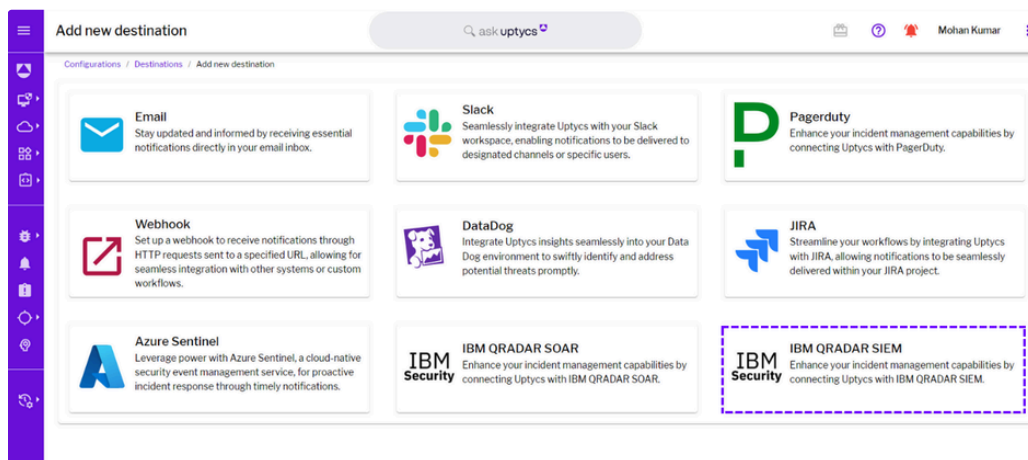




Integrating QRADAR SIEM with Uptycs

Forwarding Uptycs detection data to IBM SIEM

Login to your Uptycs tenant and create new destination for your alerts and detections with IBM QRADAR SIEM.



Fill the necessary details like Destination Name, SIEM URL(including Log Source PORT) and Detection template

Configurations / Destinations / MohanKumar-IBM-QRADAR-SIEM

Destination Type
IBM QRADAR SIEM

Name *
MohanKumar-IBM-QRADAR-SIEM ☐ Enable Role-based Destination Visibility ?

URL *
https://192.168.128.249:17293

Method *
POST

Username

Password

```

Detection Template
{
  "event_id": "uptycs_detection",
  "uptycs_detection_id": "{{{detection.id}}}",
  "uptycs_detection_name": "{{{detection.name}}}",
  "uptycs_detection_score": "{{{detection.score}}}",
  "uptycs_detection_assethostname": "{{{detection.assetHostName}}}",
  "uptycs_detection_iscontainer": "{{{detection.isContainer}}}",
  "uptycs_detection_url": "{{{detection.url}}}"
}

```

Create forwarding rule for detections to send detections to the configured destination

Configurations / Detection Forwarding Rules / Add new rule

Rule Name *

IBM SIEM FORWARD DETECTION DATA

This is a required field

Rule Description

Forwarding Detections data to IBM QRADAR SIEM.

Resource Type * ☒ Endpoint ☒ Cloud ☒ Kubernetes ☒ Container

Asset Tags & Groups

Asset Tags None selected

Asset Groups None selected

Trigger Condition * ☐ Created ☒ Completed

Severity * ☒ High ☐ Medium ☐ Low

Trigger Condition * ☐ Created ☒ Completed

Severity * ☒ High ☐ Medium ☐ Low

Advanced Conditions ☐ Lateral Movement ☐ Toolkit Present ☐ Anomaly present ☐ Remediation Enabled

Threat Score * Greater Than Value 5

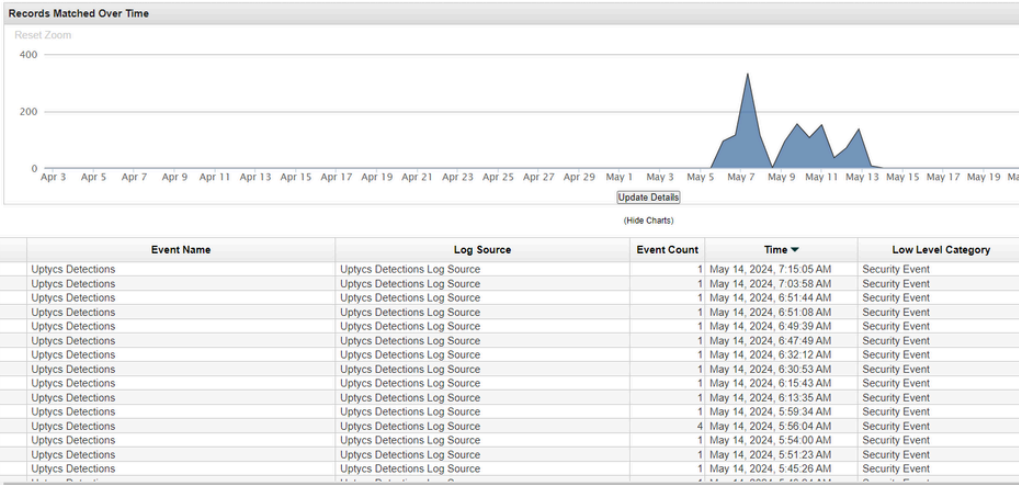
Post auto-close status * ☒ Open ☐ Assigned ☐ Closed

Destinations * Select Destinations MohanKumar-IBM-QRADAR-SIEM

Enable Rule * ☒ Yes ☐ No

SAVE CANCEL

Once the forwarding rule is configured, Event can be observed in IBM QRADAR SIEM for every detection triggered in the Uptycs tenant.



For more information, visit <https://www.uptycs.com/>

For support, please contact support@uptycs.com