ESET PROTECT Platform and IBM QRadar SIEM

Harness the power of an enhanced security posture

eset Digital Security
Progress. Protected.

SOLUTION BRIEF

For a holistic cybersecurity ecosystem

Integrating the ESET PROTECT Platform with IBM QRadar SIEM enhances your digital security by combining ESET's AI Native XDR with QRadar's powerful Security Information and Event Management (SIEM) capabilities.

Designed to support Security Operations Center (SOC) analysts, this integration simplifies monitoring and streamlines threat detection and response workflows. It addresses challenges in monitoring endpoint activities and identifying threats across multiple perimeters.

Gain centralized threat visibility, faster detection and improved incident response—all within a single-pane-of-glass system. By aggregating ESET cybersecurity data into IBM QRadar SIEM, we **ensure comprehensive security management, minimize security gaps** and **support improved compliance.**

KEY BENEFITS

STRONGER SECURITY POSTURE

Combine ESET's AI-driven threat detection with QRadar's SIEM capabilities for a holistic cybersecurity ecosystem.

CENTRALIZED THREAT MANAGEMENT

Access centralized threat data within QRadar to reduce response times and leverage its powerful analysis capabilities.

PROACTIVE THREAT RESPONSE

Enable cross-platform threat telemetry and support advanced threat response strategies.

KEY FEATURES

REAL-TIME THREAT DATA TRANSFER/ VISIBILITY

ESET continuously streams security event updates directly into QRadar SIEM—ensuring efficient and convenient threat management.

REGULAR RULE ENGINE MODULE UPDATES

Benefit from timely updates with detailed information on specific detections, keeping your defenses sharp.

COMPREHENSIVE EVENT PARSING

Custom DSM properties allow for the extraction of specific data points such as device names, threat actions, and user activity. These are ready-made to streamline your workflow without added effort.

ENHANCED QRADAR INCIDENT INVESTIGATION

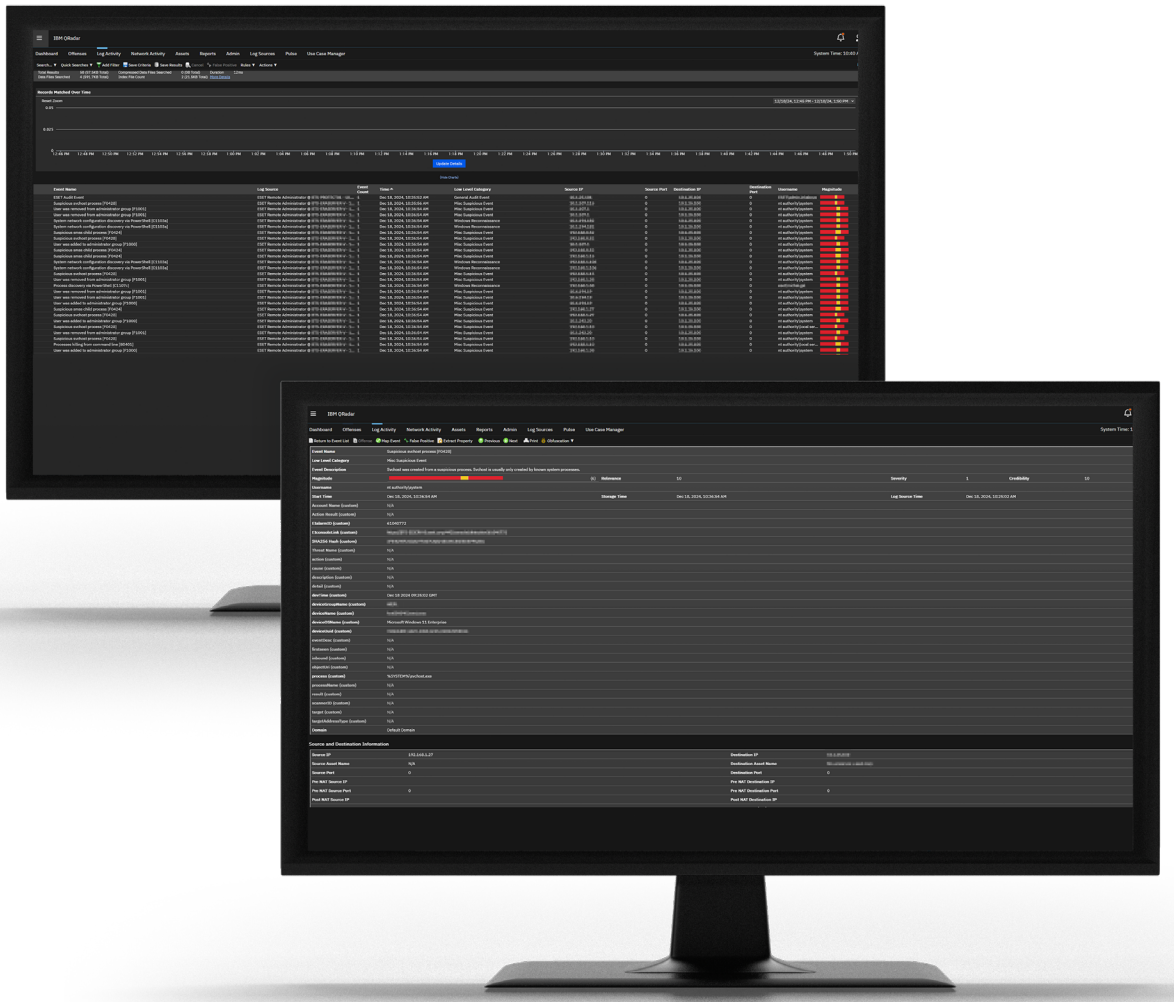
Leverage QRadar SIEM's capabilities to investigate ESET-generated alerts and threat data for faster, more effective incident response.

HOW IT WORKS

The integration of the ESET PROTECT Platform with IBM QRadar SIEM centralizes cybersecurity data by seamlessly feeding ESET telemetry into QRadar. This unifies various security insights for comprehensive management and more effective threat response.

By combining ESET's AI Native XDR platform with QRadar's SIEM capabilities, the integration enables deep visibility, actionable intelligence and faster decision-making, helping enterprises address threats across their organization.

For example, when a SOC analyst identifies a suspicious login attempt flagged by ESET as high-risk, the alert—enriched in QRadar with contextual data—allows the analyst to quickly investigate and isolate the affected device, preventing further risk. The result: streamlined operations, reduced vulnerabilities, and a stronger security posture.



About ESET

PROACTIVE DEFENSE. MINIMIZE RISKS WITH PREVENTION.

Stay one step ahead of known and emerging cyber threats with our AI Native, prevention-first approach. We combine the power of AI and human expertise to make protection easy and effective.

Experience best-in-class protection thanks to our in-house global cyber threat intelligence, compiled and examined for over 30 years, which drives our extensive R&D network led by industry-acclaimed researchers.

ESET PROTECT, our cloud-first XDR cybersecurity platform, combines next-gen prevention, detection and proactive threat hunting capabilities with a broad variety of security services, including managed detection and response. Our highly customizable solutions include local support and have minimal impact on performance. They identify and neutralize known and emerging threats before they can be executed, support business continuity and reduce the cost of implementation and management.

ESET protects your business so you can unlock the full potential of technology.

About IBM QRadar SIEM

EMPOWERING TODAY'S MODERN SOC WITH ENTERPRISE-GRADE AI

As the cost of a data breach rises and cyberattacks become increasingly sophisticated, the role of security operations center (SOC) analysts is more critical than ever. IBM QRadar SIEM is more than a tool; it is a teammate for SOC analysts—with advanced AI, powerful threat intelligence and access to the latest detection content.

IBM QRadar SIEM uses multiple layers of AI and automation to enhance alert enrichment, threat prioritization and incident correlation—presenting related alerts cohesively in a unified dashboard, reducing noise and saving time. QRadar SIEM helps maximize your security team's productivity by providing a unified experience across all SOC tools, with integrated, advanced AI and automation capabilities.

*Source: [IBM Official Page] https://www.ibm.com/products/qradar-siem

eset® Digital Security
Progress. Protected.

SOLUTION BRIEF