APTO SOLUTIONS

SIEM vs XDR vs SOAR

Understanding the Modern Security Operations Stack

aptosolutions.co.uk
March 2026

Assessed. Architected. Operated.

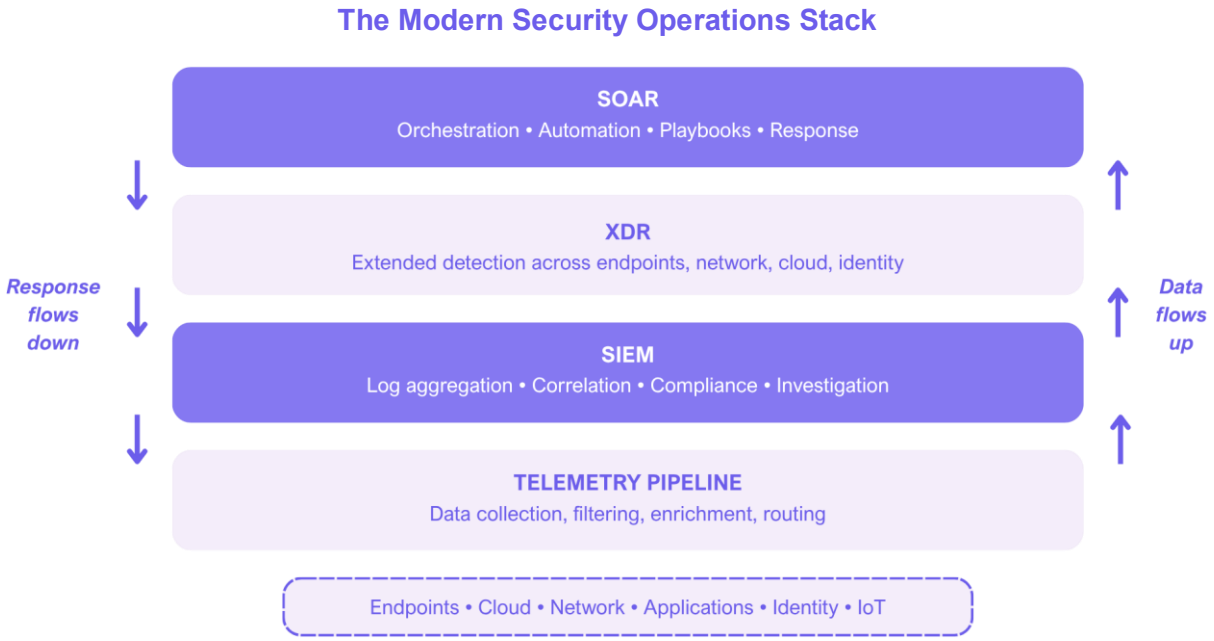
Introduction

The security operations market is flooded with acronyms, and the boundaries between product categories are increasingly blurred. SIEM, XDR, SOAR, EDR, NDR, MDR — the alphabet soup of security tooling can make it genuinely difficult to understand what you need, what overlaps, and where your money is best spent.

This confusion is not accidental. Vendors and suppliers benefit from the complexity because it drives fear-of-missing-out purchasing. The result is tool sprawl: organisations running overlapping products that create integration headaches, data duplication, and operational overhead without proportionally improving their security posture.

This guide provides a clear, vendor-neutral explanation of the three core pillars of the modern security operations stack: SIEM, XDR, and SOAR. It explains what each does, where they overlap, how they complement each other, and how to decide what your organisation actually needs.

> *Apto Solutions operates SIEM platforms (Splunk Enterprise Security, Microsoft Sentinel) and manages the data pipelines that feed them. We see the security operations stack from an operator's perspective, not a vendor's.*



The Three Pillars Explained

SIEM: Security Information and Event Management

SIEM is the backbone of security operations. At its core, a SIEM collects log data from across your IT estate — firewalls, endpoints, cloud platforms, applications, identity providers, network devices — and aggregates, normalises, and correlates this data to detect threats, support incident investigation, and meet compliance requirements.

What SIEM Does Well

- Broad data collection from virtually any source that produces logs
- Long-term log retention for compliance (PCI DSS, ISO 27001, NIS2, DORA)
- Correlation rules that detect multi-stage attacks across disparate data sources
- Rich search and investigation capabilities for forensic analysis
- Regulatory reporting and audit trail maintenance

Where SIEM Falls Short

- Historically dependent on log data only — limited visibility into endpoint, network, and cloud telemetry beyond logs
- High operational overhead: detection rules require continuous tuning to remain effective
- Alert fatigue: without careful tuning, SIEMs generate overwhelming volumes of low-fidelity alerts
- Cost: SIEM licensing is typically volume-based, and data volumes grow relentlessly
- Skills gap: operating a SIEM effectively requires specialist expertise that is scarce and expensive

Key SIEM Platforms

Platform	Deployment	Key Differentiator
Splunk Enterprise Security	Cloud, on-premises, hybrid	Unmatched search flexibility (SPL), mature risk-based alerting
Microsoft Sentinel	Azure cloud-native	Deep Microsoft ecosystem integration, free M365 ingestion
Elastic Security	Self-managed or cloud	Open-source heritage, flexible pricing
CrowdStrike Falcon LogScale(Falcon NG SIEM)	Cloud-native	High-speed search, index-free architecture
Google Chronicle	Cloud-native	Google infrastructure, fixed-price model

XDR: Extended Detection and Response

XDR emerged as an evolution of Endpoint Detection and Response (EDR). Where EDR provides deep visibility into endpoints (laptops, servers, workstations), XDR extends detection and response across endpoints, networks, cloud workloads, email, and identity — correlating signals across these domains to detect sophisticated threats that no single data source would reveal.

What XDR Does Well

- Automated correlation across multiple security telemetry domains (endpoint, network, cloud, identity)
- Built-in detection models tuned by the vendor's threat research team
- Native response actions: isolate an endpoint, block a network connection, disable a user account — directly from the platform
- Lower operational overhead than SIEM: less manual rule authoring, more vendor-managed detection
- Faster time-to-value for organisations without a large security engineering team

Where XDR Falls Short

- Vendor lock-in: most XDR platforms work best (or only) with the vendor's own endpoint, network, and cloud agents
- Limited flexibility: detection logic is largely vendor-managed, with less ability to write custom detections
- Narrow data scope: XDR typically focuses on security-specific telemetry and does not ingest the breadth of log data that a SIEM handles
- Limited compliance capabilities: XDR is not designed for long-term log retention, regulatory reporting, or audit trail management
- Third-party integration can be limited compared to SIEM's broad connector ecosystem

Key XDR Platforms

Platform	Heritage	Key Differentiator
Microsoft Defender XDR	Endpoint + cloud	Tight integration with Microsoft Sentinel and M365
CrowdStrike Falcon	Endpoint (EDR)	Industry-leading endpoint detection, strong threat intelligence
Palo Alto Cortex XDR	Network + endpoint	Strong network detection, XSOAR integration
SentinelOne Singularity	Endpoint (EDR)	Autonomous response capabilities
Trend Micro Vision One	Endpoint + email	Broad telemetry sources, managed XDR option

SOAR: Security Orchestration, Automation, and Response

SOAR platforms automate and orchestrate security workflows. They connect your security tools, define automated response playbooks, and coordinate actions across your entire security stack. If SIEM tells you what happened and XDR tells you where it happened, SOAR tells the rest of your infrastructure what to do about it.

What SOAR Does Well

- Automated incident response: execute predefined playbooks in seconds rather than waiting for an analyst to perform manual steps
- Orchestration across tools: connect SIEM, XDR, firewalls, identity providers, ticketing systems, and communication tools in unified workflows
- Enrichment automation: automatically enrich alerts with threat intelligence, asset context, and user information before they reach an analyst
- Consistent response: ensure every incident of a given type receives the same structured response, regardless of which analyst is on-call
- Metrics and reporting: track response times, playbook execution, and analyst workload

Where SOAR Falls Short

- Playbook maintenance: automated playbooks require ongoing updates as tools, APIs, and processes change
- Integration complexity: connecting dozens of tools via APIs creates a web of dependencies that must be managed
- Skills requirement: building effective playbooks requires both security expertise and scripting/automation skills
- Over-automation risk: poorly designed automation can cause more harm than the incidents it responds to (e.g., auto-isolating a critical server based on a false positive)

Key SOAR Platforms

Platform	Ecosystem	Key Differentiator
Splunk SOAR	Splunk	Deep Splunk ES integration, extensive app marketplace
Microsoft Sentinel (Logic Apps)	Azure	Native SOAR within Sentinel, Azure ecosystem
Palo Alto XSOAR	Palo Alto	Mature platform, large integration library
Tines	Independent	No-code automation, flexible pricing
Swimlane	Independent	Low-code platform, strong casemanagement

How They Fit Together

SIEM, XDR, and SOAR are not competitors — they are complementary layers of a modern security operations architecture. Understanding how they work together is more important than evaluating each in isolation.

The Integration Model

In a well-architected security operations stack:

1. SIEM provides the broad data foundation: aggregating logs from every source, correlating events across the enterprise, maintaining compliance-grade retention, and enabling forensic investigation.
2. XDR provides deep, automated detection: correlating security-specific telemetry across endpoints, network, cloud, and identity to detect sophisticated threats with minimal manual rule authoring.
3. SOAR provides automated response: executing playbooks that enrich, triage, and respond to alerts from both SIEM and XDR, orchestrating actions across the full security tool stack.

The data flow is: telemetry sources feed both SIEM and XDR. Both generate alerts and incidents. SOAR receives these alerts, enriches them automatically, executes predefined response actions, and escalates to human analysts only when automated playbooks are insufficient.

Where They Overlap

The boundaries between these categories are blurring, which contributes to buyer confusion:

- **SIEM and XDR overlap on detection:** Modern SIEMs incorporate UEBA and machine learning-based detection that was once unique to XDR. Meanwhile, some XDR platforms are expanding their data ingestion to look increasingly like SIEMs.
- **SIEM and SOAR overlap on automation:** Platforms like Microsoft Sentinel include native SOAR capabilities (Logic Apps). Splunk has acquired SOAR. The standalone SOAR market is being absorbed into SIEM platforms.
- **XDR and SOAR overlap on response:** XDR platforms include native response actions (endpoint isolation, network blocking) that overlap with SOAR's orchestration capabilities.

The trend is clear: the market is consolidating toward unified security operations platforms that combine SIEM, XDR, and SOAR in a single offering. Microsoft's unified security operations platform (combining Sentinel and Defender XDR) and Splunk's combined ES + SOAR + UBA portfolio are leading examples.

What Does Your Organisation Need?

The right combination depends on your organisation's size, maturity, regulatory environment, and existing technology investments.

If You Need Compliance and Broad Log Retention

A SIEM is non-negotiable. Regulatory frameworks like PCI DSS, ISO 27001, NIS2, and DORA require centralised log collection, retention, and audit trail capabilities that only a SIEM provides. XDR does not replace this requirement. We've been told by numerous CISO's in heavily regulated industries SIEM is non-negotiable, perhaps a subject in another guide in its own right?

If You Need Faster Detection with Fewer Resources

XDR delivers out-of-the-box detection with less operational overhead than SIEM. For organisations without a large security engineering team, XDR provides vendor-managed detection models that are continuously updated by the vendor's threat research team. It is not a substitute for SIEM, but it significantly augments detection capability, particularly for endpoint and identity-based threats.

If You Need to Scale Your Response Capability

SOAR is the answer to alert fatigue and inconsistent response. If your analysts are spending hours on repetitive triage and response tasks that follow a predictable pattern, SOAR automation frees them to focus on complex investigations that require human judgment.

The Realistic Starting Point for Most UK Organisations

For mid-market and growing enterprises, we typically recommend:

- Start with a well-operated SIEM as the foundation (Splunk ES or Microsoft Sentinel)
- Add XDR for automated endpoint and identity detection (typically Microsoft Defender XDR for Sentinel environments or CrowdStrike for Splunk environments)
- Introduce SOAR capabilities gradually, starting with automated enrichment playbooks and progressing to response automation as confidence grows
- Underpin everything with a telemetry pipeline for cost control and data quality

> *The most impactful investment is not which tools you buy, but how well you operate them. A well-tuned, well-operated Splunk ES deployment with a managed data pipeline will consistently outperform a shelfware collection of SIEM + XDR + SOAR that nobody has time to maintain.*

The Role of the Telemetry Pipeline

Regardless of which combination of SIEM, XDR, and SOAR you deploy, a telemetry pipeline is the architectural component that makes the entire stack cost-effective and operationally sustainable.

The pipeline sits between your data sources and your security platforms, performing:

- **Data reduction:** Filtering noise before it reaches your SIEM, reducing licence costs by 30–60%.
- **Schema normalisation:** Transforming data into standard schemas (OCSF) so that detection rules work consistently across all data sources.
- **Enrichment:** Adding context (GeoIP, user identity, asset classification) that improves detection fidelity and accelerates investigation.
- **Multi-destination routing:** Sending high-value security events to your SIEM, raw data to a data lake for compliance, and operational telemetry to your observability platform — from a single collection point.

Without a pipeline, your security operations stack will always be more expensive and less effective than it should be. The pipeline is the cost optimisation and data quality layer that enables everything else.

Next Steps

Ready to take action? Apto Solutions offers a range of entry-point engagements designed to give you clarity before commitment:

- **Free Assessment:** A no-obligation conversation with one of our platform specialists to understand your current state and identify quick wins.
- **SIEM Health Check:** A structured review of your existing SIEM deployment covering architecture, detection coverage, data quality, and operational efficiency.
- **Observability Maturity Assessment:** A framework-driven evaluation of your monitoring and observability capabilities against industry best practice.
- **Data Mapping and Discovery:** An analysis of your telemetry data flows, identifying redundancy, gaps, and optimisation opportunities.

> *Book your free assessment at aptosolutions.co.uk/contact or email enquiries@aptosolutions.co.uk to start the conversation.*

Assessed. Architected. Operated.
aptosolutions.co.uk