SIEM vs XDR

What’s the difference & why you might need both.

Detection | Response | Compliance

Mahesswar Shri Mohanty

Cybersecurity Visionary @CyberArk

Detection Depth & Observability

SIEM = Broad Visibility

Aggregates logs from across your entire IT environment. Great for monitoring what happened.

XDR = Deep Detection

Correlates high-fidelity telemetry across endpoints, cloud, network & more. Tells you why it happened.

Mahesswar Shri Mohanty

Cybersecurity Visionary @CyberArk

Use Case Fit

SIEM

Ideal for large teams Custom rules & dashboards Best for compliance, forensics, and long-term visibility

XDR = Deep Detection

Best for fast-moving teams
Automated detection & response
Best for real-time threat hunting

Mahesswar Shri Mohanty

Cybersecurity Visionary @CyberArk

SecOps Roles

Who uses what?

SIEM → Analysts, Compliance Officers, Forensics Teams

XDR → Incident Responders, Threat Hunters, Blue Teams

Mahesswar Shri Mohanty

Cybersecurity Visionary @CyberArk

Integration & Setup

SIEM:

Manual setup, complex integrations
Longer time to value

XDR:

Out-of-the-box integrations
Faster deployment and insights

Mahesswar Shri Mohanty

Cybersecurity Visionary @CyberArk

Threat Detection Flow

SIEM Workflow:

Rules & UEBA
Generates lots of alerts
Analysts investigate manually

XDR Workflow:

AI-driven, cross-domain analysis
Low false positives
Automated investigation & response

Mahesswar Shri Mohanty

Cybersecurity Visionary @CyberArk

Response Capabilities

SIEM:

Investigative tool
Provides evidence
Response happens elsewhere

XDR:

Built-in playbooks
Can isolate, block, and respond
Rapid remediation from within

Mahesswar Shri Mohanty

Cybersecurity Visionary @CyberArk

Why Use Both?

Better Together

SIEM = Historical data + compliance

XDR = Real-time detection + rapid response

Combined: Unified intelligence, streamlined investigations, deeper visibility

Mahesswar Shri Mohanty

Cybersecurity Visionary @CyberArk

Final Takeaway

SIEM + XDR = A Resilient Security Stack

Breadth + Depth

Visibility + Speed

Intelligence + Action

Mahesswar Shri Mohanty

Cybersecurity Visionary @CyberArk

Found these Helpful?

Repost this!

Follow for more such insights

Mahesswar Shri Mohanty

Cybersecurity Visionary @CyberArk