# The Guardium Integration Application for IBM Security SOAR

Connect IBM Security Guardium Data Protection with IBM Security SOAR for quick data incident response

Highlights

- Connect security operations with database management
- Accelerate incident investigation with automation and data visibility
- Take remediation actions from IBM Security SOAR
- Stay on-top of the complex data breach regulation environment and address notification requirements

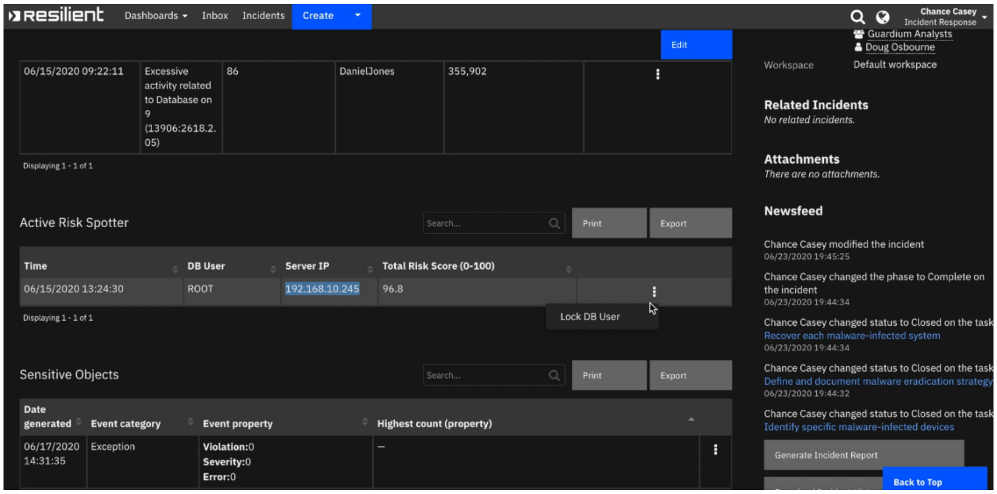
## Overview

Businesses today are embracing hybrid multicloud-based IT deployment models at an increasing rate to improve agility and gain a competitive advantage. However, expanding your data footprint across on-premises and cloud environments increases your organization's attack surface, which can result in new data security challenges.

Security teams are compelled to protect their organization's data, while struggling with limited visibility and reporting abilities. Making matters more difficult, they can become inundated with data and cybersecurity point tools--each of which focus on specific environments or use cases, adding significant operational complexity. Without a solution that can contextualize insights from multiple security tools, and separate the signal from the noise, threats and vulnerabilities can go undetected, leaving organizations exposed to a potential security breach and data exfiltration.

A security breach comes at a high cost to organizations. According to Ponemon, the average total cost of a data breach is $3.86 million, which takes into consideration multiple factors ranging from legal to brand equity, to loss of customers, among others (Ponemon Institute, 2020). For this reason, organizations benefit from taking a proactive approach to data security and from having an incident response team and plan in place to help mitigate risk and reduce hacker dwell time in the case of a security incident. The deployment of security tools that use automation, such as a Security Orchestration, Automation, and Response (SOAR) solution, can help mitigate risk and costs.

The Guardium Integration Application for IBM Security SOAR connects the data activity monitoring capabilities of IBM Security Guardium Data Protection with the incident response and automation capabilities of IBM Security SOAR. With this integration, you can empower your security team to respond fast to incidents that may put your data at risk, like insider threats or data breaches, by automatically enriching incidents with information from your databases and taking remediation actions directly from IBM Security SOAR.



| | | | | |
|---|---|---|---|---|
| 06/15/2020 09:22:11 | Excessive activity related to Database on 9 (13906:2618.2.05) | 86 | DanielJones | 355,902 |

Displaying 1 - 1 of 1

Active Risk Spotter

| Time | DB User | Server IP | Total Risk Score (0-100) |
|---|---|---|---|
| 06/15/2020 13:24:30 | ROOT | 192.168.10.245 | 96.8 |

Displaying 1 - 1 of 1

Sensitive Objects

| Date generated | Event category | Event property | Highest count (property) |
|---|---|---|---|
| 06/17/2020 14:31:35 | Exception | **Violation:**0<br>**Severity:**0<br>**Error:**0 | – |

Guardium Analysts
Doug Osbourne

Workspace Default workspace

**Related Incidents**
*No related incidents.*

**Attachments**
*There are no attachments.*

**Newsfeed**

Chance Casey modified the incident
06/23/2020 19:45:25

Chance Casey changed the phase to Complete on the incident
06/23/2020 19:44:34

Chance Casey changed status to Closed on the task
Recover each malware-infected system
06/23/2020 19:44:34

Chance Casey changed status to Closed on the task
Define and document malware eradication strategy
06/23/2020 19:44:32

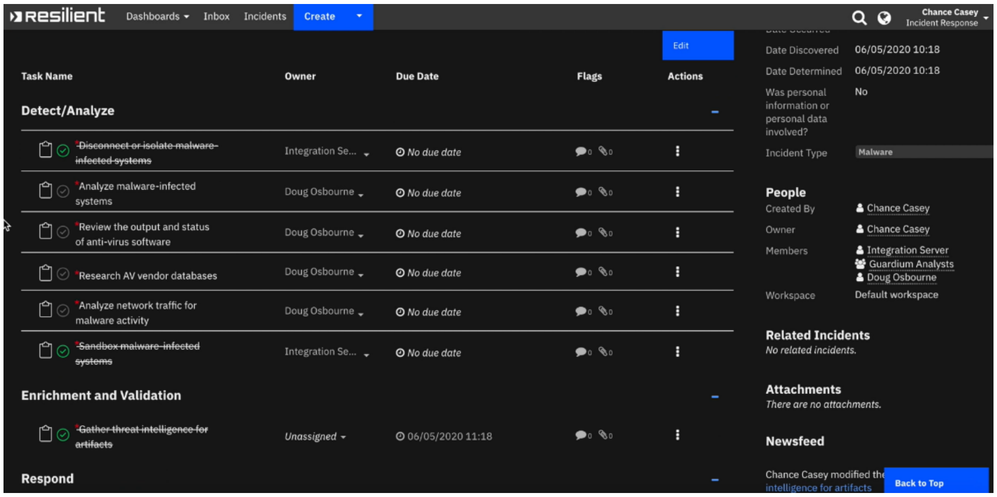
Chance Casey changed status to Closed on the task
Identify specific malware-infected devices

Guardium Activity Report in the Data Source Check Tab in IBM Security SOAR

## Enable consistent collaboration across your database and security operations

As more organizations try to find innovative ways to make Security Operations Centers more effective and efficient to make up for the shortage of skilled security talent, building bridges that connect siloed teams across the organization and that improve communication between the different teams is critical.

With the case management capabilities of IBM Security SOAR, you can help your security and privacy teams collaborate with consistency. You can assign tasks and due dates, manually or automatically, which triggers notifications for team members to complete their tasks. Communications can also extend beyond the SOC to include key stakeholders across the organizations, such as database managers, legal, human resources, etc.



| Task Name | Owner | Due Date | Flags | Actions |
|---|---|---|---|---|
| **Detect/Analyze** | | | | |
| ~~*Disconnect or isolate malware-infected systems~~ | Integration Se... | No due date | 0 0 | ⋮ |
| *Analyze malware-infected systems | Doug Osbourne | No due date | 0 0 | ⋮ |
| *Review the output and status of anti-virus software | Doug Osbourne | No due date | 0 0 | ⋮ |
| *Research AV vendor databases | Doug Osbourne | No due date | 0 0 | ⋮ |
| *Analyze network traffic for malware activity | Doug Osbourne | No due date | 0 0 | ⋮ |
| ~~*Sandbox malware-infected systems~~ | Integration Se... | No due date | 0 0 | ⋮ |
| **Enrichment and Validation** | | | | |
| ~~*Gather threat intelligence for artifacts~~ | Unassigned | 06/05/2020 11:18 | 0 0 | ⋮ |
| **Respond** | | | | |

| | |
|---|---|
| Date Discovered | 06/05/2020 10:18 |
| Date Determined | 06/05/2020 10:18 |
| Was personal information or personal data involved? | No |
| Incident Type | Malware |

**People**

| | |
|---|---|
| Created By | Chance Casey |
| Owner | Chance Casey |
| Members | Integration Server<br>Guardium Analysts<br>Doug Osbourne |
| Workspace | Default workspace |

**Related Incidents**
*No related incidents.*

**Attachments**
*There are no attachments.*

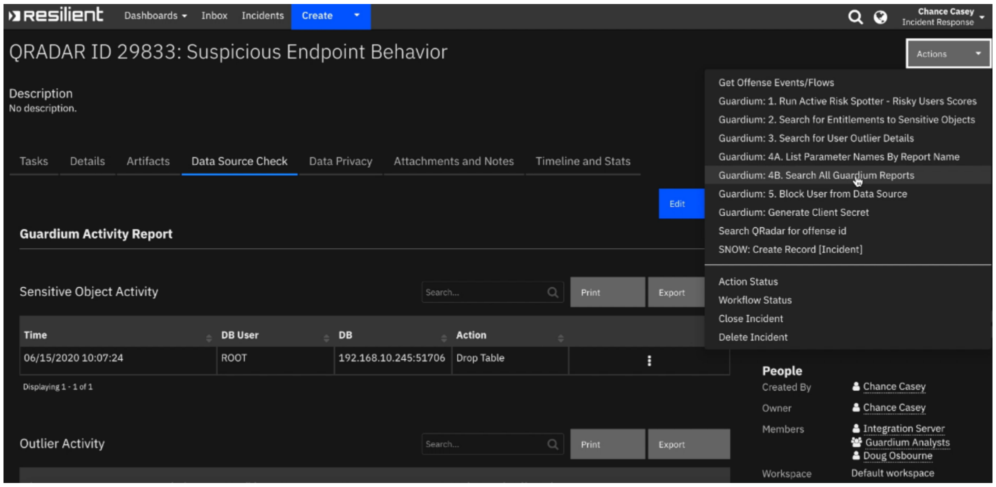
**Newsfeed**

Chance Casey modified the intelligence for artifacts

List of tasks to be completed by incident response team in IBM Security SOAR

## Reduce investigation time with automated incident enrichment from Guardium Data Protection

The orchestration and automation capabilities of IBM Security SOAR are designed to allow you to maximize your security investments by connecting with tools like Guardium Data Protection, and to save time by automating repetitive tasks such as incident enrichment. This new application is pre-configured so that IBM Security SOAR can access, manually or automatically, standard and custom Guardium Data Protection reports to get additional insight into data at risk or the nature of privacy data breach if that's the case. For instance, leveraging Guardium's Risk Spotter feature, IBM Security SOAR can automatically enrich incidents with the riskiest database users.  With this information readily available to provide context to the incident, security analysts can make decisions fast and start remediation.


Resilient
Dashboards
Inbox
Incidents
Create
Chance Casey
Incident Response
Actions
Get Offense Events/Flows
Guardium: 1. Run Active Risk Spotter - Risky Users Scores
Guardium: 2. Search for Entitlements to Sensitive Objects
Guardium: 3. Search for User Outlier Details
Guardium: 4A. List Parameter Names By Report Name
Guardium: 4B. Search All Guardium Reports
Guardium: 5. Block User from Data Source
Guardium: Generate Client Secret
Search QRadar for offense id
SNOW: Create Record [Incident]
Action Status
Workflow Status
Close Incident
Delete Incident
Tasks
Details
Artifacts
Data Source Check
Data Privacy
Attachments and Notes
Timeline and Stats
Edit
Search...
Print
Export

QRADAR ID 29833: Suspicious Endpoint Behavior

Description
No description.

Guardium Activity Report

Sensitive Object Activity

| Time | DB User | DB | Action |
|---|---|---|---|
| 06/15/2020 10:07:24 | ROOT | 192.168.10.245:51706 | Drop Table |

Displaying 1 - 1 of 1

Outlier Activity

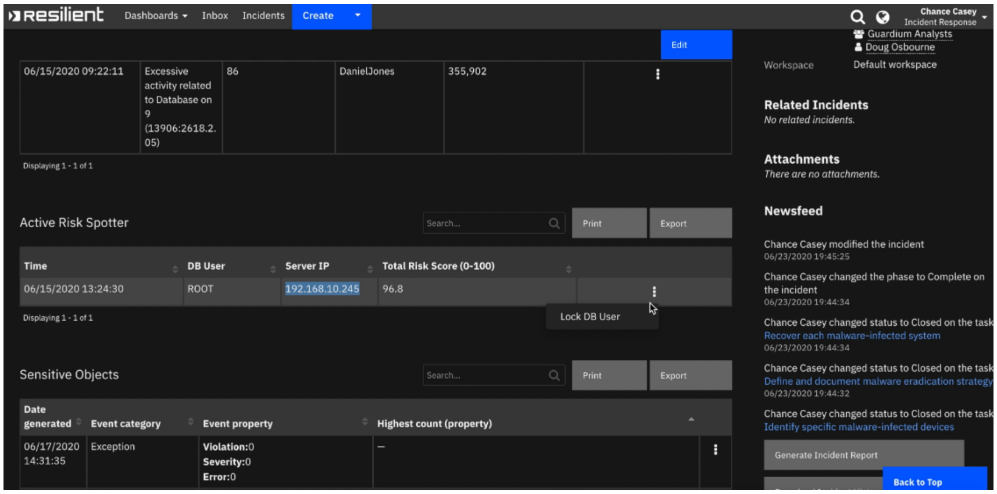
People

| | |
|---|---|
| Created By | Chance Casey |
| Owner | Chance Casey |
| Members | Integration Server<br>Guardium Analysts<br>Doug Osbourne |
| Workspace | Default workspace |

Enrich incidents with reports from IBM Security Guardium Data Protection

## Begin incident remediation and response to data privacy breaches

Once a suspicious alert becomes an incident, security analysts need to act fast to contain and remediate the threat. The Guardium Integration Application for IBM Security SOAR allows incident responders to take actions from IBM Security SOAR, such as blocking users. The application gives security analysts visibility into sensitive data entitlement and activity reports, which provide insight into who has access to the database. If a bad actor is identified, then the analyst can revoke access for that user without having to go into Guardium Data Protection.



|  |  |  |  |  |
|---|---|---|---|---|
| 06/15/2020 09:22:11 | Excessive activity related to Database on 9 (13906:2618.2.05) | 86 | DanielJones | 355,902 |

Displaying 1 - 1 of 1

Active Risk Spotter

| Time | DB User | Server IP | Total Risk Score (0-100) |
|---|---|---|---|
| 06/15/2020 13:24:30 | ROOT | 192.168.10.245 | 96.8 |

Displaying 1 - 1 of 1

Sensitive Objects

| Date generated | Event category | Event property | Highest count (property) |
|---|---|---|---|
| 06/17/2020 14:31:35 | Exception | **Violation:**0<br>**Severity:**0<br>**Error:**0 | – |

Guardium Analysts
Doug Osbourne

Workspace Default workspace

**Related Incidents**
*No related incidents.*

**Attachments**
*There are no attachments.*

**Newsfeed**

Chance Casey modified the incident
06/23/2020 19:45:25

Chance Casey changed the phase to Complete on the incident
06/23/2020 19:44:34

Chance Casey changed status to Closed on the task
Recover each malware-infected system
06/23/2020 19:44:34

Chance Casey changed status to Closed on the task
Define and document malware eradication strategy
06/23/2020 19:44:32

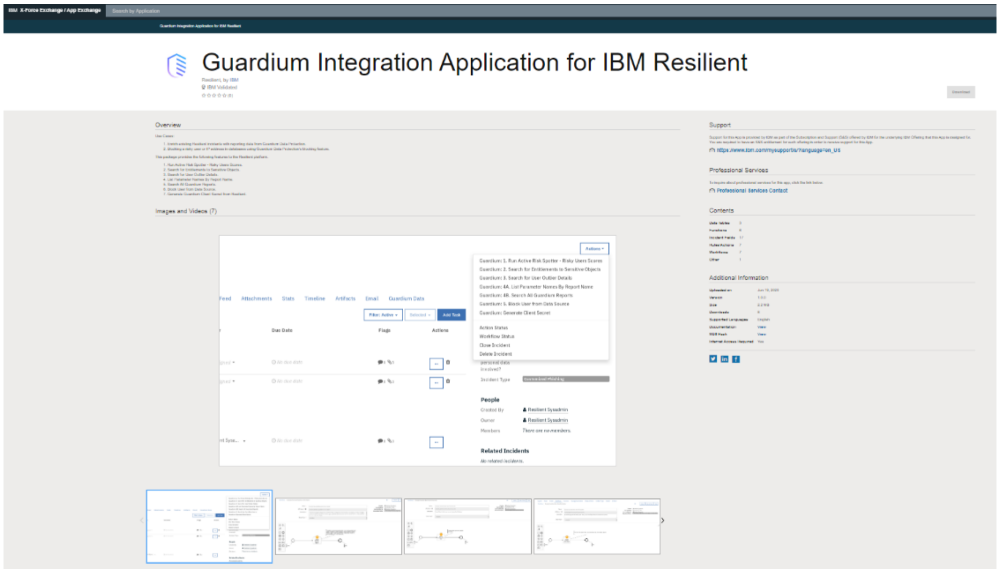
Chance Casey changed status to Closed on the task
Identify specific malware-infected devices

Lock user in IBM Security Guardium Data Protection from IBM Security SOAR

If a data privacy breach is determined during an incident, security analysts can start the process with a guided response from IBM Security SOAR, which integrates privacy use cases into security case management. It supports security and privacy teams throughout the complex breach notification process. With the Global Privacy Regulations Knowledge-base at the heart of the solution, IBM Security SOAR can alert to over 180 global regulations, including GDPR, PIPEDA, HIPAA, CCPA and all 50 stated breach notification rules to guide security and privacy teams throughout the complex breach notification process and help your security and privacy teams as they address compliance.

## Deploy and install the application in minutes

The Guardium Integration Application for IBM Security SOAR is available to download from the IBM Security App Exchange. With AppHost, the integration server of IBM Security SOAR, once you download the application, you can install it from the user interface with a guided installation process, which allows for editable settings and configurations.



IBM X-Force Exchange / App Exchange
Search by Application
Guardium Integration Application for IBM Resilient

Guardium Integration Application for IBM Resilient

Resilient, by IBM
IBM Validated

Overview

Use Cases:

1. Enrich existing Resilient incidents with reporting data from Guardium Data Protection.
2. Blocking a risky user or IP address in databases using Guardium Data Protection's blocking feature.

This package provides the following features to the Resilient platform:

1. Run Active Risk Spotter - Risky Users Scores.
2. Search for Entitlements to Sensitive Objects.
3. Search for User Outlier Details.
4. List Parameter Names By Report Name.
5. Search All Guardium Reports.
6. Block User from Data Source.
7. Generate Guardium Client Secret from Resilient.

Images and Videos (7)

Actions
Guardium: 1. Run Active Risk Spotter - Risky Users Scores
Guardium: 2. Search for Entitlements to Sensitive Objects
Guardium: 3. Search for User Outlier Details
Guardium: 4A. List Parameter Names By Report Name
Guardium: 4B. Search All Guardium Reports
Guardium: 5. Block User from Data Source
Guardium: Generate Client Secret
Action Status
Workflow Status
Close Incident
Delete Incident
Feed
Attachments
Stats
Timeline
Artifacts
Email
Guardium Data
Filter: Active
Selected
Add Task
Due Date
Flags
Actions
No due date

personal data involved?

Incident Type

People

Created By: Resilient Sysadmin
Owner: Resilient Sysadmin
Members: There are no members.

Related Incidents

No related incidents.

Support

Support for this App is provided by IBM as part of the Subscription and Support (S&S) offered by IBM for the underlying IBM Offering that this App is designed for. You are required to have an S&S entitlement for such offering in order to receive support for this App.

https://www.ibm.com/mysupport/s/?language=en_US

Professional Services

To inquire about professional services for this app, click the link below.

Professional Services Contact

Contents

| | |
|---|---|
| Data tables | 3 |
| Functions | 6 |
| Incident fields | 17 |
| Rules/Actions | 7 |
| Workflows | 7 |
| Other | 1 |

Additional Information

| | |
|---|---|
| Uploaded on | Jun 10, 2020 |
| Version | 1.0.0 |
| Size | 2.2 MB |
| Downloads | 8 |
| Supported Languages | English |
| Documentation | View |
| SHA Hash | View |
| Internet Access Required | Yes |

Download the application from the IBM Security App Exchange

With this new integration, your organization will take a step towards a more robust zero-trust strategy, and your security team will be well positioned to respond to incidents that put your data at risk.

Visit the IBM Security App Exchange for more information on this app.

*Sources: 1. Ponemon Institute. 2020 Cost of a Data Breach Report. June 2020*

## About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. 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 systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. 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.

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:

Gold
Business
Partner

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

## For more information

To learn more about IBM Security SOAR and IBM Security Guardium Data Protection, please contact your IBM representative or IBM Business Partner, or visit the following websites:

ibm.com/products/resilient-soar-platform
ibm.com/products/ibm-guardium-data-protection

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: ibm.com/financing

Gold
Business
Partner