From Zero to a DevSecOps Hero: Extending Microsoft Sentinel

Gareth Emslie
Product Manager &
Tech Evangelist

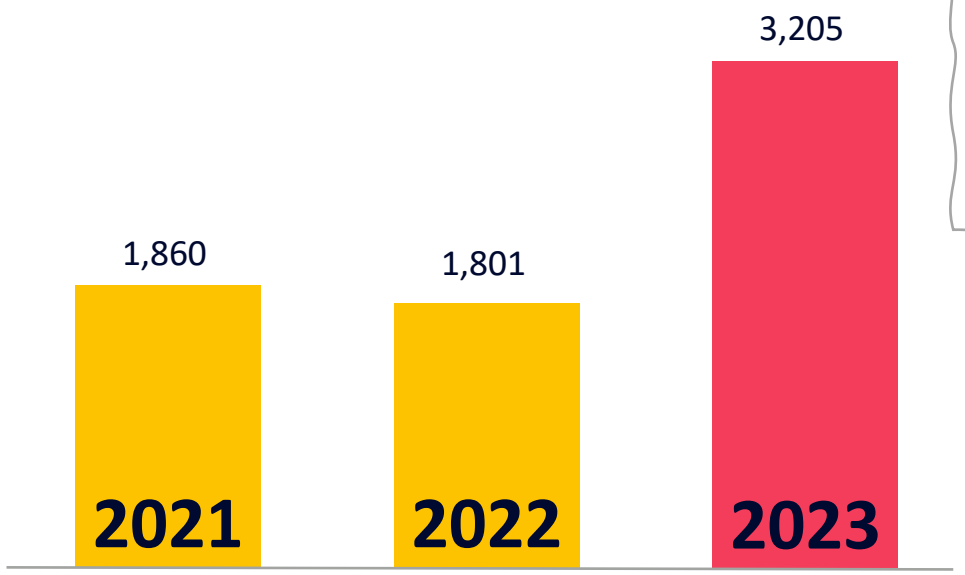
Disclaimer

- The information presented in this session is based on my personal experience and opinions and not those of my employer
- Mention of any specific product or service does not imply endorsement
- I don’t claim to be an expert in ***all | any*** the areas we will talk about today 😀

“The world’s most valuable resource is no longer oil, but data “

6th May 2017

The value of data has not gone un-noticed by attackers



353,027,892 individuals

78% increase

Source: Identity Theft Resource Center 2023 Data Breach Report; secureframe;

Social engineering & Ransomware lead the pack; Malware and Zero Day attacks jumped significantly during this period

18.5%

Social engineering

10.4%

Ransomware

4.9%

Malware

4.6%

Zero-Day

74% of all breaches included a human element

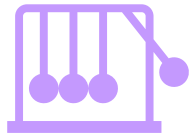
Source: Identity Theft Resource Center 2023 Data Breach Report; secureframe;

Today's operations teams are not only challenged by attackers

Complexity

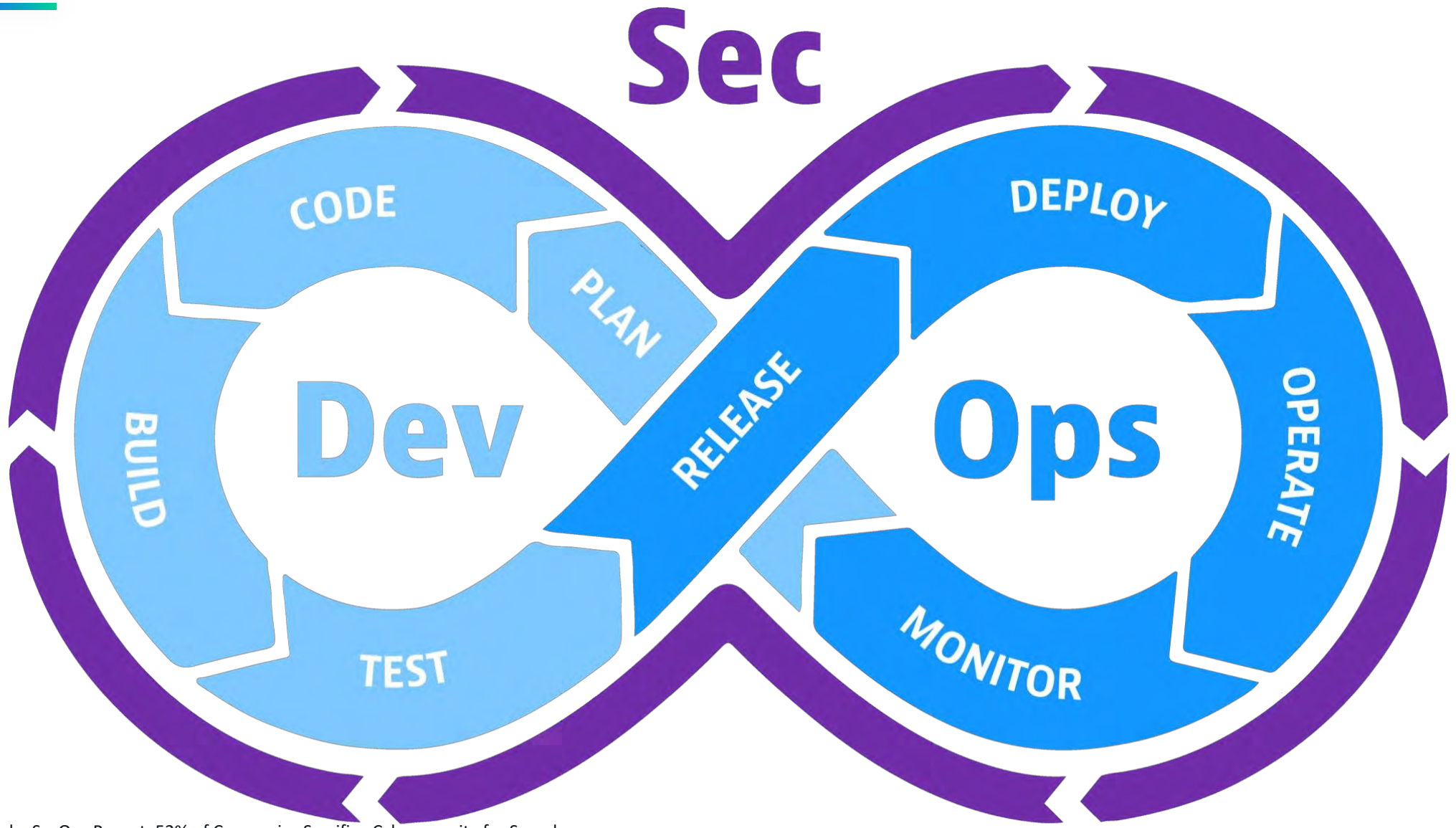
Volume

Cost



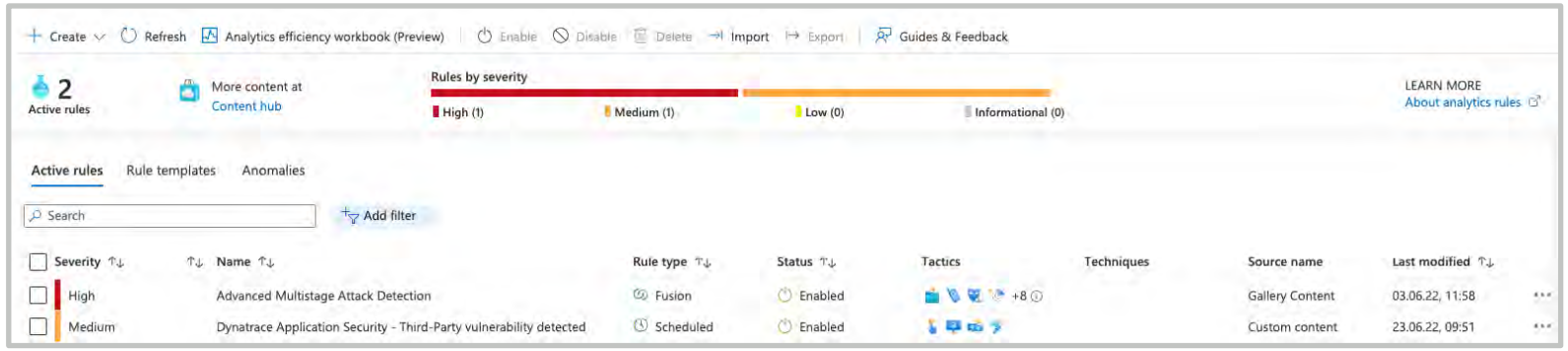
Correlation

52% of organizations report sacrificing cybersecurity for speed-to-market



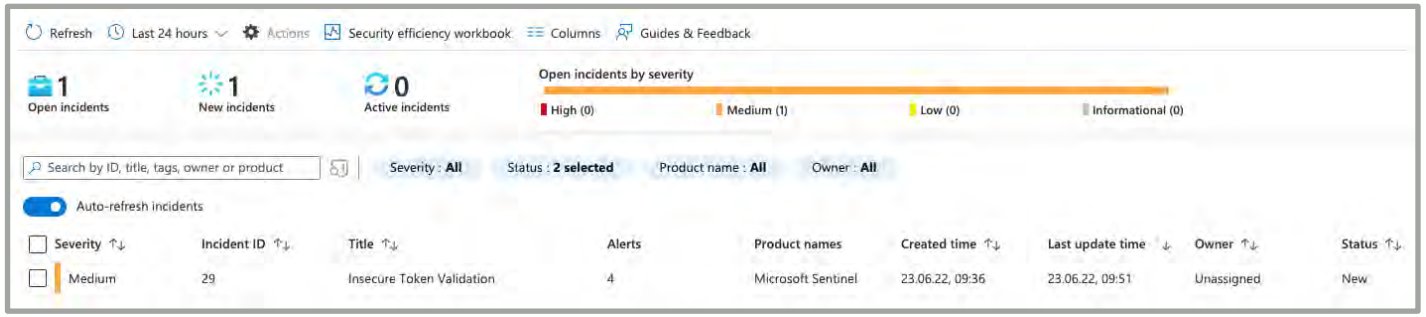
Source: Threat Stack - SecOps Report: 52% of Companies Sacrifice Cybersecurity for Speed

Sentinel enables SOC teams to perform threat hunting, leverage SOAR capabilities for incident lifecycle; Remediation tasks can also be defined within external systems



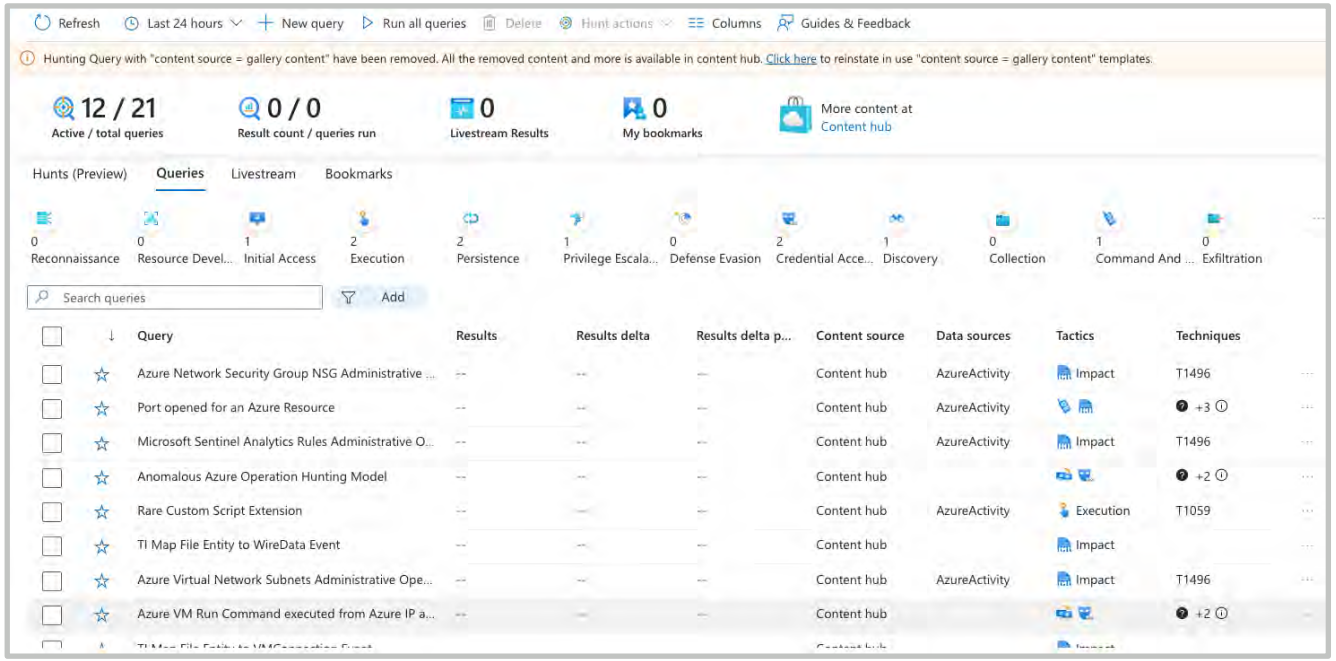
- Define complex analytics rules
- Trigger automated Incident creation

- Manage Incidents centrally
- Trigger remediation tasks



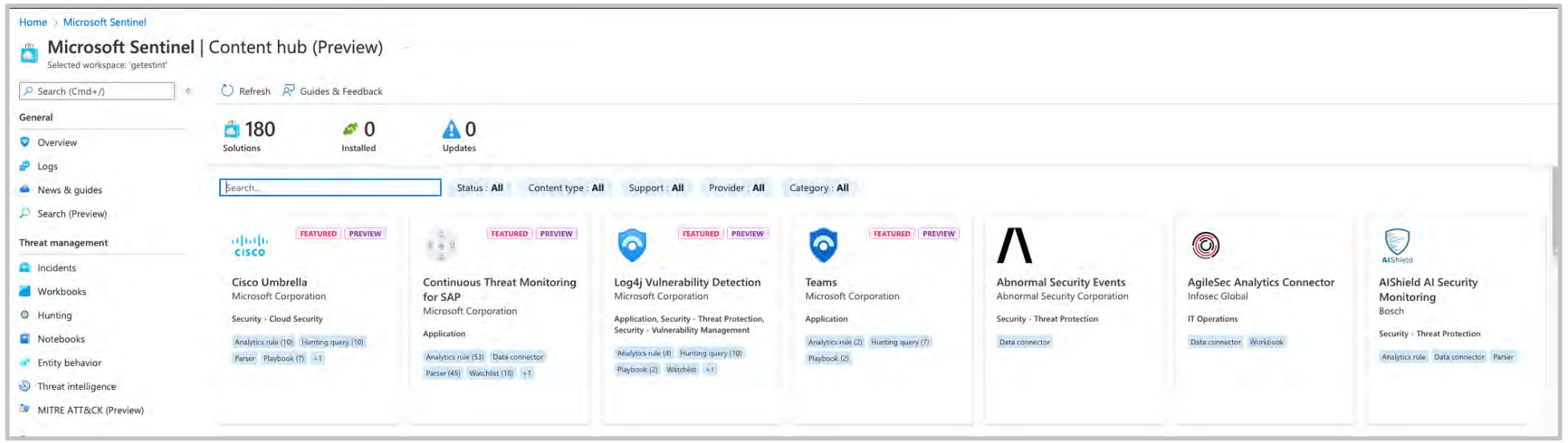
Microsoft Sentinel uses the MITRE ATT&CK framework to categorize and order queries by tactics

Search and query tools in Microsoft Sentinel to hunt for security threats and tactics throughout your environment



Built-in queries help guide your hunting and help you follow the correct trails uncovering issues in your environment

Microsoft Sentinel allows SOC teams to acquire connectors from a public content hub



Microsoft partners are able to publish their connectors to the Sentinel Content Hub for easy acquisition by their customers

Choose a vendor who has important insights that we could add to our DevSecOps lifecycle

Dynatrace's Runtime Application Protection

- Detection of SQL injection, JNDI injection, command injection, and SSRF attacks
- Code-level visibility provided by OneAgent
- Configurable automatic blocking of detected attacks

- Get all attacks
- Get attack details

Azure Logic Apps

- ☑ Acquired through the Content Hub
- ☐/ Intermed… support
- ☒ Additiona… resource…

VS

Azure Functions

- ☑ Acquired through the Content Hub
- ☑ Advanced… support
- ☒ Additiona… resources

VS

Codeless Connector Framework

- ☑ Acquired through the Content Hub
- ☒ Limited Rest-API support
- ☑ No additional Azure resources required

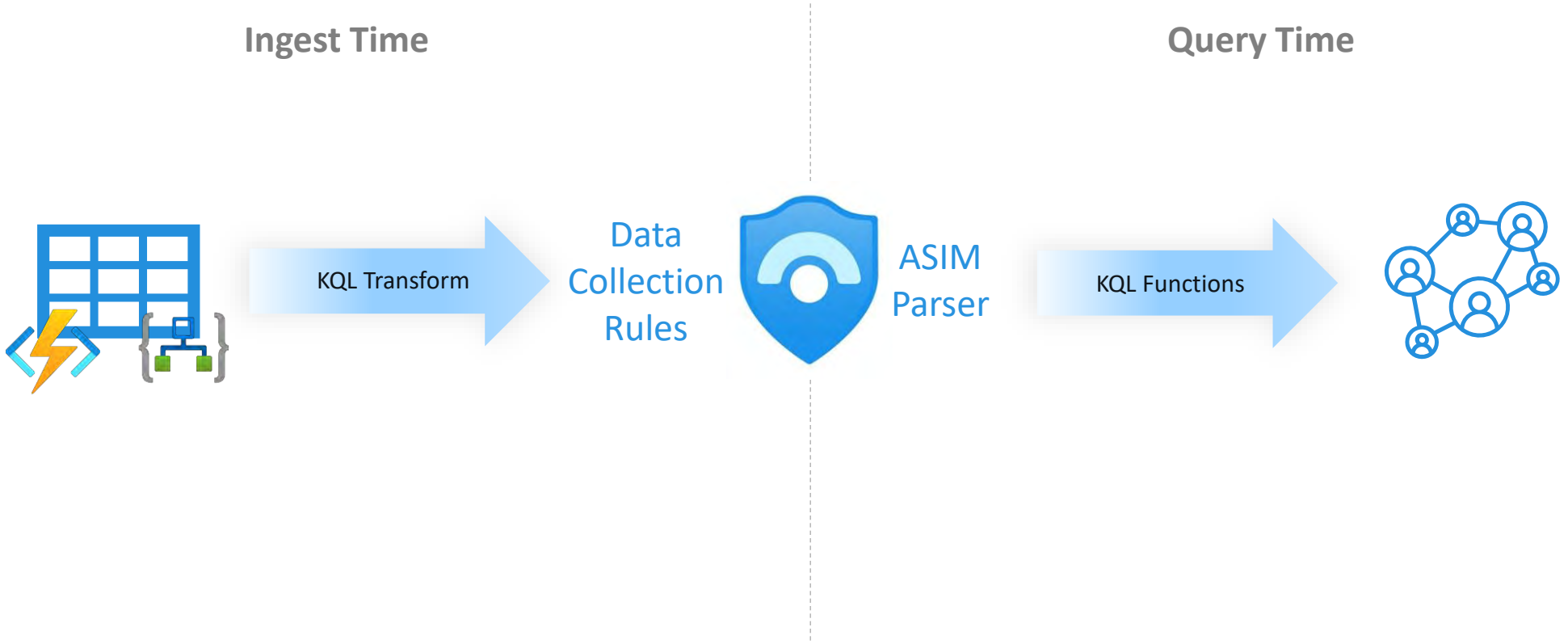
Data Connector ingests the raw Json response from a REST API

HTTP Data Collector API

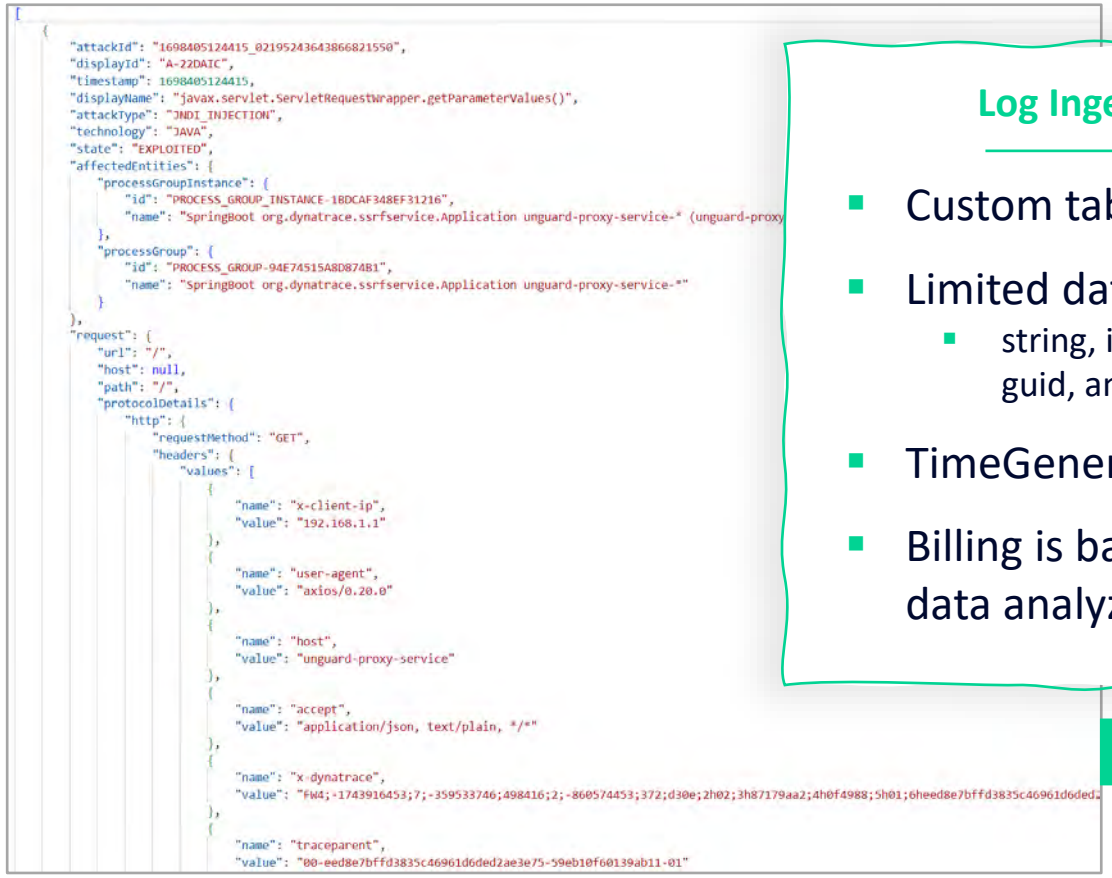
- Table schema was automagically defined on ingest
- Fields were suffixed with type, i.e. “_s” for string and tables with “_CL”

TimeGenerated [UTC]	attackId_s
03/12/2025, 14:36:28.810	1764772304333_169
TenantId	
SourceSystem	
TimeGenerated [UTC]	
attackId_s	
displayId_s	
timestamp_d	
displayName_s	
attackType_s	
technology_s	
state_s	
request_url_s	
request_path_s	
request_protocolDetails_http_requestMethod_s	

Data transformation and Advanced Security Information Model (ASIM)

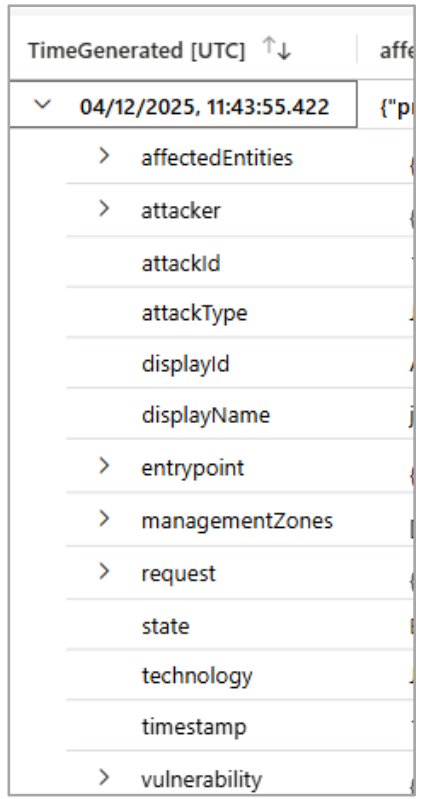


Data Connector ingests the raw Json response from a REST API



Log Ingestion API(with DCR)

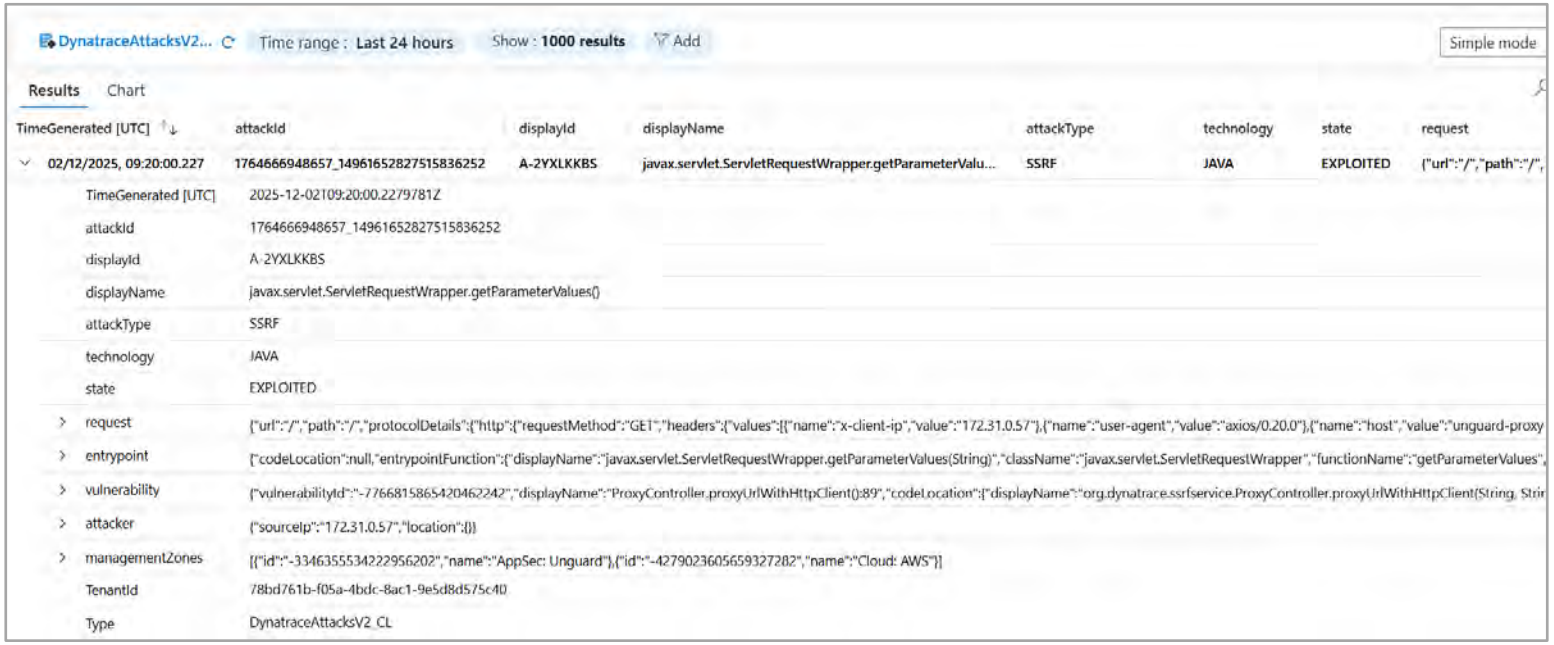
- Custom tables use a suffix of **_CL**
- Limited data types
  - string, int, long, real, boolean, dateTime, guid, and dynamic
- TimeGenerated field required
- Billing is based on the volume of data analyzed and storage



Data Collection Rules allow us to define the ingestion pipeline upfront

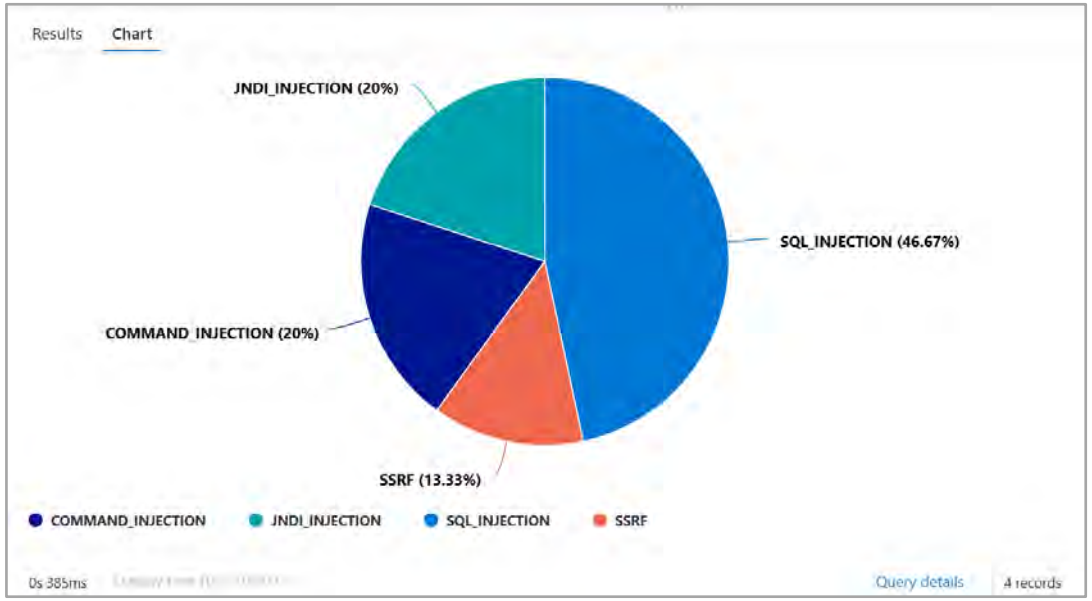
```
"dataFlows": [{
"streams": ["Custom-DynatraceAttacksV2"],
"destinations": ["clv2ws1"],
"transformKql": "let fromUnixTime = (t: long) {\ndatetime(1970-01-01) + t *
1ms\n};\nsource | extend TimeGenerated = fromUnixTime(timestamp) | project-
away timestamp",
"outputStream": "Custom-DynatraceAttacksV2_CL"
}]
```

- Define the Table Schema
- Apply transformations i.e., filtering
- Send data to multiple destinations



KQL your language for turning security relevant telemetry into insights

```
DynatraceAttacksV2_CL
  | where state != 'ALLOWLISTED'
  | summarize  Count=count() by attackType
```



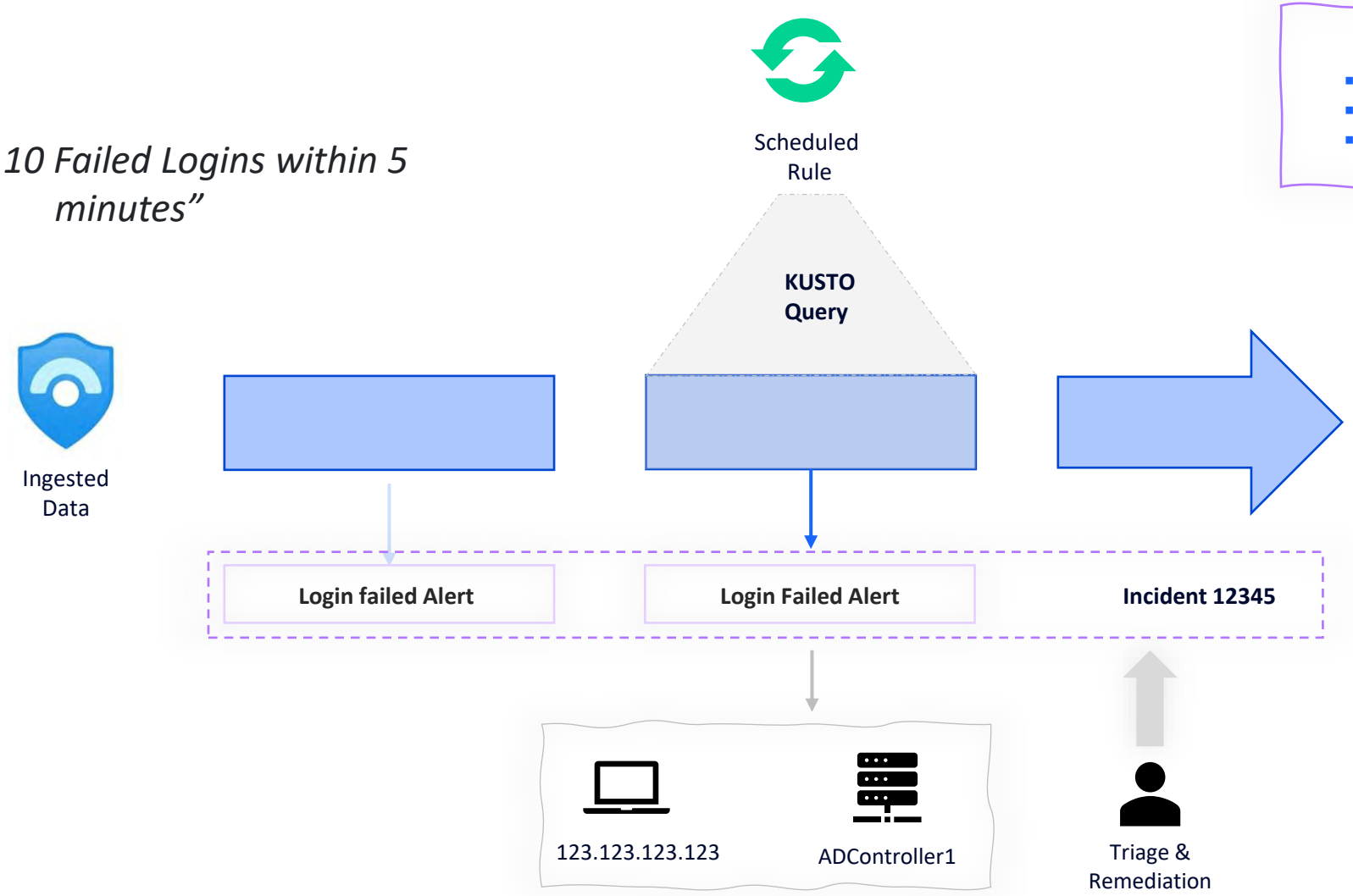

```
DynatraceAttacksV2_CL
  | where state != 'ALLOWLISTED'
  | summarize  Count=count() by tostring(attacker.sourceIp)
  | order by Count
  | limit 10
```

Results | Chart

attacker_sourceIp	Count
172.31.0.57	3
184.195.3.131	3
19.21.221.83	2
182.7.180.66	2
101.58.202.167	2
66.96.37.30	1
113.167.100.35	1
35.183.42.70	1
172.175.183.17	1
48.130.188.78	1

Reduce human error & increase accuracy by automating threat detection

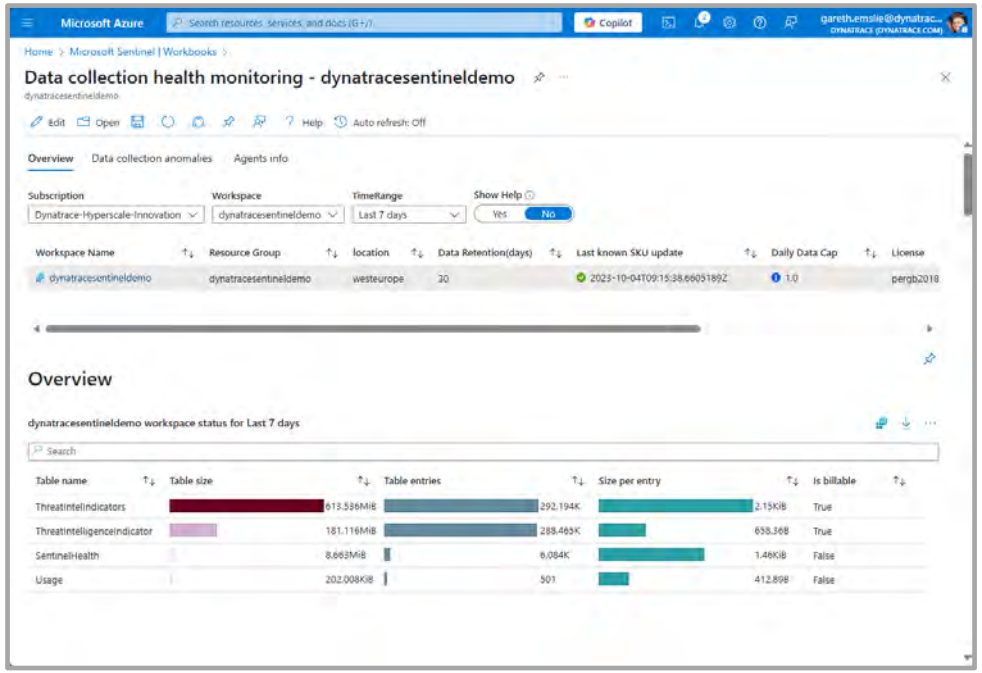
"Alert on 10 Failed Logins within 5 minutes"



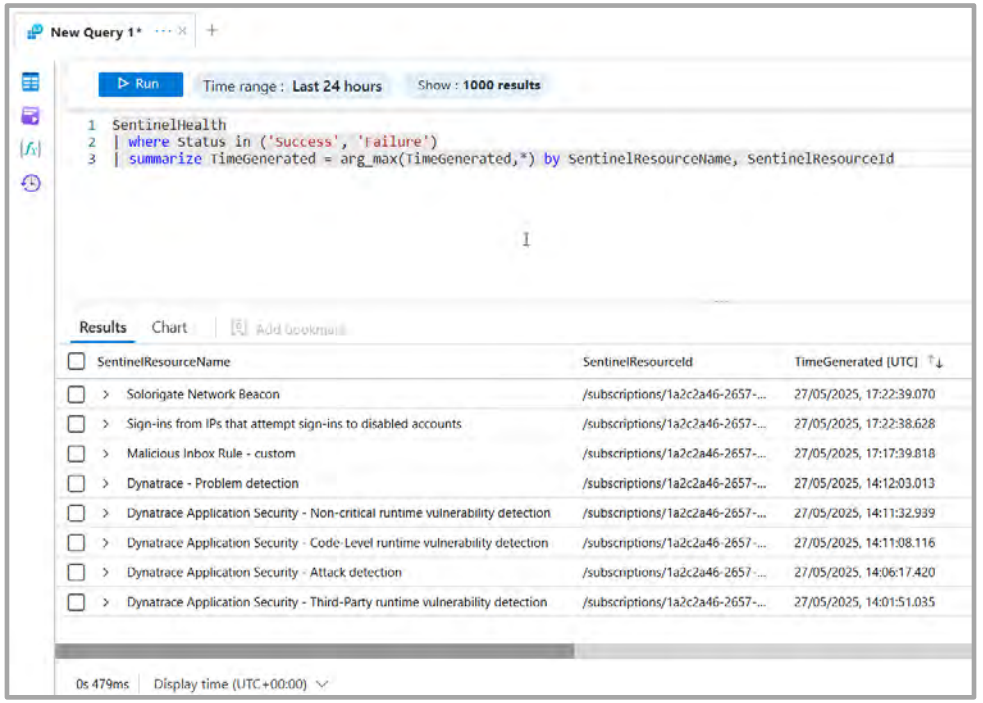
Other Rule Types

- Near-Real-time (NRT) Rules
- Anomaly Rules
- Microsoft Security Rules

Monitoring the Health of your sentinel ingestion



Data collection health monitoring workbook



SentinelHealth data table

DEMO

Microsoft Sentinel Integration

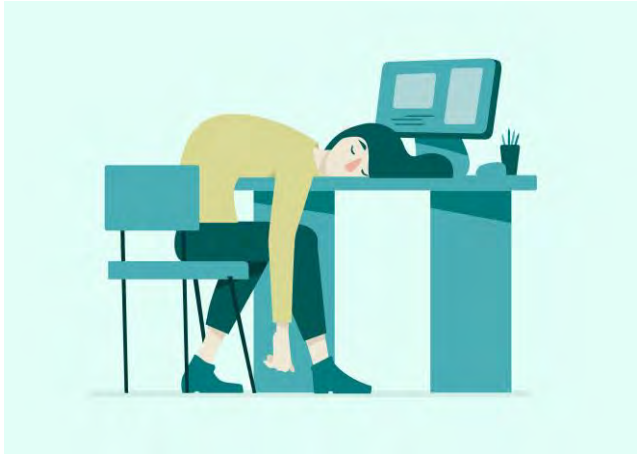
Building your first connector

How are connectors, analytics rules built (http://bit.ly/4dJcGpE)

Limit threat impact by triggering immediate response on threat detection

Manual Triage & Remediation

- Slow & error prone
- 24x7 availability
- Expensive



- Continuous evaluation
- Immediate response
- Low cost

Automated Triage and Remediation

dynatrace

CLOUD DONE RIGHT

Gareth Emslie
Product Manager &
Tech Evangelist