Let’s go

CISCO The bridge to possible

The Security is Coming from Inside the Application!

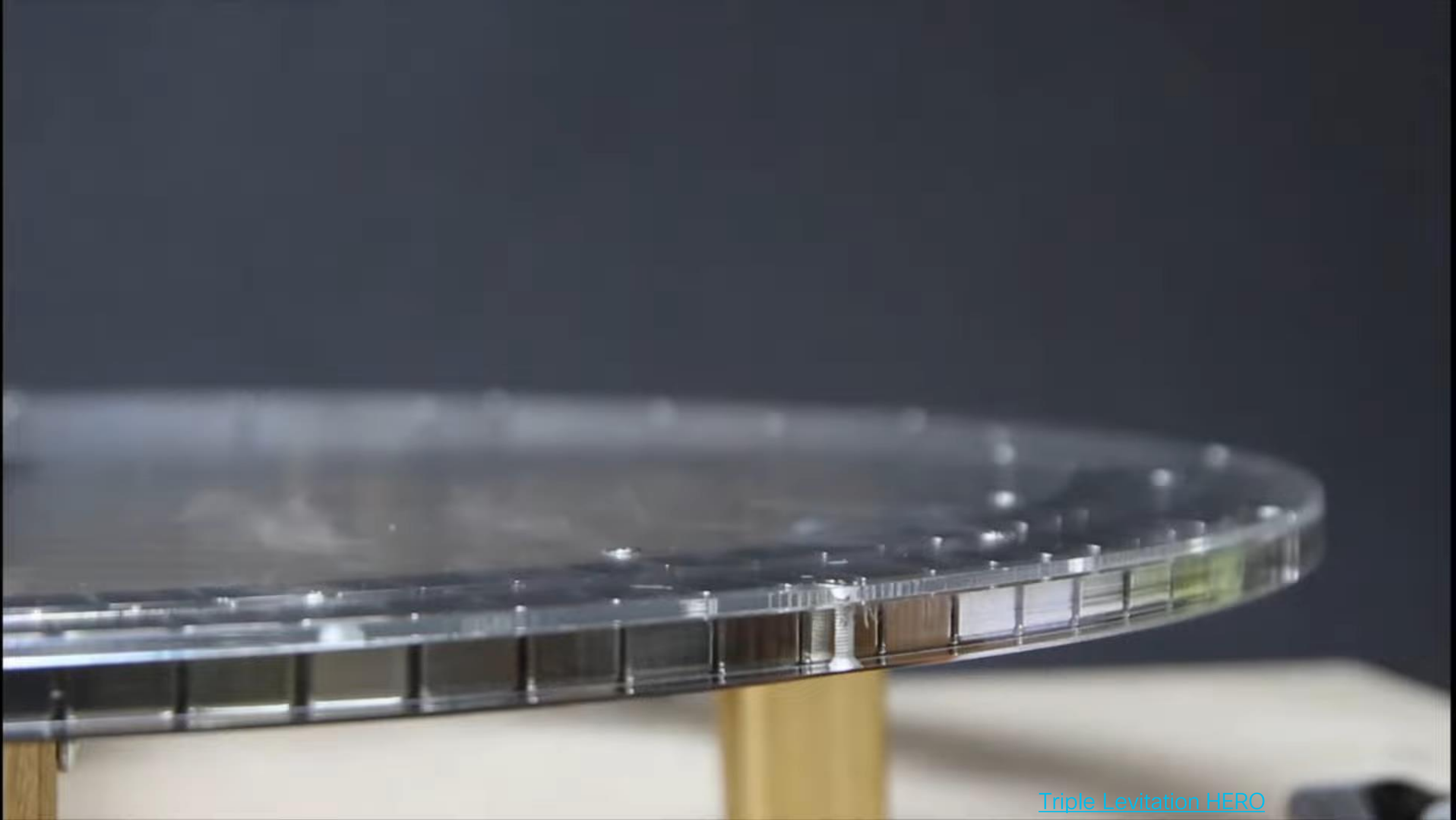
Cisco AppDynamics Teams Up with Cisco XDR for App-Triggered Protection

David Staudt, DevNet Developer Advocate / Principal Engineer
@dstaudtatcisco

Agenda

- xOps – Unite and Conquer
- Name a More Iconic Pair
- DevOps+SecOps+Netops = 4Ever
- What / Where / When / How
- Demo Tour
- Conclusion / Q&A

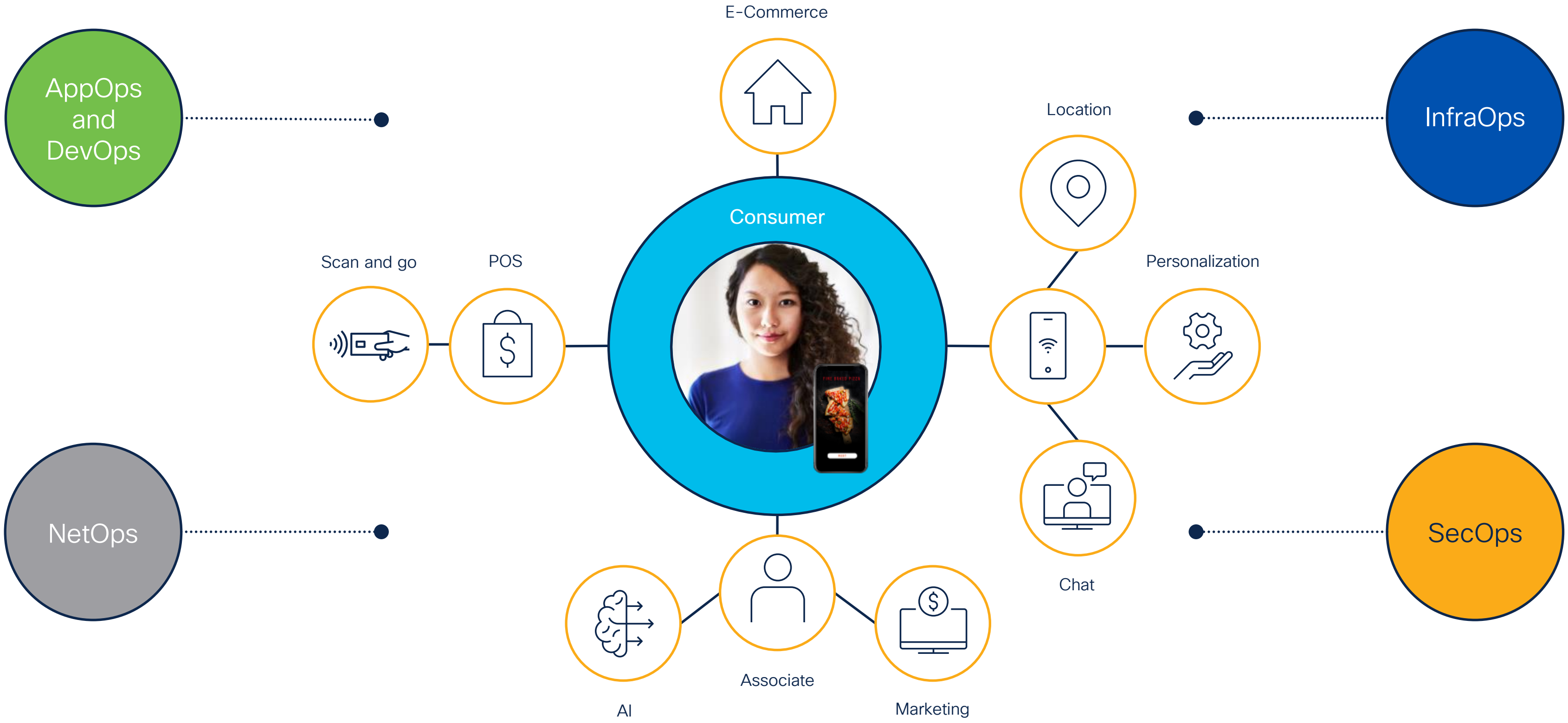
xOps – Unite and Conquer



Triple Levitation HERO

Full stack observability – Full stack synergy

Security / Infrastructure / Network / Application Co-operation

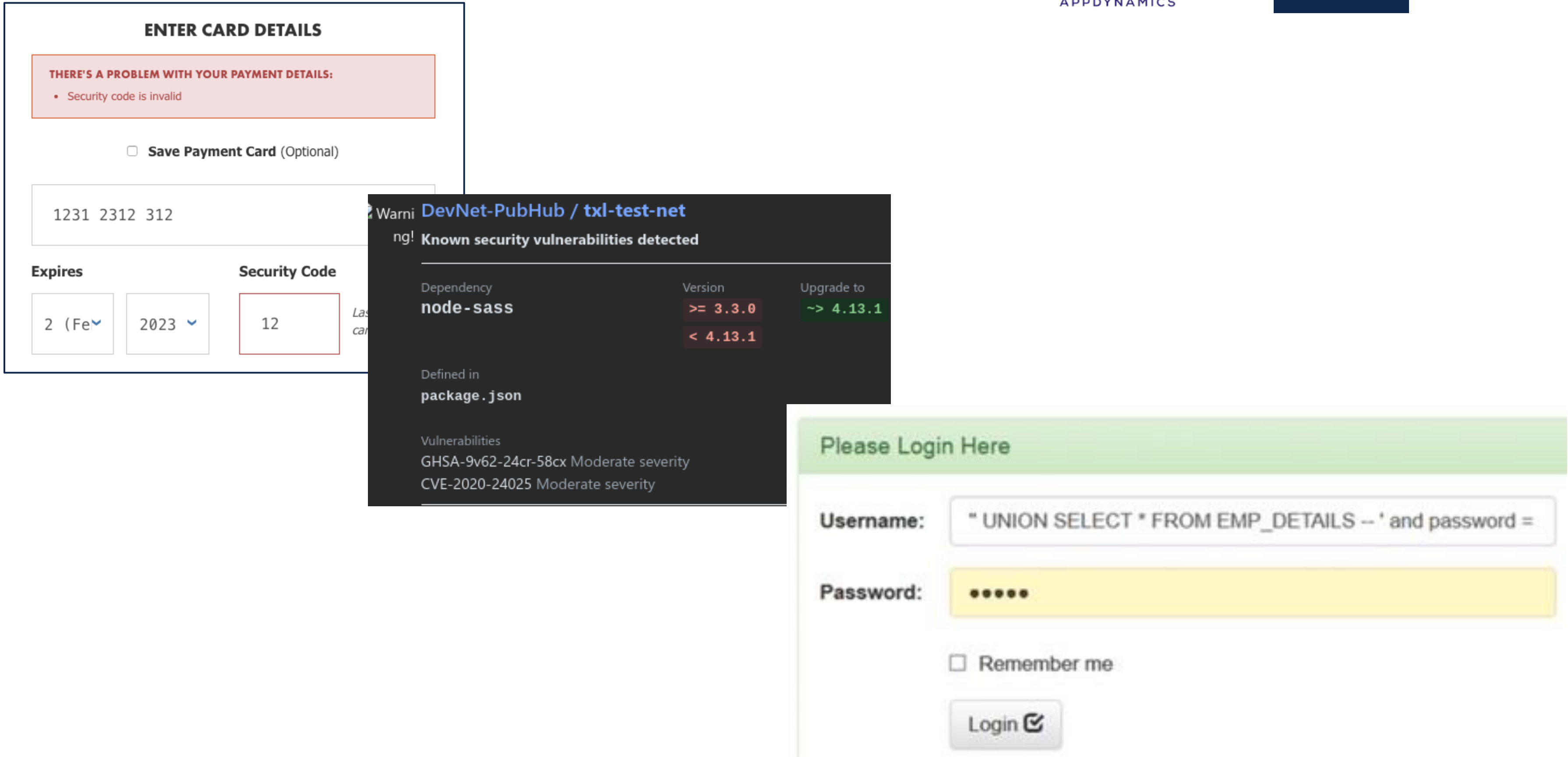


DevOps+NetOps+SecOps = 4Ever

Use-Cases / Scenarios

APPDYNAMICS

Cisco XDR



ENTER CARD DETAILS

THERE'S A PROBLEM WITH YOUR PAYMENT DETAILS:

- Security code is invalid

□ **Save Payment Card** (Optional)

1231 2312 312

Expires		**Security Code**
2 (Fe	2023	12

Las
car

Warning!

DevNet-PubHub / txl-test-net

Known security vulnerabilities detected

Dependency	Version	Upgrade to

`node-sass`	`>= 3.3.0`
	`< 4.13.1`
		`~> 4.13.1`

Defined in
`package.json`

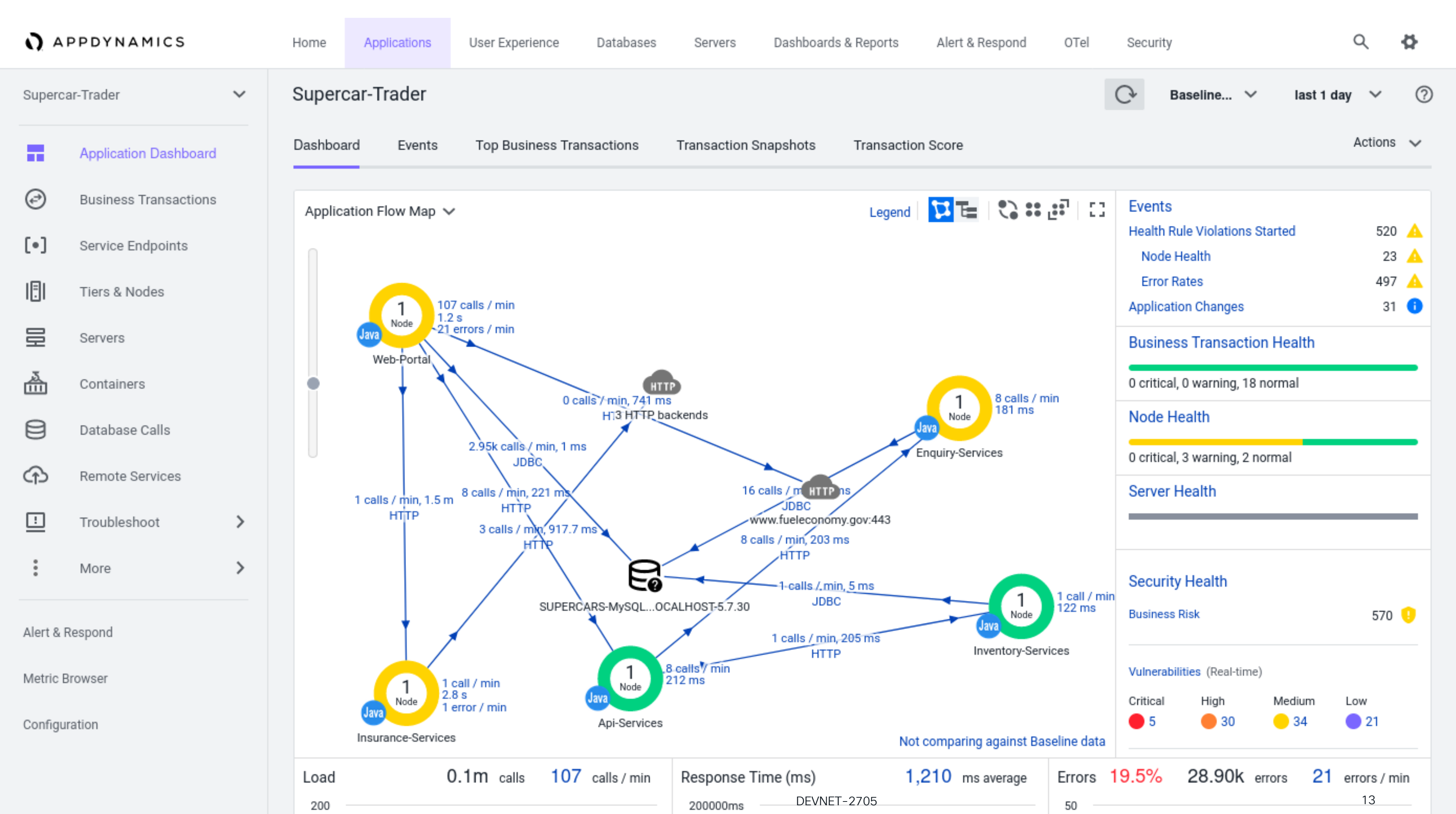
Vulnerabilities
GHSA-9v62-24cr-58cx Moderate severity
CVE-2020-24025 Moderate severity

Please Login Here

Username:	" UNION SELECT * FROM EMP_DETAILS -- ' and password =
Password:	●●●●●

□ Remember me

Cisco AppDynamics



Supercar-Trader

Events

Health Rule Violations Started	520
Node Health	23
Error Rates	497
Application Changes	31

Business Transaction Health

0 critical, 0 warning, 18 normal

Node Health

0 critical, 3 warning, 2 normal

Server Health

Security Health

Business Risk 570

Vulnerabilities (Real-time)

Critical	High	Medium	Low
5	30	34	21

Load 0.1m calls 107 calls / min

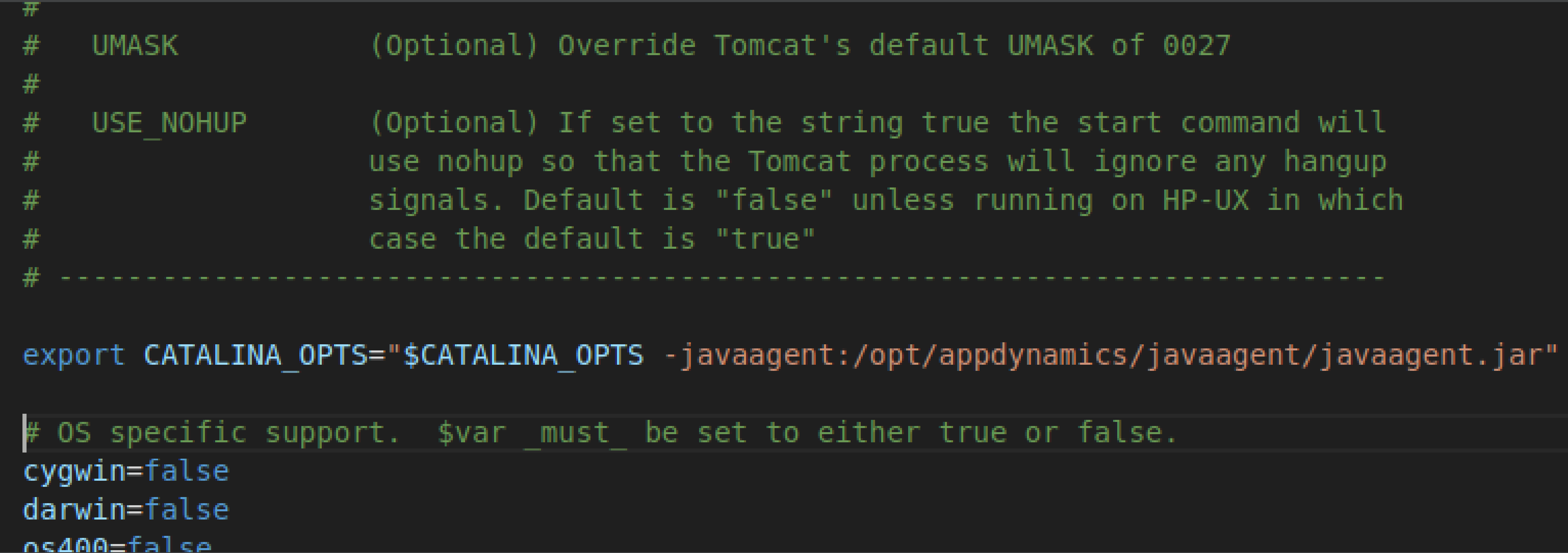
200

Response Time (ms) 1,210 ms average

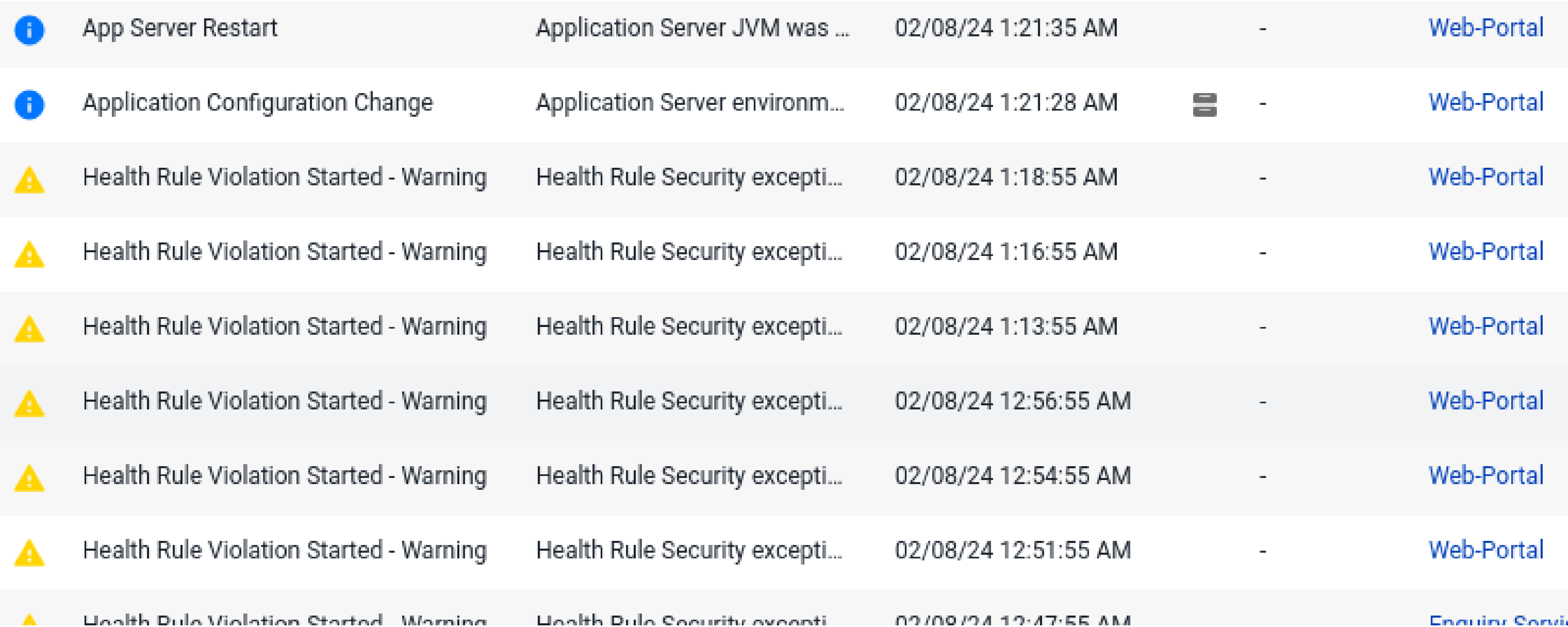
200000ms

Errors 19.5% 28.90k errors 21 errors / min

50

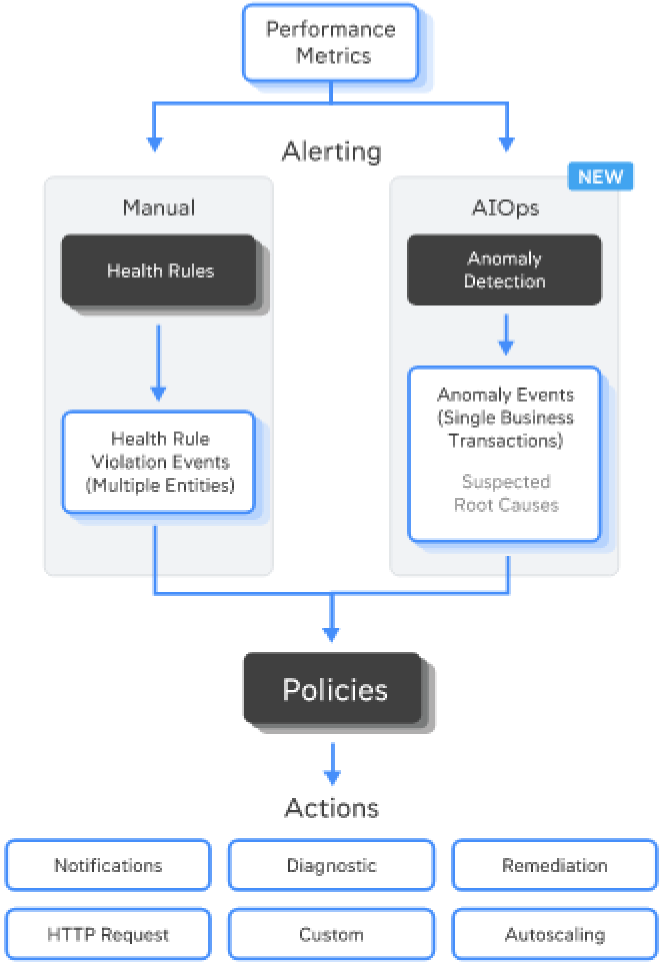


```
#
#   UMASK           (Optional) Override Tomcat's default UMASK of 0027
#
#   USE_NOHUP       (Optional) If set to the string true the start command will
#                   use nohup so that the Tomcat process will ignore any hangup
#                   signals. Default is "false" unless running on HP-UX in which
#                   case the default is "true"
# -----------------------------------------------------------------------------

export CATALINA_OPTS="$CATALINA_OPTS -javaagent:/opt/appdynamics/javaagent/javaagent.jar"

# OS specific support.  $var _must_ be set to either true or false.
cygwin=false
darwin=false
os400=false
```



ℹ	App Server Restart	Application Server JVM was ...	02/08/24 1:21:35 AM		-	Web-Portal
ℹ	Application Configuration Change	Application Server environm...	02/08/24 1:21:28 AM	🗄	-	Web-Portal
⚠	Health Rule Violation Started - Warning	Health Rule Security excepti...	02/08/24 1:18:55 AM		-	Web-Portal
⚠	Health Rule Violation Started - Warning	Health Rule Security excepti...	02/08/24 1:16:55 AM		-	Web-Portal
⚠	Health Rule Violation Started - Warning	Health Rule Security excepti...	02/08/24 1:13:55 AM		-	Web-Portal
⚠	Health Rule Violation Started - Warning	Health Rule Security excepti...	02/08/24 12:56:55 AM		-	Web-Portal
⚠	Health Rule Violation Started - Warning	Health Rule Security excepti...	02/08/24 12:54:55 AM		-	Web-Portal
⚠	Health Rule Violation Started - Warning	Health Rule Security excepti...	02/08/24 12:51:55 AM		-	Web-Portal
⚠	Health Rule Violation Started - Warning	Health Rule Security excepti...	02/08/24 12:47:55 AM			Enquiry Servi

Alert and Respond Overview



Performance Metrics

Alerting

Manual

Health Rules

Health Rule Violation Events (Multiple Entities)

NEW

AIOps

Anomaly Detection

Anomaly Events (Single Business Transactions)

Suspected Root Causes

Policies

Actions

Notifications

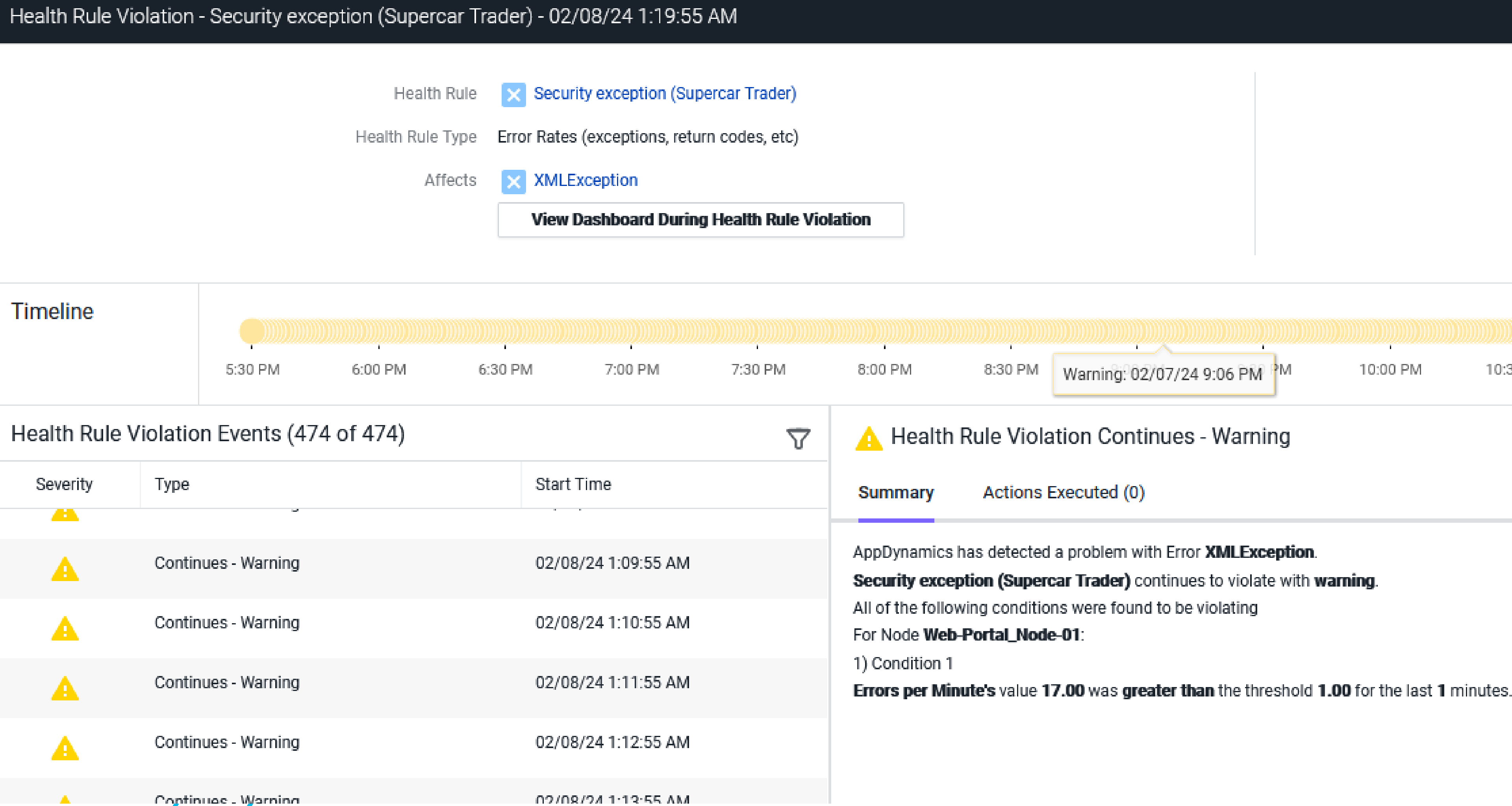
Diagnostic

Remediation

HTTP Request

Custom

Autoscaling



Health Rule Violation - Security exception (Supercar Trader) - 02/08/24 1:19:55 AM

Health Rule: Security exception (Supercar Trader)

Health Rule Type: Error Rates (exceptions, return codes, etc)

Affects: XMLException

Health Rule Violation Events (474 of 474)

Severity	Type	Start Time
⚠	Continues - Warning	02/08/24 1:09:55 AM
⚠	Continues - Warning	02/08/24 1:10:55 AM
⚠	Continues - Warning	02/08/24 1:11:55 AM
⚠	Continues - Warning	02/08/24 1:12:55 AM
⚠	Continues - Warning	02/08/24 1:13:55 AM

⚠ Health Rule Violation Continues - Warning

AppDynamics has detected a problem with Error **XMLException**.

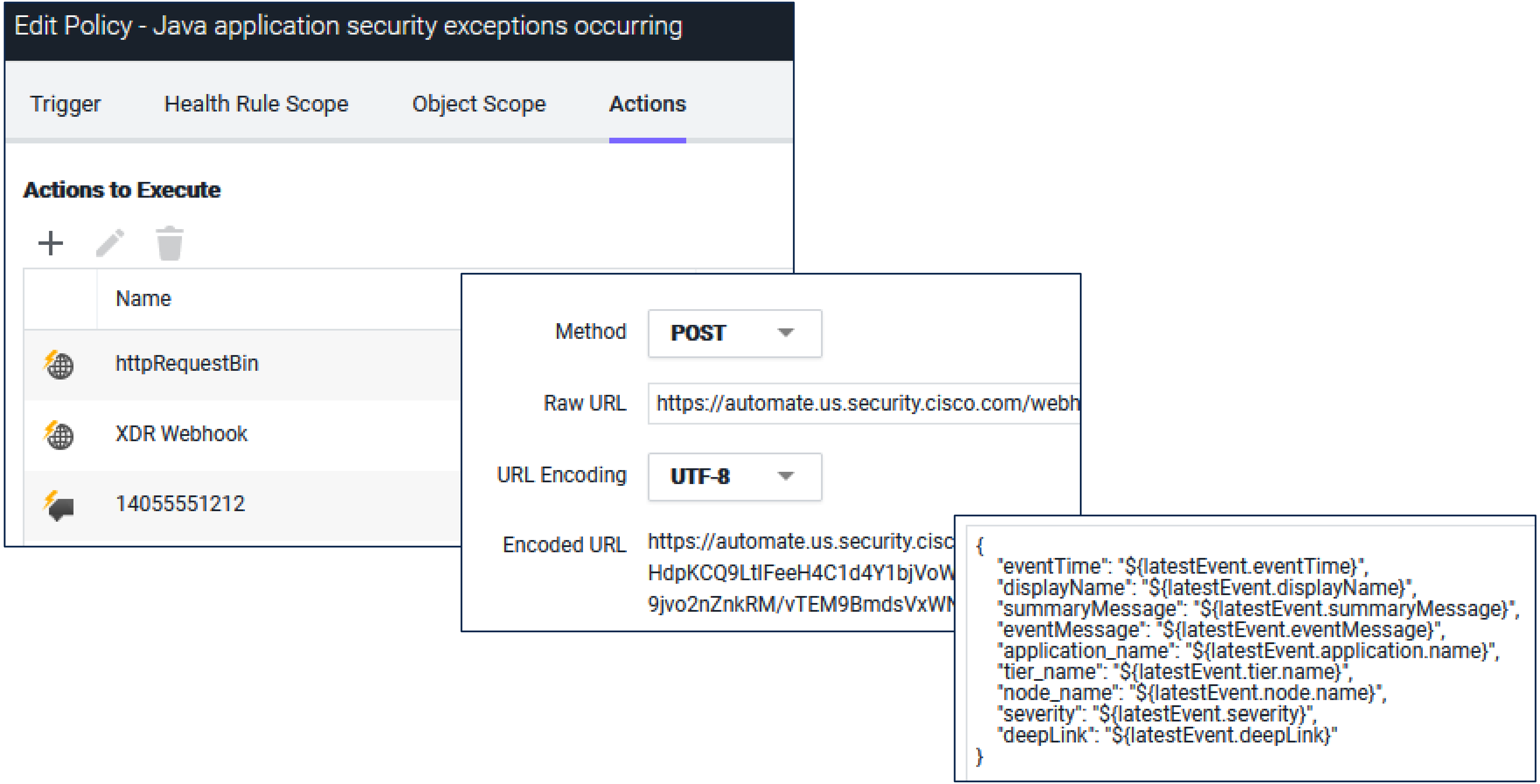
Security exception (Supercar Trader) continues to violate with **warning**.

All of the following conditions were found to be violating

For Node **Web-Portal_Node-01**:

1) Condition 1

Errors per Minute's value **17.00** was **greater than** the threshold **1.00** for the last **1** minutes.



Edit Policy - Java application security exceptions occurring

Actions to Execute

Name
httpRequestBin
XDR Webhook
14055551212

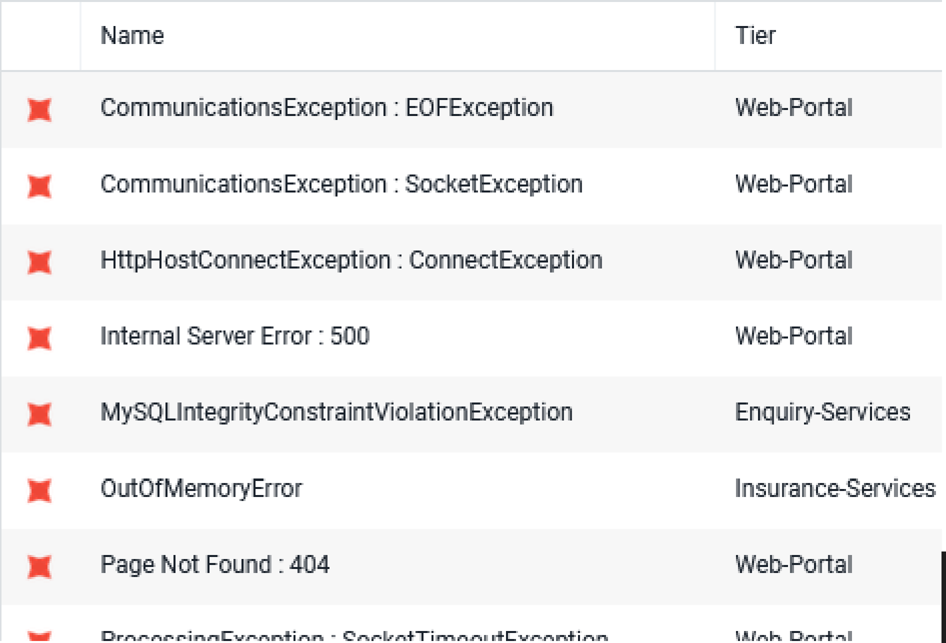
Method: POST

Raw URL: https://automate.us.security.cisco.com/webh

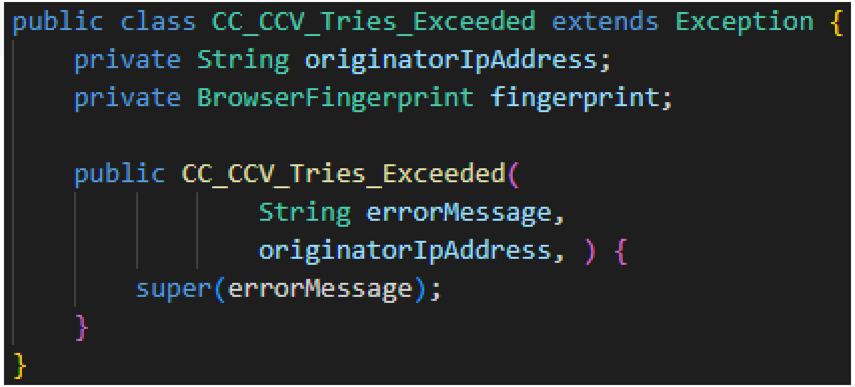
URL Encoding: UTF-8

Encoded URL: https://automate.us.security.cisc
HdpKCQ9LtlFeeH4C1d4Y1bjVoW
9jvo2nZnkRM/vTEM9BmdsVxWN

```
{
  "eventTime": "${latestEvent.eventTime}",
  "displayName": "${latestEvent.displayName}",
  "summaryMessage": "${latestEvent.summaryMessage}",
  "eventMessage": "${latestEvent.eventMessage}",
  "application_name": "${latestEvent.application.name}",
  "tier_name": "${latestEvent.tier.name}",
  "node_name": "${latestEvent.node.name}",
  "severity": "${latestEvent.severity}",
  "deepLink": "${latestEvent.deepLink}"
}
```

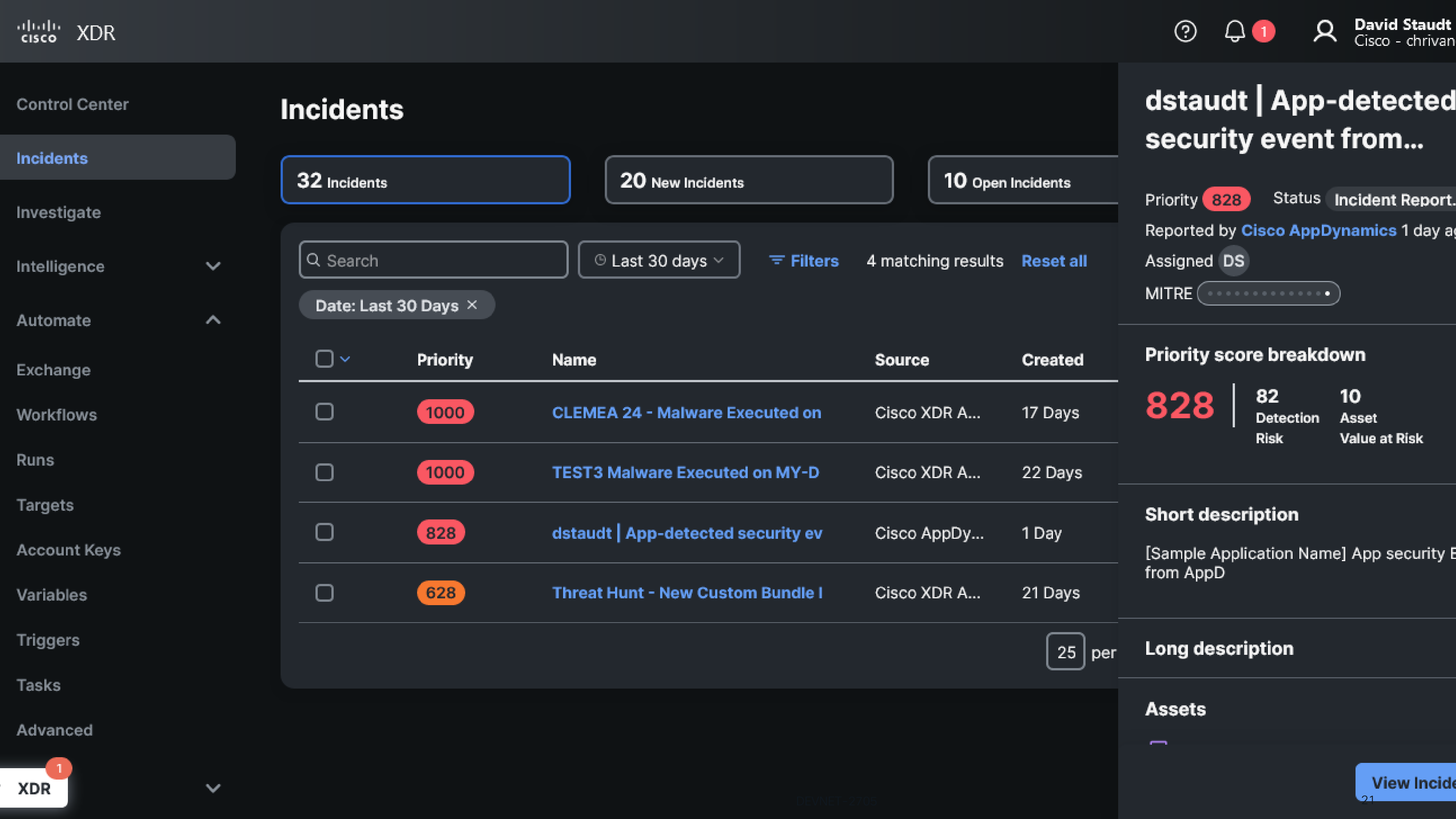


	Name	Tier
✖	CommunicationsException : EOFException	Web-Portal
✖	CommunicationsException : SocketException	Web-Portal
✖	HttpHostConnectException : ConnectException	Web-Portal
✖	Internal Server Error : 500	Web-Portal
✖	MySQLIntegrityConstraintViolationException	Enquiry-Services
✖	OutOfMemoryError	Insurance-Services
✖	Page Not Found : 404	Web-Portal
✖	ProcessingException : SocketTimeoutException	Web-Portal



```
public class CC_CCV_Tries_Exceeded extends Exception {
    private String originatorIpAddress;
    private BrowserFingerprint fingerprint;

    public CC_CCV_Tries_Exceeded(
            String errorMessage,
            originatorIpAddress, ) {
        super(errorMessage);
    }
}
```

Cisco XDR



Incidents

32 Incidents | 20 New Incidents | 10 Open Incidents

Search | Last 30 days | Filters | 4 matching results | Reset all

Date: Last 30 Days ✕

□	Priority	Name	Source	Created
□	1000	CLEMEA 24 - Malware Executed on	Cisco XDR A...	17 Days
□	1000	TEST3 Malware Executed on MY-D	Cisco XDR A...	22 Days
□	828	dstaudt | App-detected security ev	Cisco AppDy...	1 Day
□	628	Threat Hunt - New Custom Bundle I	Cisco XDR A...	21 Days

25 per

dstaudt | App-detected security event from...

Priority 828 Status Incident Report.

Reported by Cisco AppDynamics 1 day ag

Assigned DS

MITRE

Priority score breakdown

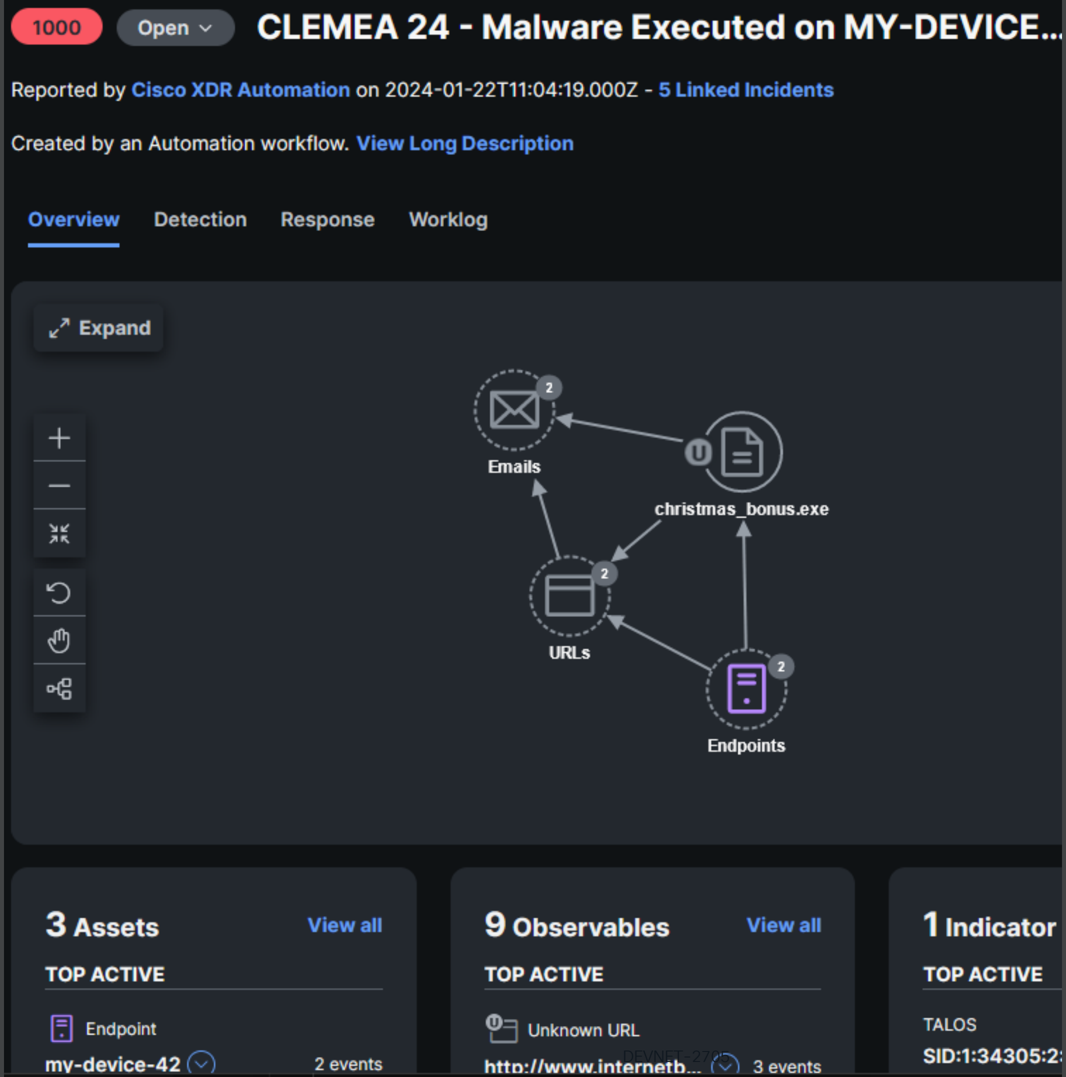
828 | 82 Detection Risk | 10 Asset Value at Risk

Short description

[Sample Application Name] App security E from AppD

Long description

Assets



1000 Open

CLEMEA 24 - Malware Executed on MY-DEVICE...

Reported by Cisco XDR Automation on 2024-01-22T11:04:19.000Z - 5 Linked Incidents

Created by an Automation workflow. View Long Description

3 Assets View all

TOP ACTIVE

Endpoint

my-device-42 2 events

9 Observables View all

TOP ACTIVE

Unknown URL

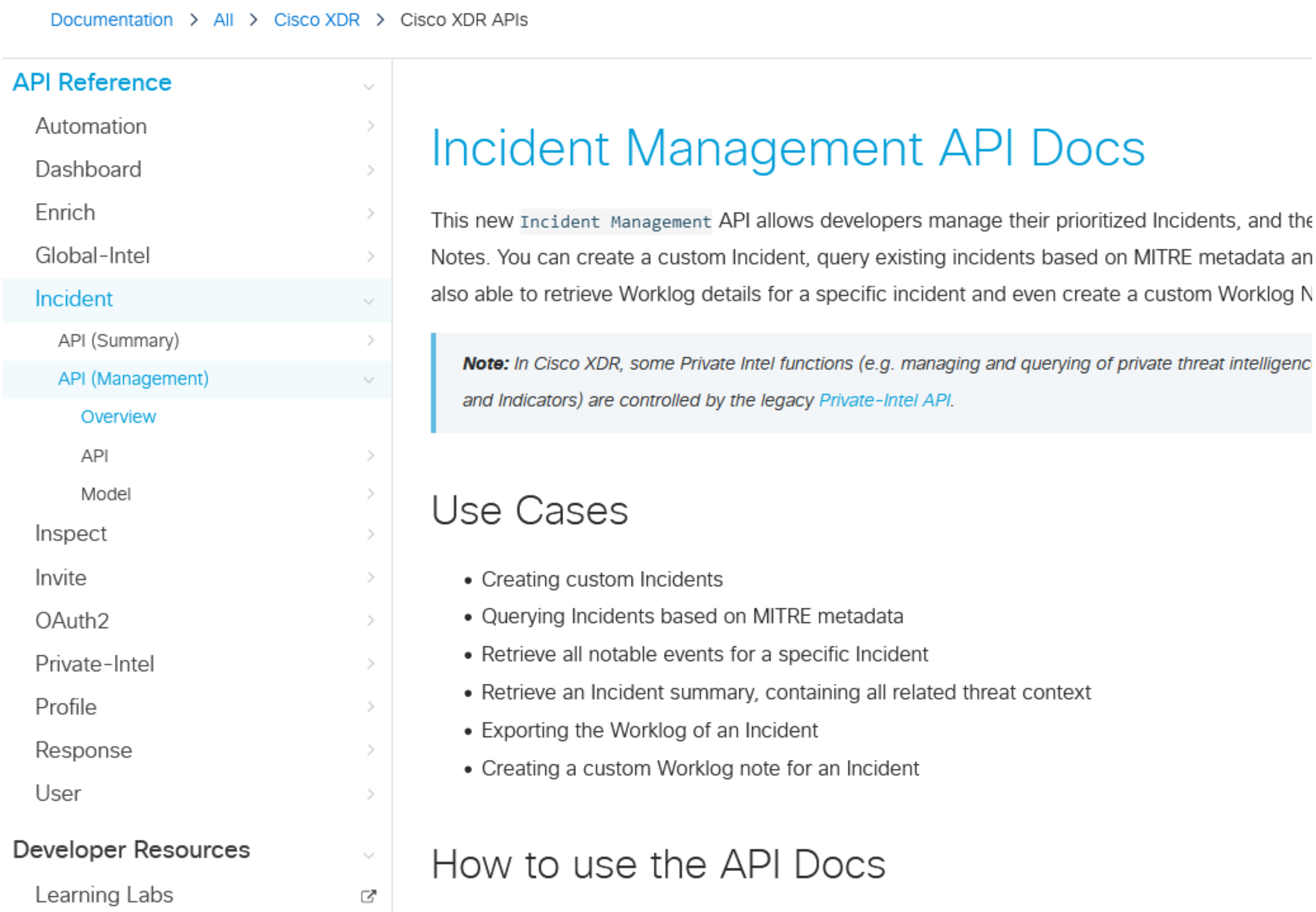
http://www.internetb... 3 events

1 Indicator

TOP ACTIVE

TALOS

SID:1:34305:2



Incident Management API Docs

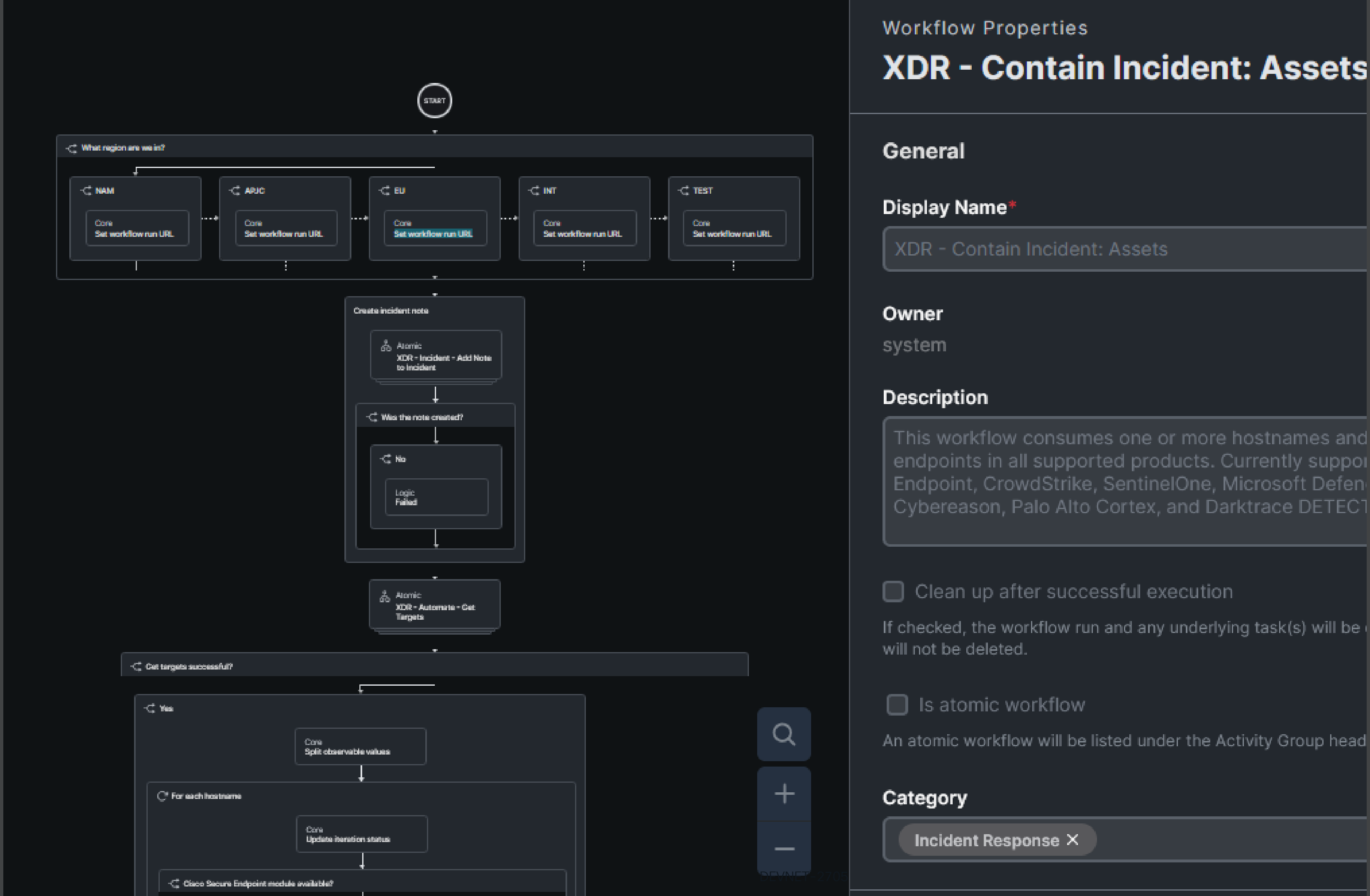
This new `Incident Management` API allows developers manage their prioritized Incidents, and the Notes. You can create a custom Incident, query existing incidents based on MITRE metadata an also able to retrieve Worklog details for a specific incident and even create a custom Worklog N

> ***Note:*** *In Cisco XDR, some Private Intel functions (e.g. managing and querying of private threat intelligenc and Indicators) are controlled by the legacy Private-Intel API.*

Use Cases

- Creating custom Incidents
- Querying Incidents based on MITRE metadata
- Retrieve all notable events for a specific Incident
- Retrieve an Incident summary, containing all related threat context
- Exporting the Worklog of an Incident
- Creating a custom Worklog note for an Incident

How to use the API Docs



Workflow Properties

XDR - Contain Incident: Assets

General

Display Name*

XDR - Contain Incident: Assets

Owner

system

Description

This workflow consumes one or more hostnames and
endpoints in all supported products. Currently suppo
Endpoint, CrowdStrike, SentinelOne, Microsoft Defen
Cybereason, Palo Alto Cortex, and Darktrace DETECT

□ Clean up after successful execution

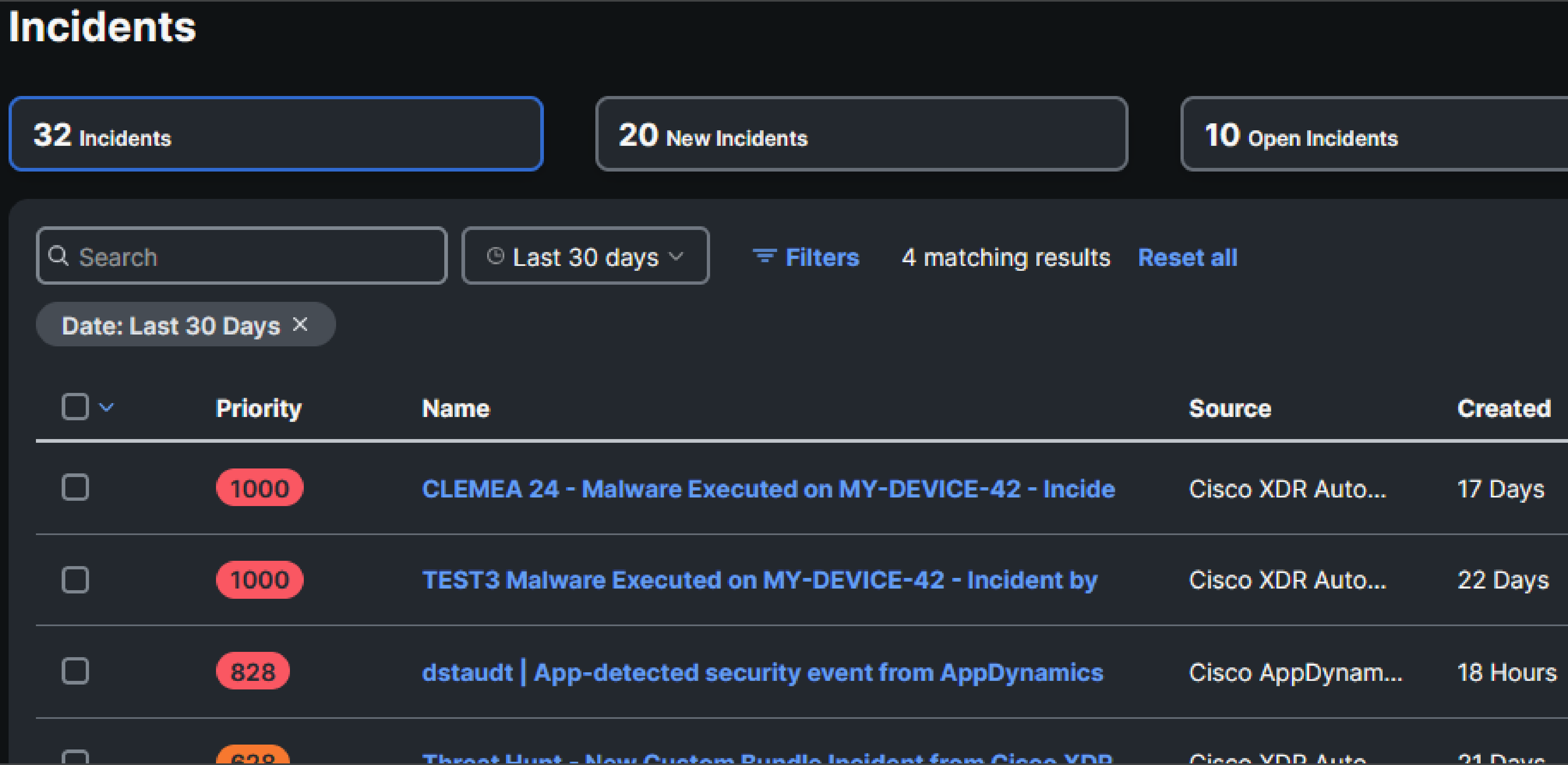
If checked, the workflow run and any underlying task(s) will be
will not be deleted.

□ Is atomic workflow

An atomic workflow will be listed under the Activity Group head

Category

Incident Response ✕



Incidents

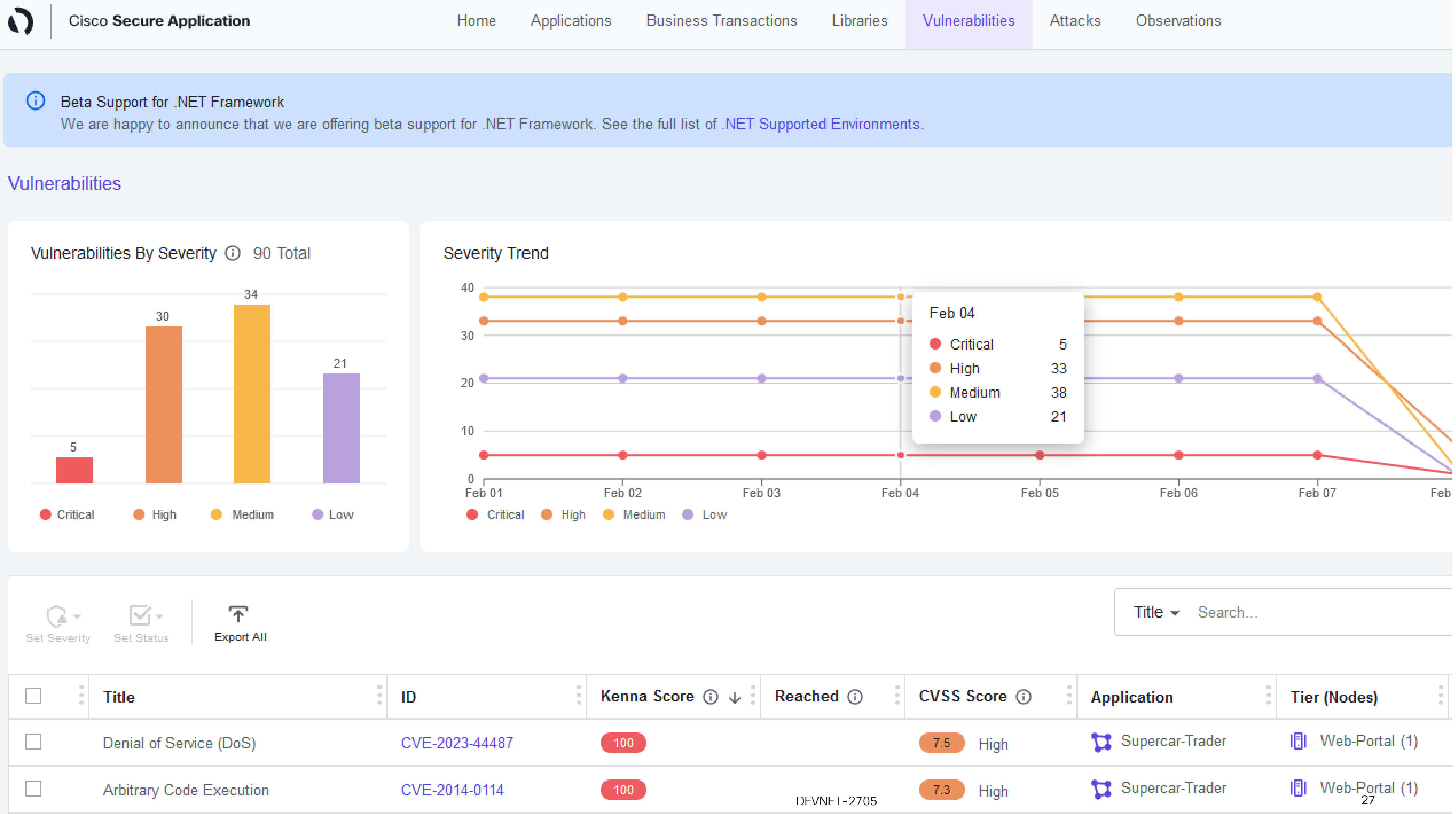
32 Incidents | 20 New Incidents | 10 Open Incidents

Search | Last 30 days | Filters | 4 matching results | Reset all

Date: Last 30 Days ×

□	Priority	Name	Source	Created
□	1000	CLEMEA 24 - Malware Executed on MY-DEVICE-42 - Incide	Cisco XDR Auto...	17 Days
□	1000	TEST3 Malware Executed on MY-DEVICE-42 - Incident by	Cisco XDR Auto...	22 Days
□	828	dstaudt | App-detected security event from AppDynamics	Cisco AppDynam...	18 Hours
□	628	Threat Hunt - New Custom Bundle Incident from Cisco XDR	Cisco XDR Auto...	21 Days

Cisco Appdynamics
+
Cisco Secure Application

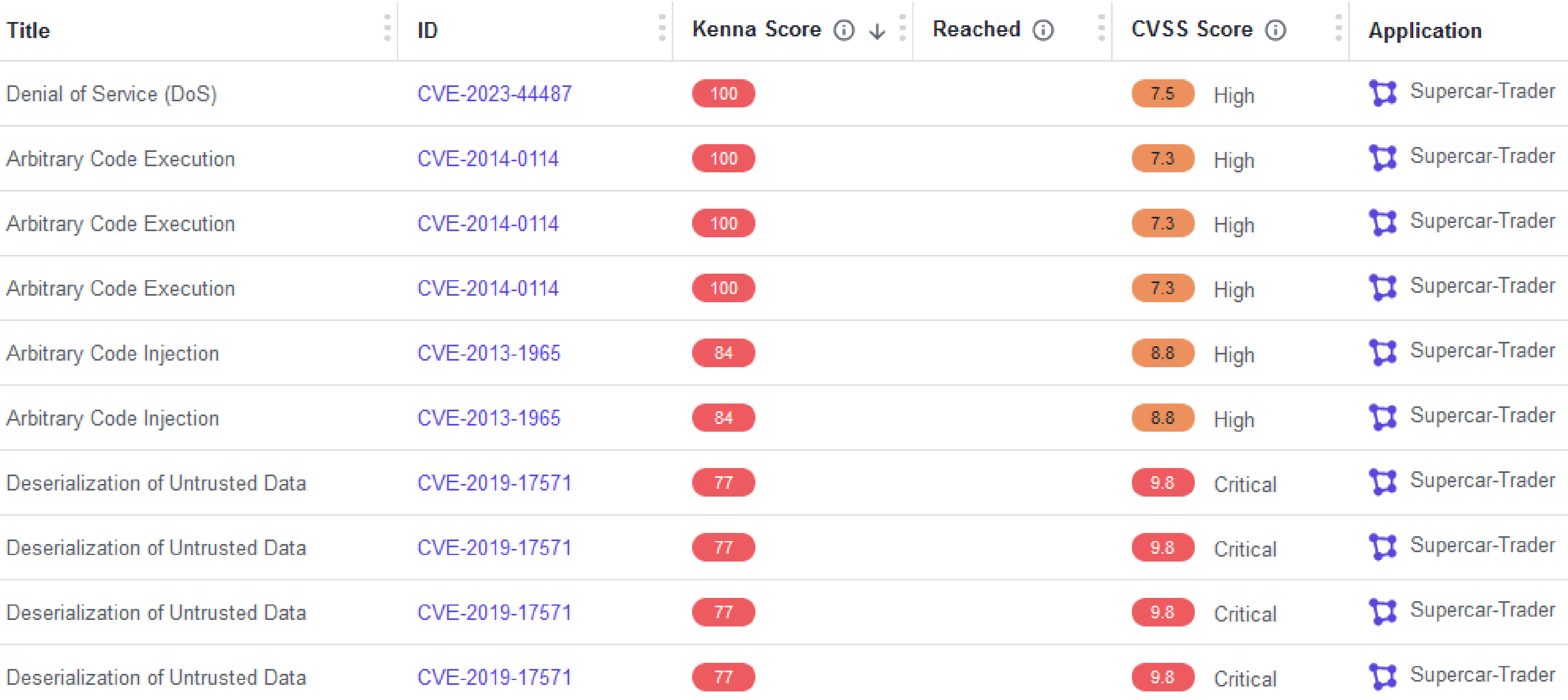


Beta Support for .NET Framework

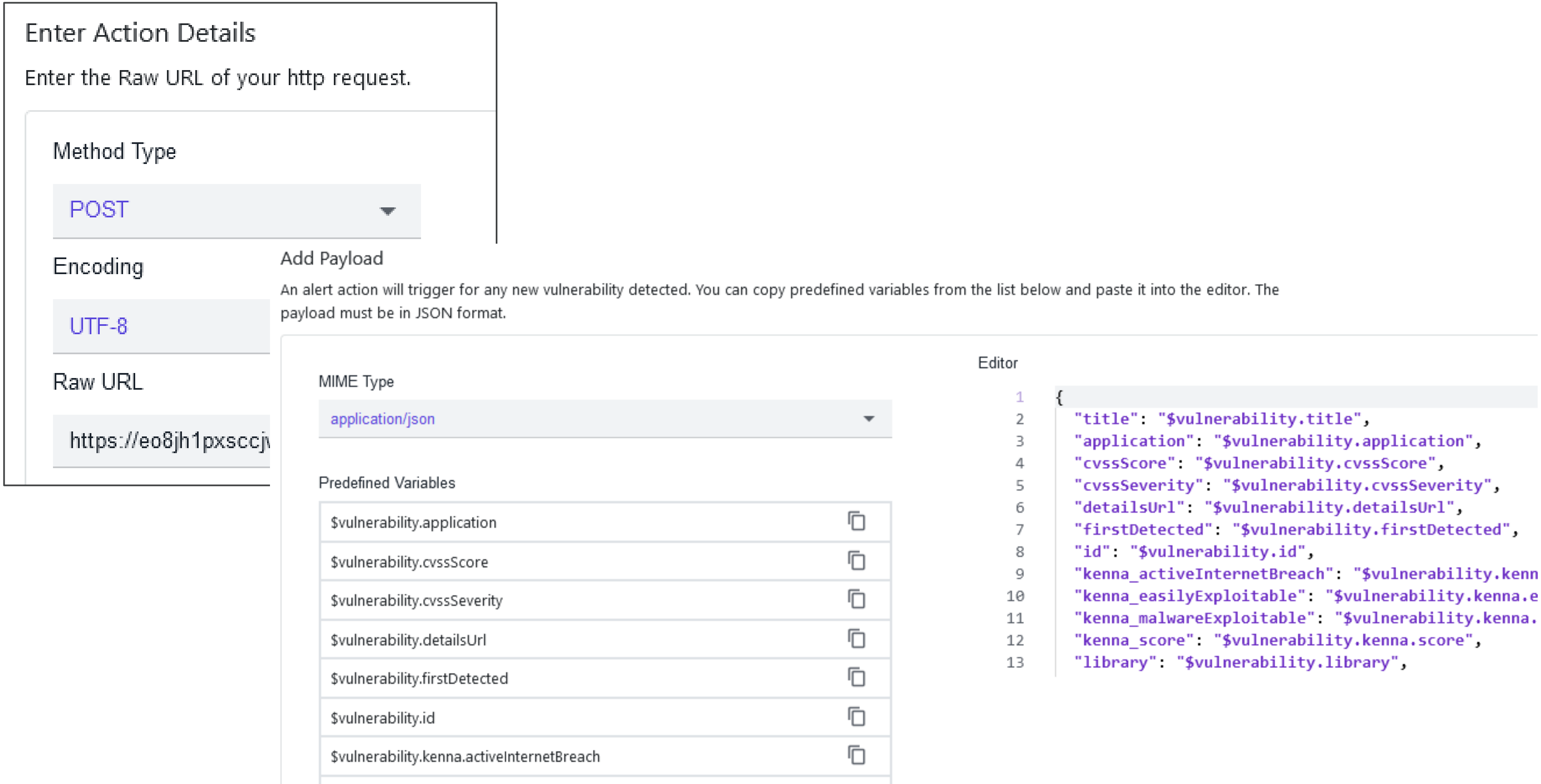
We are happy to announce that we are offering beta support for .NET Framework. See the full list of .NET Supported Environments.

Vulnerabilities

☐	Title	ID	Kenna Score	Reached	CVSS Score	Application	Tier (Nodes)
☐	Denial of Service (DoS)	CVE-2023-44487	100		7.5 High	Supercar-Trader	Web-Portal (1)
☐	Arbitrary Code Execution	CVE-2014-0114	100		7.3 High	Supercar-Trader	Web-Portal (1)



Title	ID	Kenna Score ⓘ ↓	Reached ⓘ	CVSS Score ⓘ		Application
Denial of Service (DoS)	CVE-2023-44487	100		7.5	High	Supercar-Trader
Arbitrary Code Execution	CVE-2014-0114	100		7.3	High	Supercar-Trader
Arbitrary Code Execution	CVE-2014-0114	100		7.3	High	Supercar-Trader
Arbitrary Code Execution	CVE-2014-0114	100		7.3	High	Supercar-Trader
Arbitrary Code Injection	CVE-2013-1965	84		8.8	High	Supercar-Trader
Arbitrary Code Injection	CVE-2013-1965	84		8.8	High	Supercar-Trader
Deserialization of Untrusted Data	CVE-2019-17571	77		9.8	Critical	Supercar-Trader
Deserialization of Untrusted Data	CVE-2019-17571	77		9.8	Critical	Supercar-Trader
Deserialization of Untrusted Data	CVE-2019-17571	77		9.8	Critical	Supercar-Trader
Deserialization of Untrusted Data	CVE-2019-17571	77		9.8	Critical	Supercar-Trader



Enter Action Details

Enter the Raw URL of your http request.

Method Type: POST

Encoding: UTF-8

Raw URL: https://eo8jh1pxsccj

Add Payload

An alert action will trigger for any new vulnerability detected. You can copy predefined variables from the list below and paste it into the editor. The payload must be in JSON format.

MIME Type: application/json

Predefined Variables

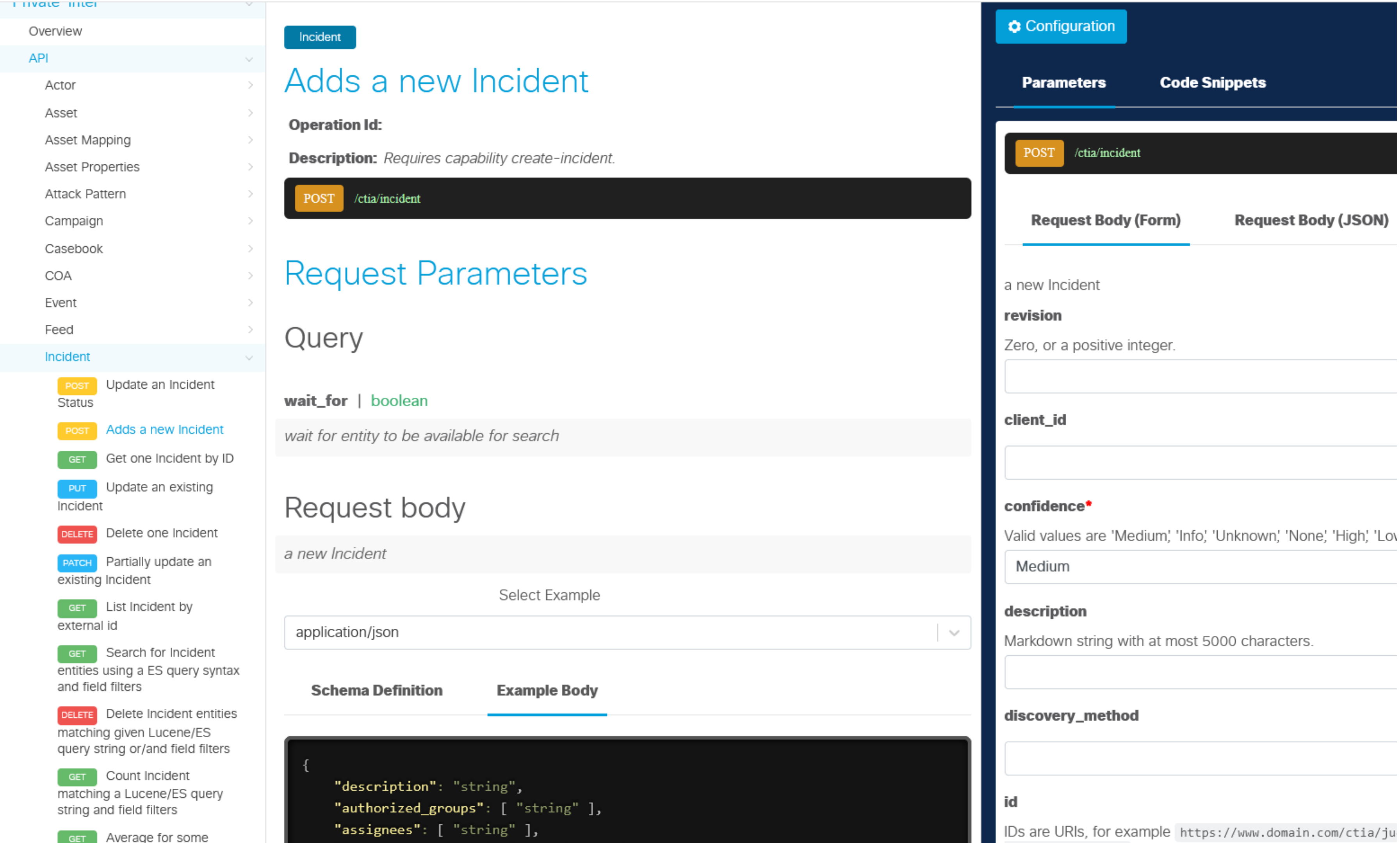
- $vulnerability.application
- $vulnerability.cvssScore
- $vulnerability.cvssSeverity
- $vulnerability.detailsUrl
- $vulnerability.firstDetected
- $vulnerability.id
- $vulnerability.kenna.activeInternetBreach

Editor

```
{
  "title": "$vulnerability.title",
  "application": "$vulnerability.application",
  "cvssScore": "$vulnerability.cvssScore",
  "cvssSeverity": "$vulnerability.cvssSeverity",
  "detailsUrl": "$vulnerability.detailsUrl",
  "firstDetected": "$vulnerability.firstDetected",
  "id": "$vulnerability.id",
  "kenna_activeInternetBreach": "$vulnerability.kenn
  "kenna_easilyExploitable": "$vulnerability.kenna.e
  "kenna_malwareExploitable": "$vulnerability.kenna.
  "kenna_score": "$vulnerability.kenna.score",
  "library": "$vulnerability.library",
```

Cisco XDR

	Known	Unknown
Known	KK	KU
Unknown	UK	UU



Private Intel

Overview

API

- Actor
- Asset
- Asset Mapping
- Asset Properties
- Attack Pattern
- Campaign
- Casebook
- COA
- Event
- Feed
- Incident
  - POST Update an Incident Status
  - POST Adds a new Incident
  - GET Get one Incident by ID
  - PUT Update an existing Incident
  - DELETE Delete one Incident
  - PATCH Partially update an existing Incident
  - GET List Incident by external id
  - GET Search for Incident entities using a ES query syntax and field filters
  - DELETE Delete Incident entities matching given Lucene/ES query string or/and field filters
  - GET Count Incident matching a Lucene/ES query string and field filters
  - GET Average for some

Incident

Adds a new Incident

Operation Id:

Description: *Requires capability create-incident.*

POST /ctia/incident

Request Parameters

Query

wait_for | boolean

wait for entity to be available for search

Request body

a new Incident

Select Example

application/json

Schema Definition | Example Body

```
{
    "description": "string",
    "authorized_groups": [ "string" ],
    "assignees": [ "string" ],
```

Configuration

Parameters | Code Snippets

POST /ctia/incident

Request Body (Form) | Request Body (JSON)

a new Incident

revision

Zero, or a positive integer.

client_id

confidence*

Valid values are 'Medium', 'Info', 'Unknown', 'None', 'High', 'Lo

Medium

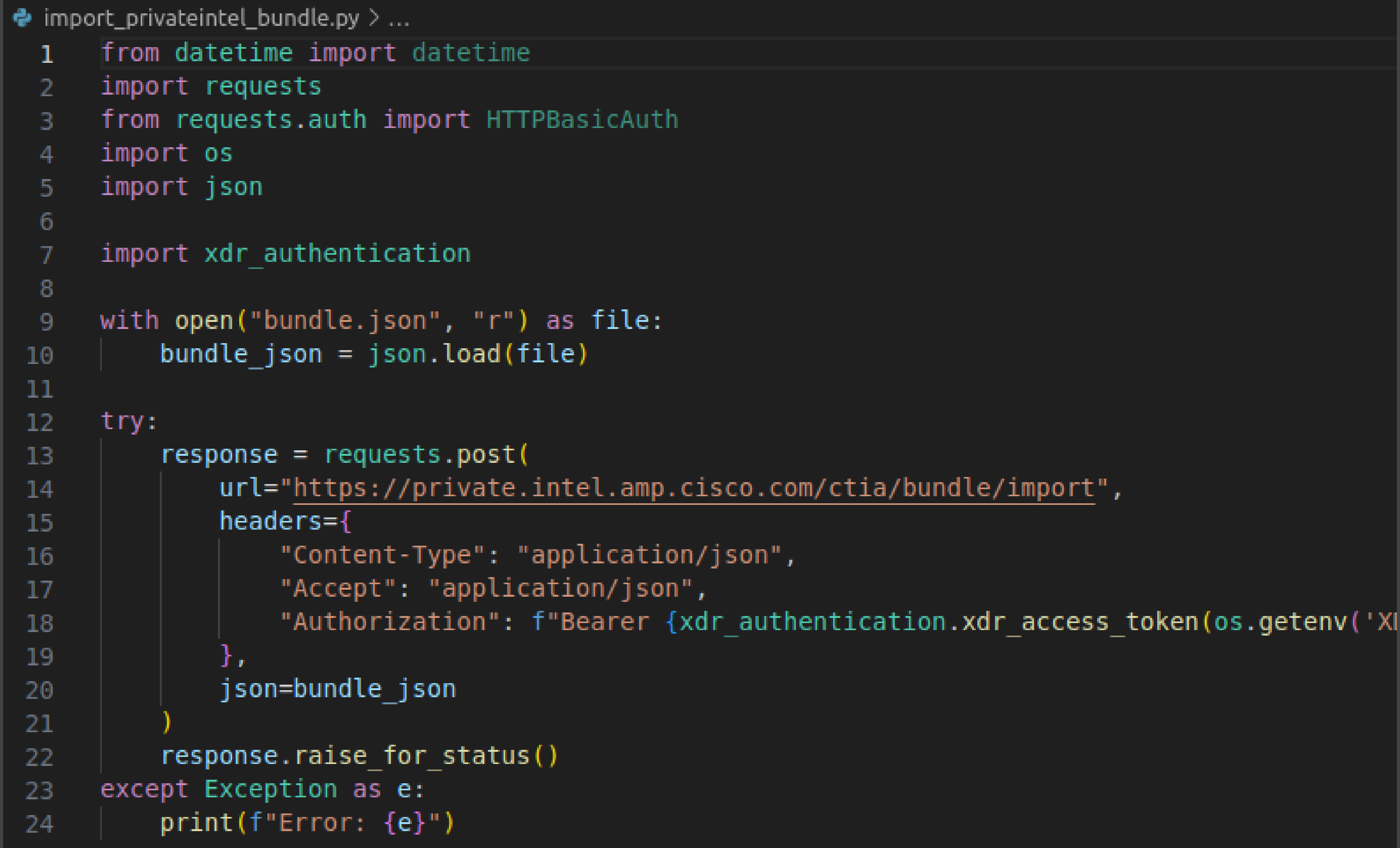
description

Markdown string with at most 5000 characters.

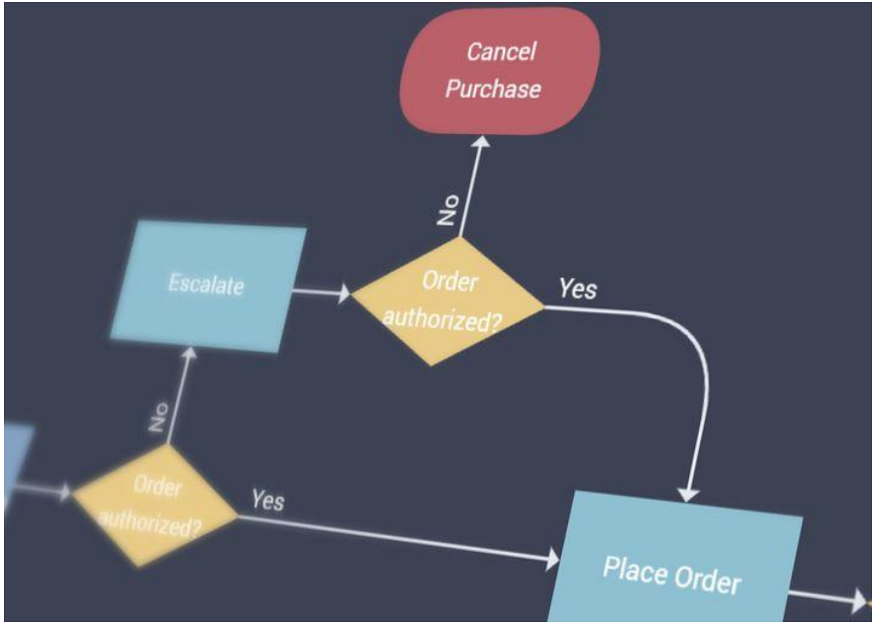
discovery_method

id

IDs are URIs, for example `https://www.domain.com/ctia/ju`

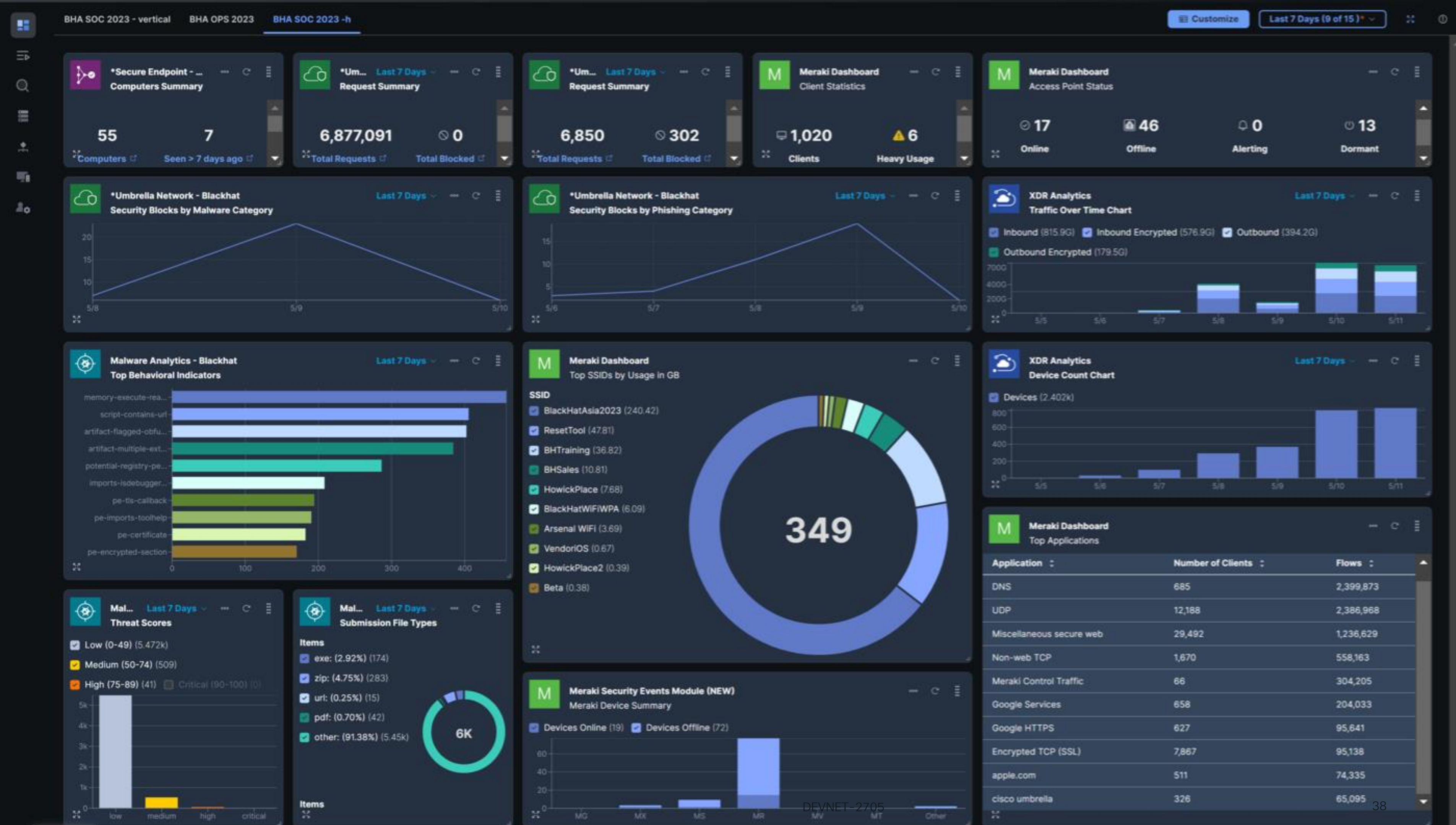


```python
from datetime import datetime
import requests
from requests.auth import HTTPBasicAuth
import os
import json

import xdr_authentication

with open("bundle.json", "r") as file:
    bundle_json = json.load(file)

try:
    response = requests.post(
        url="https://private.intel.amp.cisco.com/ctia/bundle/import",
        headers={
            "Content-Type": "application/json",
            "Accept": "application/json",
            "Authorization": f"Bearer {xdr_authentication.xdr_access_token(os.getenv('X
        },
        json=bundle_json
    )
    response.raise_for_status()
except Exception as e:
    print(f"Error: {e}")
```


Cancel Purchase
No
Escalate
Order authorized?
Yes
No
Order authorized?
Yes
Place Order

Cisco XDR

Better Together



***Secure Endpoint - ...**
Computers Summary

55 Computers
7 Seen > 7 days ago

***Um...**
Request Summary

6,877,091 Total Requests
0 Total Blocked

***Um...**
Request Summary

6,850 Total Requests
302 Total Blocked

Meraki Dashboard
Client Statistics

1,020 Clients
⚠ 6 Heavy Usage

Meraki Dashboard
Access Point Status

17 Online
46 Offline
0 Alerting
13 Dormant

***Umbrella Network - Blackhat**
Security Blocks by Malware Category

***Umbrella Network - Blackhat**
Security Blocks by Phishing Category

XDR Analytics
Traffic Over Time Chart

☑ Inbound (815.9G) ☑ Inbound Encrypted (576.9G) ☑ Outbound (394.2G)
☑ Outbound Encrypted (179.5G)

Malware Analytics - Blackhat
Top Behavioral Indicators

Meraki Dashboard
Top SSIDs by Usage in GB

SSID
☑ BlackHatAsia2023 (240.42)
☑ ResetTool (47.81)
☑ BHTraining (36.82)
☑ BHSales (10.81)
☑ HowickPlace (7.68)
☑ BlackHatWiFiWPA (6.09)
☑ Arsenal WiFi (3.69)
☑ VendorIOS (0.67)
☑ HowickPlace2 (0.39)
☑ Beta (0.38)

XDR Analytics
Device Count Chart

☑ Devices (2.402k)

Meraki Dashboard
Top Applications

Application	Number of Clients	Flows
DNS	685	2,399,873
UDP	12,188	2,386,968
Miscellaneous secure web	29,492	1,236,629
Non-web TCP	1,670	558,163
Meraki Control Traffic	66	304,205
Google Services	658	204,033
Google HTTPS	627	95,641
Encrypted TCP (SSL)	7,867	95,138
apple.com	511	74,335
cisco umbrella	326	65,095

Mal...
Threat Scores

☑ Low (0-49) (5.472k)
☑ Medium (50-74) (509)
☑ High (75-89) (41) □ Critical (90-100) (0)

Mal...
Submission File Types

Items
☑ exe: (2.92%) (174)
☑ zip: (4.75%) (283)
☑ url: (0.25%) (15)
☑ pdf: (0.70%) (42)
☑ other: (91.38%) (5.45k)

Items

Meraki Security Events Module (NEW)
Meraki Device Summary

☑ Devices Online (19) ☑ Devices Offline (72)

The bridge to possible

Thank you

cisco Live!

Let’s go