The evolving threat landscape

With organizations facing an overwhelming increase in data due to digital transformation, networks are also becoming bigger and more complex. These growing networks require the use of multiple tools and a traditional security information and event management (SIEM) tool that tends to focus only on log ingestion. Huge logs of event data from various tools and a distributed workforce without any additional context leave security teams with the heavy burden of correlating threats and analyzing devices. Adding to this is a rise in increasingly complex malicious and automated cyber activity which often originates at the endpoint.

To stay on top of these trends, organizations are looking for smart solutions that will not only help defend against advanced unknown attacks but also lighten the workload for security teams.

IBM Security® QRadar® SIEM clients can now ingest IBM Security QRadar EDR alerts without any impact on their EPS count.

Talk to an IBM representative or IBM Business Partner to learn about a complimentary increase in EPS capacity when you integrate IBM Security® QRadar® EDR.
IBM Security QRadar EDR: AI-powered, automated endpoint security

IBM Security® QRadar EDR® is an industry-leading endpoint detection and response (EDR) solution that delivers autonomous, near real-time and fully customizable endpoint protection to organizations, but without the complexity.

By using AI and machine learning, QRadar EDR is able to detect and remediate highly sophisticated known and unknown threats with minimal requirements for analyst effort or experience level.

To help further reduce analyst workloads, Cyber Assistant, part of the QRadar EDR AI-powered alert management system, autonomously handles alerts. Cyber Assistant can reduce the total overall managed alerts because it learns from an analyst’s decision instantly after seeing a given alert only once.

QRadar EDR makes proactive threat hunting fast, easy and effective for analysts with easy-to-create detection and response use cases that can return results in seconds. Beyond built-in detection and response, use cases can be created as needed and deployed across the organization without the need to reboot endpoints.

Enrich SIEM logs with smart endpoint telemetry

Organizations can now take advantage of the native integration between QRadar EDR and QRadar SIEM and maximize their existing QRadar SIEM investment with the IBM Security QRadar EDR Device Support Module (DSM).

This integration solution enriches SIEM logs in near real-time and provides the ability to automatically call application programming interfaces (APIs) to QRadar EDR, helping organizations take quick corrective actions such as ending processes, isolating endpoints and more.

When connected, QRadar EDR’s AI engines automatically collect and group many endpoint events and consolidate them into a few high-fidelity alerts that are forwarded to QRadar SIEM. This significantly reduces noise and saves analysts time so they’re able to work on more important tasks, offering considerable savings on EPS licensing.

Further alleviating analyst workloads are many readily available rules that QRadar SIEM supports. To facilitate flexibility, QRadar SIEM also includes custom properties to create tailor-made scenarios.

IBM fully supports the QRadar EDR DSM. By combining QRadar SIEM with QRadar EDR, customers benefit from a single IBM support contact to get issues resolved quickly.
Why IBM Security QRadar EDR?

- Near real-time reconstruction of attack activity across the endpoint ecosystem with minimal high-fidelity alerts
- Powered with AI and advanced automation levels to help analysts remediate advanced unknown threats with minimal effort
- Hypervisor layer-based monitoring delivers deep visibility for security teams while being designed to be invisible to malware and attackers
- Speedier forensic data retrieval while preserving the integrity of information for post-breach response

How it works

When installed, the DSM pulls QRadar EDR alerts to QRadar SIEM. These alerts appear in the form of events in the QRadar SIEM log activity tab which can be monitored with active SIEM rules. This process generates actionable offenses within QRadar SIEM. By using the offenses tab within the SIEM console, security teams can access the data they need for correlation, triage and investigation. This process expedites accurate anomaly detection.

Searches and queries for QRadar EDR telemetry data can be visualized automatically on the QRadar SIEM dashboards to show complete threat contexts. With all threat events outlined and correlated visually, analysts don’t need to look through thousands of event logs to uncover threat patterns. This can help save time and increase productivity so the analyst can focus on other priorities.
Take effective and quick remediation actions

With the QRadar SIEM and QRadar EDR integration, organizations can easily perform endpoint triage and response. Security teams can access insights and recommendations from QRadar SIEM to perform complex threat hunting and response from QRadar EDR. The threat-hunting capabilities of QRadar EDR help SIEM analysts retrieve forensic data while preserving the integrity of information for post-breach response.

The flexibility of the integration allows running many threat scenarios, such as tracking suspicious activity followed by exfiltration, identifying potentially phished users and compromised accounts, and many other readily available or custom-created rules.

Conclusion

Collectively, QRadar EDR and QRadar SIEM give organizations deep visibility of natively integrated workflows to support consistency in proactive detection and response. Organizations can now opt for a defense system that unifies “protect and detect” capabilities to help shield against high-impact cyberthreats that could compromise your business.

To learn more, contact your IBM representative or IBM Business Partner. For a demo, visit the IBM Security QRadar EDR site for more details.

Image shows QRadar EDR events that can be queried on the QRadar Console.