SOLUTION BRIEF

Adaptive Analytic Detection (AAD)

The sophistication of cyber threats continues to evolve. So why do so many cybersecurity tools rely on rule and signature-based analytics? These tools are good at stopping what they are programmed to identify, but unfortunately, leave gaps that threat actors find and exploit.

The nLighten XDR platform reviews security data based on more than 250 behaviors. Its machine learning detection recognizes anomalies and finds what others miss to help stay ahead of attackers. We call it Adaptive Analytic Detection (AAD)

Reduce Noisy Alerts 97% More Effectively Than Typical SIEM

nLighten's machine learning and AI-based behavioral analytic detections analyze massive log and alert volumes to detect behaviors that elude rules and signatures. As a result, AAD recognizes patterns and threats, providing a handful of curated cases instead of thousands of alerts. This gives you an extraordinarily high noise-to-signal ratio, eliminating alert fatigue and improving your security posture with a more accurate, focused approach.

$3.8M
cost of a data breach savings for organizations w/fully developed AI and Automation

97% better alert reduction than typical SIEM products

99% automated case creation, our expert SOC team covers the rest

Eliminate over 95% of false positives

Adaptive Analytic Detection (AAD) at a Glance

	nLighten	Industry Standard SIEMs
Standard	✓ The same rule and signature-based analytics that standard SIEMs use are also used by the nLighten as a starting point	• Rules and signatures are entered into the system and used as filters to create alerts. The system can only find threats that have an existing rule or signature implemented.
Advanced	✓ 250+ ML/AI behavioural analytic detections, more are continuously being added ✓ Streaming real-time analysis ✓ Threat Intel Feed – anonymized malicious indicator tracking across all customers	• No ML, AI, or additional analytics are provided • Batch processing analysis
Automation	✓ Automated case creation ✓ Extensive dashboards based on insights, log sources, and custom IoCs and IoTs are pre-built and can be customized ✓ Custom log searches with reporting are correlated to cases ✓ Direct integrations with ticketing systems are available	• Manual entry in to the IRT ticket system is required • Manual alert correlation and research is required • Additional products for automation and integration are required

SOLUTION BRIEF

Strengthen and Simplify Security Operations with Automation

Typical SIEM products leave you and your team to manually investigate, sort, correlate, and prioritize massive volumes of logs and alerts. Adding other SOAR and automation point-solutions reduces these volumes. However, because they rely solely on rule and signature-based analytics, they stop at entity-level analysis.

AAD exponentially reduces entity-level records down to case-level. As part of the nLighten Autonomous SIEM, AAD automatically creates 96% of cases, and our expert SOC team covers the rest. Its ML and AI-based automation collect, analyze, and sort through millions of logs and alerts to correlate and prioritize threats. Eliminating this workload eliminates human error and improves scalability; it also supercharges your cybersecurity operations by reducing false positives by 95%.

> PatientLock is a great partner that really takes the SIEM market to the level of applicability that it should have been since the beginning of SIEM.
>
> By offering a true correlation of events, you are able to focus on what needs to be investigated quickly.
>
> - Kevin Cleveland, CTO Mednetworx

Call PatientLock 866-938-4250

linkedin.com/company/patientlock

twitter.com/patientlock

www.patientlock.net

866-938-4250
info@patientlock.net

Corporate Woods - Building 51
9393 W. 110th Street, Ste. 500
Overland Park, KS 66210