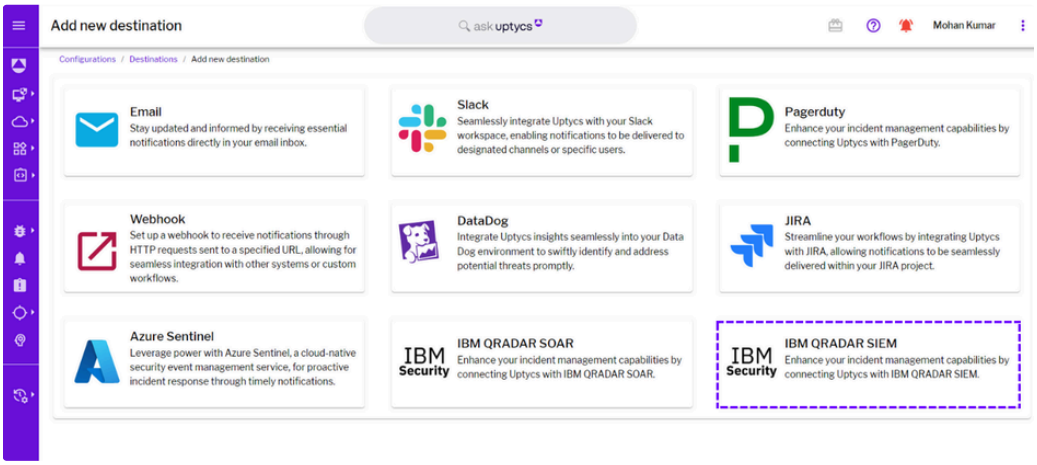
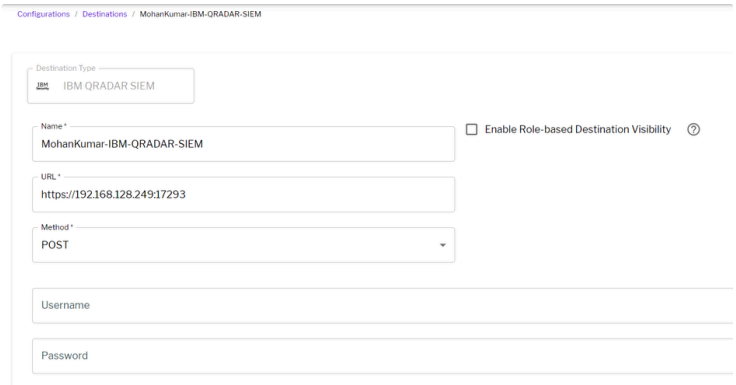
Integrating QRADAR SIEM with Uptycs

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.



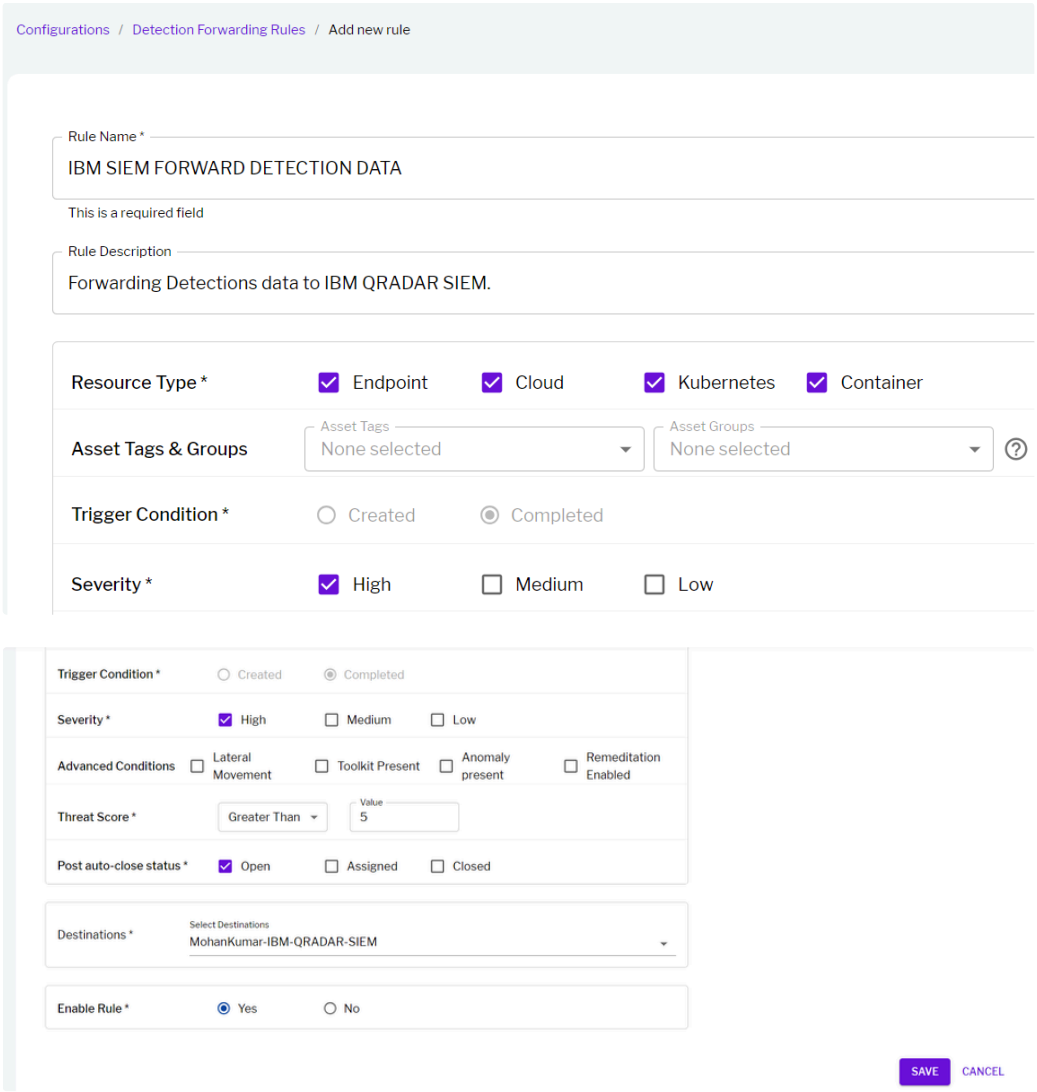
Fill the necessary details like Destination Name, SIEM URL(including Log Source PORT) and Detection template



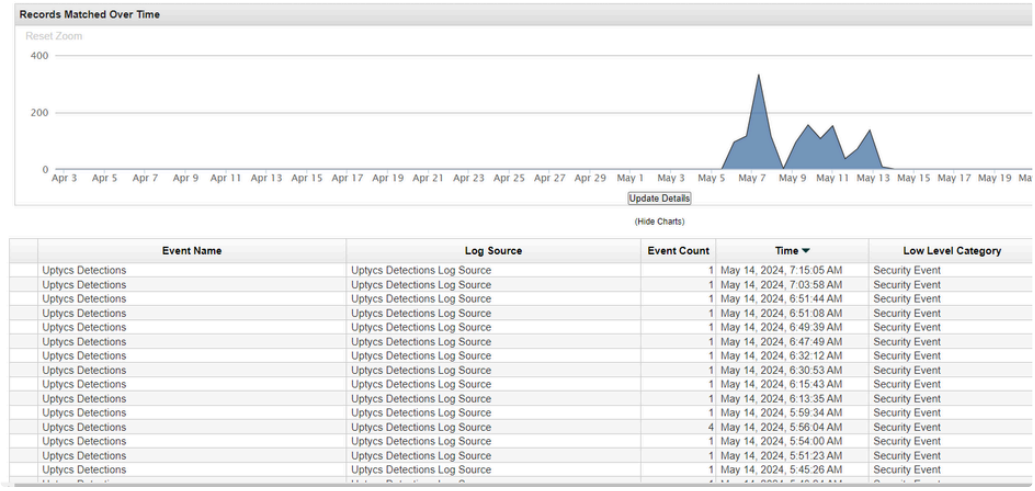
Detection Template

```
{
    "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



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



Event Name	Log Source	Event Count	Time	Low Level Category
Uptycs Detections	Uptycs Detections Log Source	1	May 14, 2024, 7:15:05 AM	Security Event
Uptycs Detections	Uptycs Detections Log Source	1	May 14, 2024, 7:03:58 AM	Security Event
Uptycs Detections	Uptycs Detections Log Source	1	May 14, 2024, 6:51:44 AM	Security Event
Uptycs Detections	Uptycs Detections Log Source	1	May 14, 2024, 6:51:08 AM	Security Event
Uptycs Detections	Uptycs Detections Log Source	1	May 14, 2024, 6:49:39 AM	Security Event
Uptycs Detections	Uptycs Detections Log Source	1	May 14, 2024, 6:47:49 AM	Security Event
Uptycs Detections	Uptycs Detections Log Source	1	May 14, 2024, 6:32:12 AM	Security Event
Uptycs Detections	Uptycs Detections Log Source	1	May 14, 2024, 6:30:53 AM	Security Event
Uptycs Detections	Uptycs Detections Log Source	1	May 14, 2024, 6:15:43 AM	Security Event
Uptycs Detections	Uptycs Detections Log Source	1	May 14, 2024, 6:13:35 AM	Security Event
Uptycs Detections	Uptycs Detections Log Source	1	May 14, 2024, 5:59:34 AM	Security Event
Uptycs Detections	Uptycs Detections Log Source	4	May 14, 2024, 5:56:04 AM	Security Event
Uptycs Detections	Uptycs Detections Log Source	1	May 14, 2024, 5:54:00 AM	Security Event
Uptycs Detections	Uptycs Detections Log Source	1	May 14, 2024, 5:51:23 AM	Security Event
Uptycs Detections	Uptycs Detections Log Source	1	May 14, 2024, 5:45:26 AM	Security Event

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

For support, please contact support@uptycs.com