliss in a world of cyber breaches and massive ransomware outages–it's a potential liability. What you don't know or can't see often poses the greatest risk. Cyber risks lurk in cloud services, hybrid environments, and the darknet. In a typical business environment, there are countless gaps in which threats can evade detection before leading to a business disruption event.

In the face of persistent cyber adversaries, expanding digital exposures, and increasing accountability, organizations are struggling to focus constrained resources to manage these risks. Some typical gaps in mid-market organizations include a lack of cloud email security, weak Virtual Private Network (VPN) authentication, unpatched software, and more. However, the main cybersecurity issue many organizations face is the need for proper resources and visibility into an IT network to help identify these gaps in security.

So, what do you need to do to get proactive about security?

A good start is to address your organization's ongoing technical debt by retiring obsolete or unsecure IT systems. These systems require significant patching and are often no longer supported by its vendors. Cybercriminals use these vulnerabilities as well-known exploit vectors.

Streamlining IT infrastructure reduces your overall threat profile so you can focus monitoring and responding to IT systems most used by your organization. It also allows your IT and security teams to prioritize planning and training. With more effective incident response drills, everyone will know what to do when an incident occurs.

Prioritizing Proactive Security Measures

In the face of such odds, it's easy for business leaders to adopt a fatalistic approach. They might surrender to unstoppable threat actors and put too much faith in their backup systems and cyber insurance coverage to weather the storm. This absolutist perspective can lead to reluctance to invest in information security tools, personnel, or alterations to business processes because they cannot guarantee to resolve an issue completely. As the adage goes, there are never enough resources to do it right, but there are always resources to do it over.

This perspective commonly manifests in a bias toward minimum security requirements, skewed to investment in backup systems, disaster recovery services, and an incident response retainer. The fallacy and consequence of this mindset are expensive security breaches, lost productivity and revenue, costly penalties and clean-up costs, and irreparable reputational harm.

However, insurance companies are starting to notice the negative consequences of customers taking this approach. Most cyber insurance policies with claims lost money for the underwriter. Insurance companies are increasing premiums, reducing coverage, and tightening minimum policyholder security standards to break the claim-first response to security attacks.

People want a simple checklist full of things to do that will guarantee that their network is as secure as possible. Unfortunately, checklist security has been proven to be a dangerous and unhelpful approach to security. Every network is unique, so each must be audited by trained security professionals whose recommendations are then put into practice.

Want to learn more about the business benefits of being proactive and how to advance both your bottom line and information security? Read our full whitepaper on navigating proactive cybersecurity.

Read "The Importance of Proactive Security"

adlumin

Finding the Right Security Operations Mix

Complexity, skills gaps, and retention issues drive most mid-sized organizations to outsource security to organizations designed to keep pace with changing trends and offer challenging work to experts along multiple career paths. It's a win-win. Smaller organizations can tap these resources in a mutually cost-effective relationship.

In 2016, Gartner minted a new security category and published a Market Guide for Managed Detection and Response (MDR); spun from the incumbent Managed Security Services Provider (MSSP) magic quadrant. Traditional MSSP provides day-to-day management and maintenance of IT and security systems, with some alerting processes when a suspicious event is detected. MDR focuses on threats rather than device management and offers turnkey threat identification and containment delivered remotely via a 24x7 Security Operations Center (SOC).

A vast majority of organizations have chosen to find a security operations platform plus MDR services mainly because of expertise, lack of resources, and cost-effectiveness. MDR services deliver benefits scaled for organization 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.

This section explores three critical elements to incorporate into your cybersecurity strategy as your threat profile expands.

Critical Element 1: Threat Hunting

Threat hunting is often a manual process backed by automated searches and existing collected network data correlation. Proactive threat hunting quickly establishes itself as a critical pillar in security strategies and ensures situational awareness that other methods do not offer.

Critical Element 2: User & Entity Behavior Analytics

User and Entity Behavior Analytics (UEBA) is a cybersecurity process and analytic tool that develops a baseline of what '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' baseline activity patterns.

Critical Element 3: Security Orchestration, Automation, and Response

Another MDR capability deemed essential is Security Orchestration, Automation, and Response (SOAR). 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.

To dive deeper into what the perfect integrated mix of security operations looks like for your organization, read the full whitepaper here.

Read "Three Critical Elements for the Perfect Security Operations Mix"

Breaking Down the Stages of Threat Lifecycle Management

In the face of aggressive cyber adversaries, expanding digital exposures, and increasing accountability, organizations are struggling to focus constrained resources to manage risks. Below we examine the evolution of the threat landscape and the model by which you can protect your organization broken down into the following stages:

Stage 0: Collection

The first stage is to collect a full spectrum of security data and telemetry from across network access points, security controls, remote access points, employee activity, cloud services, systems logs, administrative actions, etc.

Stage 1: Ingestion

The ability to ingest security data includes normalization, correlation, and aggregation—the aggregated telemetry results in an enormous data set of log events, alerts, and analytics. Again, security operations move into the realm of data management.

Stage 2: Enrichment

The resulting data and telemetry are then augmented and enriched with threat intelligence feed correlation data with known common vulnerabilities or exposures (CVEs) and advanced persistent threats (APTs). Some vendors offer Darknet monitoring to expose previously compromised credentials and confidential information valuable to criminals in attacks.

Stage 3: Threat Hunting

Workflows and alerting in the MDR platform provide enhanced forensics information that facilitates analyst investigation of potential threats. As a turnkey service, SOC analysts provide tactical investigations of alerts and anomalies, conduct research, and determine if suspicious activity warrants containment or reporting.

Stage 4: Containment

When unauthorized activity or threats are identified, SOC analysts use a host of containment actions to prevent the attack from progressing to data exfiltration or a business-altering impact such as a ransomware outage.

Stage 5: Remediation

Post containment, MDR services have evolved to include basic remediation services, including automated blocking, policy management, system patching, and rules publishing based on discovered threats. This level of service reduces the risk of repeat or return attacks and streamlines device management.

Stage 6: Reporting

Client notification and portal-based ticketing and reporting are fundamental MDR platform components. However, this basic service often eludes vendors that have built swivel-chair or fractional services that prevent the automated generation of reports.

Interested in learning more about each stage of the evolving threat lifecycle and the importance of understanding MDR architecture? Read our full whitepaper here.

Read "Full Threat Lifecycle Management Model Applications"

Conclusion

Illuminate Threats, Eliminate Risks with Adlumin

Most technologies or managed services providers give organizations partial visibility or bare-minimum management resources. A Security Operations Platform plus Managed Detection and response services offer differentiated delivery options. Adlumin's Security Operations Platform includes the best of all MDR 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 managing the ever-changing threat landscape challenging. So, instead of trying to manage it all by themselves, they turn to Security Operations Platform as a service.

Implementing and utilizing 24x7 services, one-touch compliance reporting, UEBA, and SOAR capabilities is the start of 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 by engaging our Security Operations Platform 24x7. No matter what journey they take, Adlumin is their command center for security operations giving easy access to everything in one place.

EDR vs. XDR vs. MDR: The Cybersecurity ABCs Explained

What Solution Is Right for Your Organization?

This eBook guides you through the complex landscape of EDR, XDR, and MDR solutions, empowering you to make informed decisions and strengthen your organization's cybersecurity defenses. Download today!

Authors

Mark Sangster, VP, Chief of Strategy, Adlumin
Brittany Demendi, Corporate Communications Manager, Adlumin

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.