Release announcement: IBM QRadar SIEM integration with ESET Protect Platform

2024-11-13 - Steef | ESET Nederland - Comments (0) - Feature release

The integration provides enhanced and faster threat detection with greater accuracy, the ability to manage threats and responses from a unified interface, alerts prioritization and incident response automation. The integration reduces manual intervention and simplifies security teams' operations.

ESET PROTECT Platform sends event logs and telemetry in a LEEF format to IBM QRadar SIEM, where data is parsed and made available for correlation and reporting.

Key functionalities:

ESET PROTECT Platform continuously sends updates on security events directly into QRadar SIEM via Syslog

DSM Plugin allows the extraction of specific data points like device names, threat actions, and user activity. (ready-made, the customer doesn’t need to do parsing themselves)

Users can leverage QRadar SIEM to investigate ESET-generated alerts and threat information for rapid incident response.

Release details:

- Release date: November, 13 2024 at 15:00 GMT
- Integration Type: Log-based integration
- Availability: Global

GitHub Repository: https://github.com/eset/ESET-Integration/releases

DSM Plugin Download:
https://github.com/eset/ESET-Integration/releases/download/latest/QRadar-EsetProtectInspect.zip

Help page to learn more about how to set up the integration:
https://help.eset.com/eset_connect/en-US/qradar.html