adlumin™

DATA SHEET

Adlumin Incident Response

Rapid Recovery When You Need It

Adlumin's Incident Response provides lean teams with the expertise necessary to understand the full scope of a breach, remove the threat, and provide actions to strengthen security. When faced with a security breach, gain the confidence of knowing you are covered every step of the way.

Our incident response team is comprised of highly skilled and certified professionals with extensive experience in cybersecurity incident response. With a deep understanding of the threat landscape and the latest attack techniques, we deliver expert guidance and support during critical incidents, ensuring your organization is in capable hands.

With Adlumin's incident response, you'll get:

Rapid Incident Response: Our incident response subscription offers a 24x7 dedicated response team that acts swiftly in the event of a security breach. With years of expertise paired with our Security Operations Platform, we minimize the threat and mitigate risk, reducing potential damage and downtime.

Comprehensive Forensics and Investigation: Adlumin's incident response experts conduct thorough forensic analysis to identify the root cause of incidents and gather critical evidence for post-incident analysis and regulatory compliance. Our detailed investigations not only help in recovering from the incident but also provide actionable insights to strengthen your overall security posture.

Advanced Threat Intelligence: Our team is continually researching the latest tactics and trends, so you gain insight into the threat landscape and what techniques are being used to evade detections. Our intelligence-driven approach ensures that your organization is protected from emerging threats and targeted attacks.

Proactive Threat Hunting: Adlumin takes a proactive approach by combining threat-hunting capabilities with our incident response subscription. Our dedicated team actively hunts for threats within your environment and neutralizes emerging threats before they escalate into full-blown incidents. We also provide retroactive analysis for certain major vulnerabilities to identify potential exploitation.

Get peace of mind knowing you are covered.

Adlumin's Security Operation Platform and Managed Detection and Response (MDR) offering already reduce risk by providing a multi-layer detection approach and a team monitoring your environment 24x7. Adversaries look to stay a step ahead and find ways to evade detection, especially in highly targeted industries.

With our Incident Response Subscription, you will get:

Complete Visibility:
As an Adlumin customer, your security data is being stored from across your whole environment enabling our team to respond quickly and be able to tell the full story, knowing the data hasn't been tampered with by the adversary.

Improve Security Posture:
You will get insights into the latest threats that have evaded detection, an understanding of any industry threat trends we are seeing, and a dedicated team actively looking for threats in your environment.

Minimize Expenses:
Eliminate any unexpected financial burdens associated with incident response. Our offering is designed for organizations with lean teams, we can quickly remediate incidents and get your business back into operation.

Better Together

Pairing our incident response capabilities, one year log retention*, with continuous threat monitoring and detection, we provide a comprehensive security solution that offers proactive threat hunting, real-time alerts, and rapid incident response.

Capabilities	Managed Detection and Response (MDR)	Incident Response
Detection		
Continuous Threat Monitoring	✓	
IOC based detections	✓	
AI-based detections	✓	
UEBA	✓	
Custom Rules	✓	
Real-time Alerting	✓	
Incident Detection	✓	
Investigation and Response		
Incident Validation	✓	✓
Containment	Alert Based	Across environment as needed
Alert Triage and Investigation	Alert Based	Investigative based
Remediation	Recommendations	✓
Incident Response Scoping		✓
Eradication and Recovery		✓
Root Cause Analysis	Alert Based	✓
Malware Analysis		✓
Forensic Investigation		✓
Post-Incident Reporting		✓
Threat Intelligence		
Human-driven Threat Hunting	✓	✓
Threat Intel Notifications		✓
Quarterly Threat Hunting Reports		✓

*Incident response subscription requires a one year log retention

adlumin

DATA SHEET

Learn more about how Adlumin's Incident Response can enhance your organization's cybersecurity posture:

www.adlumin.com

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.