IBM Security QRadar SIEM and IBM Security QRadar EDR integration

Enhance QRadar SIEM with proactive threat hunting and remediation with QRadar EDR integration

Highlights
Enrich SIEM logs with high-fidelity endpoint alerts

Help increase security teams' productivity with unified endpoint investigation

Take quick and effective remediation actions

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

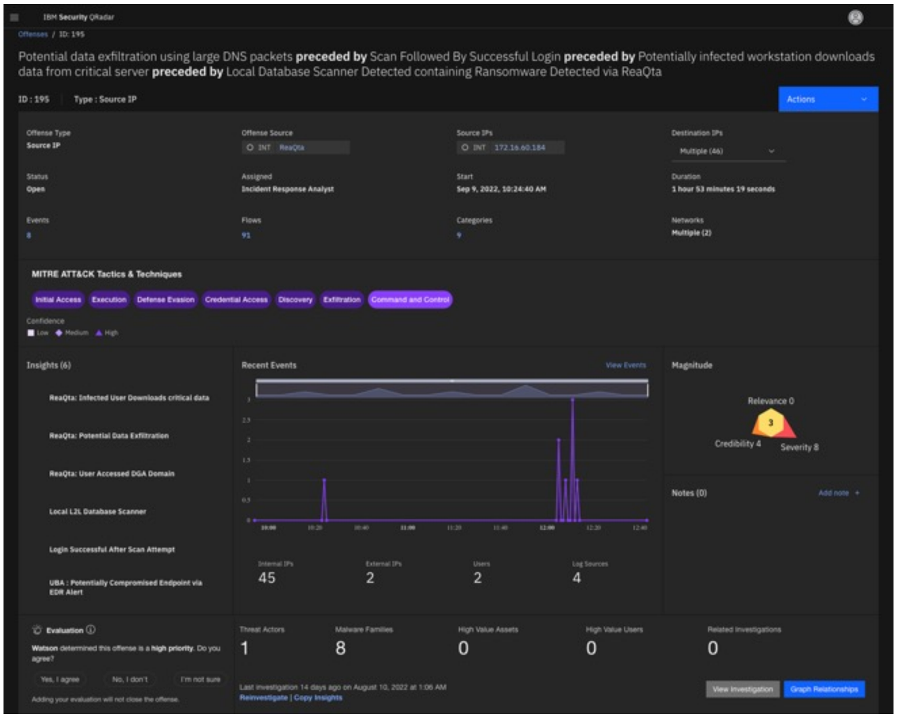
Powered with AI and advanced automation levels to help analysts remediate advanced unknown threats with minimal effort

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.



Potential data exfiltration using large DNS packets **preceded by** Scan Followed By Successful Login **preceded by** Potentially infected workstation downloads data from critical server **preceded by** Local Database Scanner Detected containing Ransomware Detected via ReaQta

ID : 195 | Type : Source IP

Offense Type: Source IP
Offense Source: INT ReaQta
Source IPs: INT 172.16.60.184
Destination IPs: Multiple (46)
Status: Open
Assigned: Incident Response Analyst
Start: Sep 9, 2022, 10:24:40 AM
Duration: 1 hour 53 minutes 19 seconds
Events: 8
Flows: 91
Categories: 9
Networks: Multiple (2)

MITRE ATT&CK Tactics & Techniques

Initial Access · Execution · Defense Evasion · Credential Access · Discovery · Exfiltration · Command and Control

Confidence: ■ Low ◆ Medium ▲ High

Insights (6)

- ReaQta: Infected User Downloads critical data
- ReaQta: Potential Data Exfiltration
- ReaQta: User Accessed DGA Domain
- Local L2L Database Scanner
- Login Successful After Scan Attempt
- UBA : Potentially Compromised Endpoint via EDR Alert

Recent Events

Internal IPs: 45
External IPs: 2
Users: 2
Log Sources: 4

Magnitude

Notes (0)

Evaluation

Watson determined this offense is a **high priority**. Do you agree?

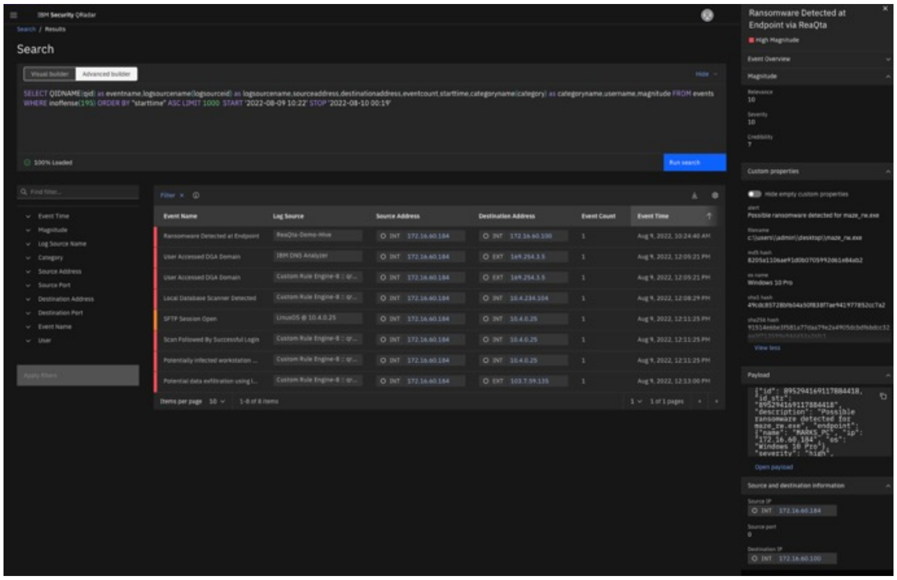
Adding your evaluation will not close the offense.

Threat Actors: 1
Malware Families: 8
High Value Assets: 0
High Value Users: 0
Related Investigations: 0

Last investigation 14 days ago on August 10, 2022 at 1:06 AM
Reinvestigate | Copy Insights

Image shows ransomware detection made by QRadar EDR on the QRadar Console.

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.



```
SELECT QIDNAME(qid) as eventname,logsourcename(logsourceid) as logsourcename,sourceaddress,destinationaddress,eventcount,starttime,categoryname(category) as categoryname,username,magnitude FROM events
WHERE inoffense(195) ORDER BY "starttime" ASC LIMIT 1000 START '2022-08-09 10:22' STOP '2022-08-10 00:19'
```

100% Loaded

Event Name	Log Source	Source Address	Destination Address	Event Count	Event Time
Ransomware Detected at Endpoint	ReaQta-Demo-Hive	INT 172.16.60.184	INT 172.16.60.100	1	Aug 9, 2022, 10:24:40 AM
User Accessed DGA Domain	IBM DNS Analyzer	INT 172.16.60.184	EXT 169.254.3.5	1	Aug 9, 2022, 12:05:21 PM
User Accessed DGA Domain	Custom Rule Engine-8 :: qr...	INT 172.16.60.184	EXT 169.254.3.5	1	Aug 9, 2022, 12:05:21 PM
Local Database Scanner Detected	Custom Rule Engine-8 :: qr...	INT 172.16.60.184	INT 10.4.234.104	1	Aug 9, 2022, 12:08:29 PM
SFTP Session Open	LinuxOS @ 10.4.0.25	INT 172.16.60.184	INT 10.4.0.25	1	Aug 9, 2022, 12:11:25 PM
Scan Followed By Successful Login	Custom Rule Engine-8 :: qr...	INT 172.16.60.184	INT 10.4.0.25	1	Aug 9, 2022, 12:11:25 PM
Potentially infected workstation ...	Custom Rule Engine-8 :: qr...	INT 172.16.60.184	INT 10.4.0.25	1	Aug 9, 2022, 12:11:25 PM
Potential data exfiltration using l...	Custom Rule Engine-8 :: qr...	INT 172.16.60.184	EXT 103.7.59.135	1	Aug 9, 2022, 12:13:00 PM

Items per page 10 1-8 of 8 items 1 1 of 1 pages

Ransomware Detected at Endpoint via ReaQta

High Magnitude

Event Overview

Magnitude

Relevance
10

Severity
10

Credibility
7

Custom properties

Hide empty custom properties

alert
Possible ransomware detected for maze_rw.exe

filename
c:\\users\\admin\\desktop\\maze_rw.exe

md5 hash
8205a1106ae91d0b0705992d61e84ab2

os name
Windows 10 Pro

sha1 hash
49c8c85728bfb04a50f838f7ae941977852cc7a2

sha256 hash
[illegible]

View less

Payload

```
{"id": 895294169117884418,
"id_str":
"895294169117884418",
"description": "Possible
ransomware detected for
maze_rw.exe", "endpoint":
{"name": "MARKS_PC", "ip":
"172.16.60.184", "os":
"Windows 10 Pro"},
"severity": "high",
```

Open payload

Source and destination information

Source IP
INT 172.16.60.184

Source port
0

Destination IP
INT 172.16.60.100

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

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.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
May 2023

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

The client is responsible for ensuring compliance with all applicable laws and regulations. IBM does not provide legal advice nor represent or warrant that its services or products will ensure that the client is compliant with any law or regulation..