

SECURITY
OPERATIONS & SIEM.

Attack signals don't announce themselves — **they hide inside millions of logs across endpoints, network, and cloud** every day. SIEM correlates that noise into the alerts analysts can actually act on.

- LOG AGGREGATION
- CORRELATION & DETECTION
- ALERT TRIAGE
- INCIDENT ESCALATION

01 THE MECHANISM



Log Aggregation & Normalization
Collecting event data from endpoints, network, and cloud into one system, then **normalizing formats for analysis**.



Correlation & Detection
Applying rules and analytics to spot patterns that **a single event alone wouldn't reveal**.



Alert Triage & Escalation
Enriching high-confidence alerts with context and routing them **to analysts for response**.

02 THE FLOW

The Detection Cycle CONTINUOUS

1

Logs from endpoints, network, cloud, and applications are **ingested and normalized**.

2

Correlation rules and analytics score events against **known attack patterns**.

3

High-confidence alerts are enriched with context and **routed to analysts for triage**.

The Incident Cycle LIVE EVENT

1

An anomalous event matches a correlation rule **in real time**.

2

An analyst triages the alert, using context to **confirm a true positive**.

3

Confirmed incidents are escalated, contained, and **documented for post-incident review**.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Log Aggregation	Collects and normalizes log data from endpoints, network, and cloud sources.
Correlation & Detection	Applies rules and analytics to link related events into meaningful alerts.
Alert Triage	Enriches and prioritizes alerts so analysts investigate what matters most.
Incident Escalation	Routes confirmed incidents to response teams with full supporting context.

04 SECURITY MONITORING APPROACHES COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
Manual Log Review	No	Doesn't scale past a handful of systems and misses time-sensitive threats.
Point-Product Alerts Alone	No	Each tool sees only its own slice, missing cross-system attack patterns.
Antivirus / EDR Alone	No	Flags device-level threats but misses network and identity-based attacks.
Compliance-Only Logging	No	Retains logs for audits without active correlation or alerting.
SIEM (Aggregation + Correlation + Triage)	Yes	Connects signals across the environment and surfaces what needs action.

SECURITY OPERATIONS & SIEM.

AGGREGATE · CORRELATE · TRIAGE

05 PROGRAM OPERATIONS

Alert volume without tuning creates fatigue.

Analysts drown in low-value alerts and miss the ones that matter.

Detection rules need continuous tuning.

Threats evolve, and static rules quickly become blind spots.

24/7 coverage is a staffing problem too.

Around-the-clock monitoring requires shift coverage or automation.

Log source gaps create blind spots.

Unmonitored systems generate zero signal, no matter how good the SIEM is.

06 CONTROL MAPPING

NIST SP 800-92

Log management guidance defining generation, storage, and analysis practices.

PCI DSS

Daily log review required for centralized monitoring of cardholder data environments.

SOC 2

Monitoring criteria requiring detection and response capability for security incidents.

ISO 27001

Event logging controls under Annex A, covering monitoring and clock synchronization.

07 WHAT THIS DOES NOT SOLVE

Alert fatigue management

SIEM generates the alerts; it can't force analysts to triage them without burning out.

Unmonitored systems

Coverage gaps mean **zero visibility**, no matter how strong the detection rules are elsewhere.

Skilled analyst shortage

Tooling doesn't replace the **trained staff** needed to interpret and act on alerts.

Attack prevention

SIEM detects and alerts on activity; it **doesn't stop the attack by itself**.

08 MYTHS VS. REALITY

MYTH	REALITY
"More alerts means better security."	Alert volume without tuning creates fatigue and buries true positives .
MYTH	REALITY
"SIEM stops attacks automatically."	It detects and alerts; response still requires human or SOAR action .
MYTH	REALITY
"Deploying a SIEM is a one-time project."	Detection rules and log sources need continuous tuning .
MYTH	REALITY
"All logs are equally useful."	Coverage gaps in untracked systems create real blind spots .
MYTH	REALITY
"24/7 monitoring means instant response."	Triage time and escalation paths still determine actual speed .

09 SPEAK THE PROGRAM — KEY TERMS

SIEM

Security Information and Event Management: technology that aggregates, correlates, and alerts on log data.

LOG AGGREGATION

Collecting log data from many sources into **one centralized system** for analysis.

CORRELATION RULE

Logic that links related events across sources to **reveal patterns** single events miss.

ALERT TRIAGE

The process of reviewing and prioritizing alerts to **separate real threats** from noise.

FALSE POSITIVE

An alert that **looks malicious but reflects benign, legitimate activity**.

MTTD

Mean Time to Detect: the average time between **an intrusion and its discovery**.