

# From Zero to a DevSecOps Hero: Extending Microsoft Sentinel

---



Gareth Emslie  
Product Manager &  
Tech Evangelist

# Disclaimer

---

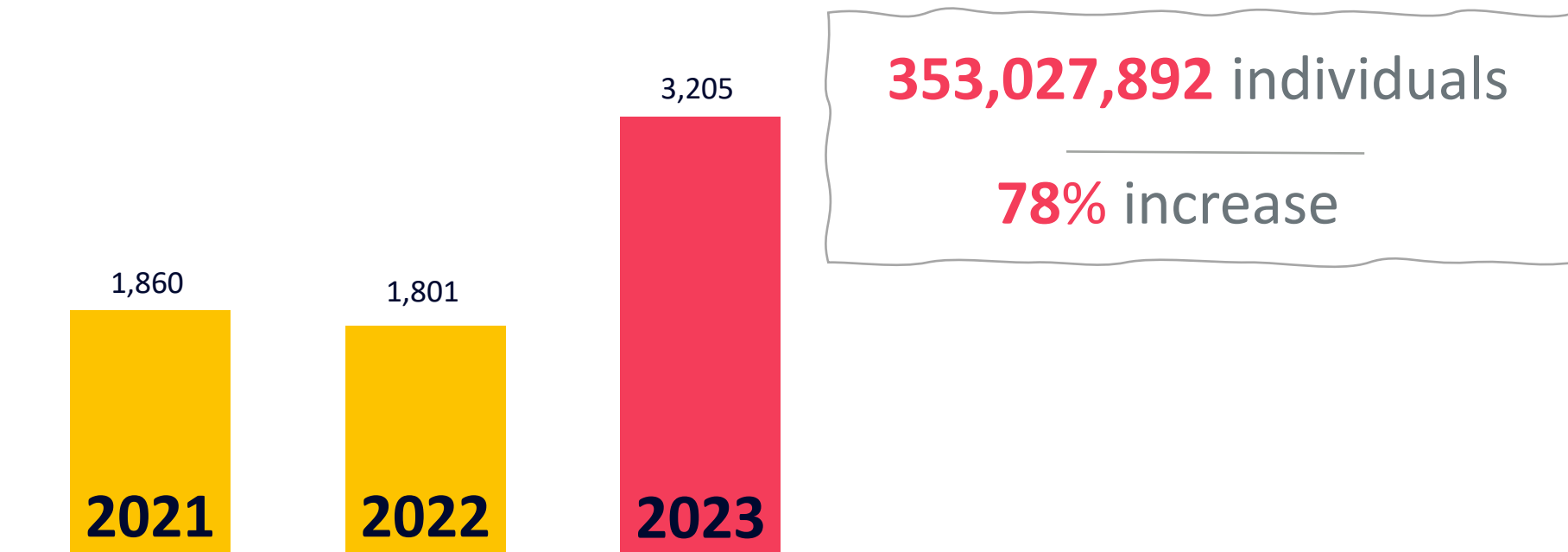
- The information presented in this session is based on my personal experience and opinions and not those of my employer
- Mention of any specific product or service does not imply endorsement
- I don't claim to be an expert in **\*all | any\*** the areas we will talk about today 😊

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


**The  
Economist**

6<sup>th</sup> May 2017

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



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



**74%** of all breaches included a human element

# Today's operations teams are not only challenged by attackers

---



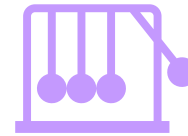
**Complexity**



**Volume**

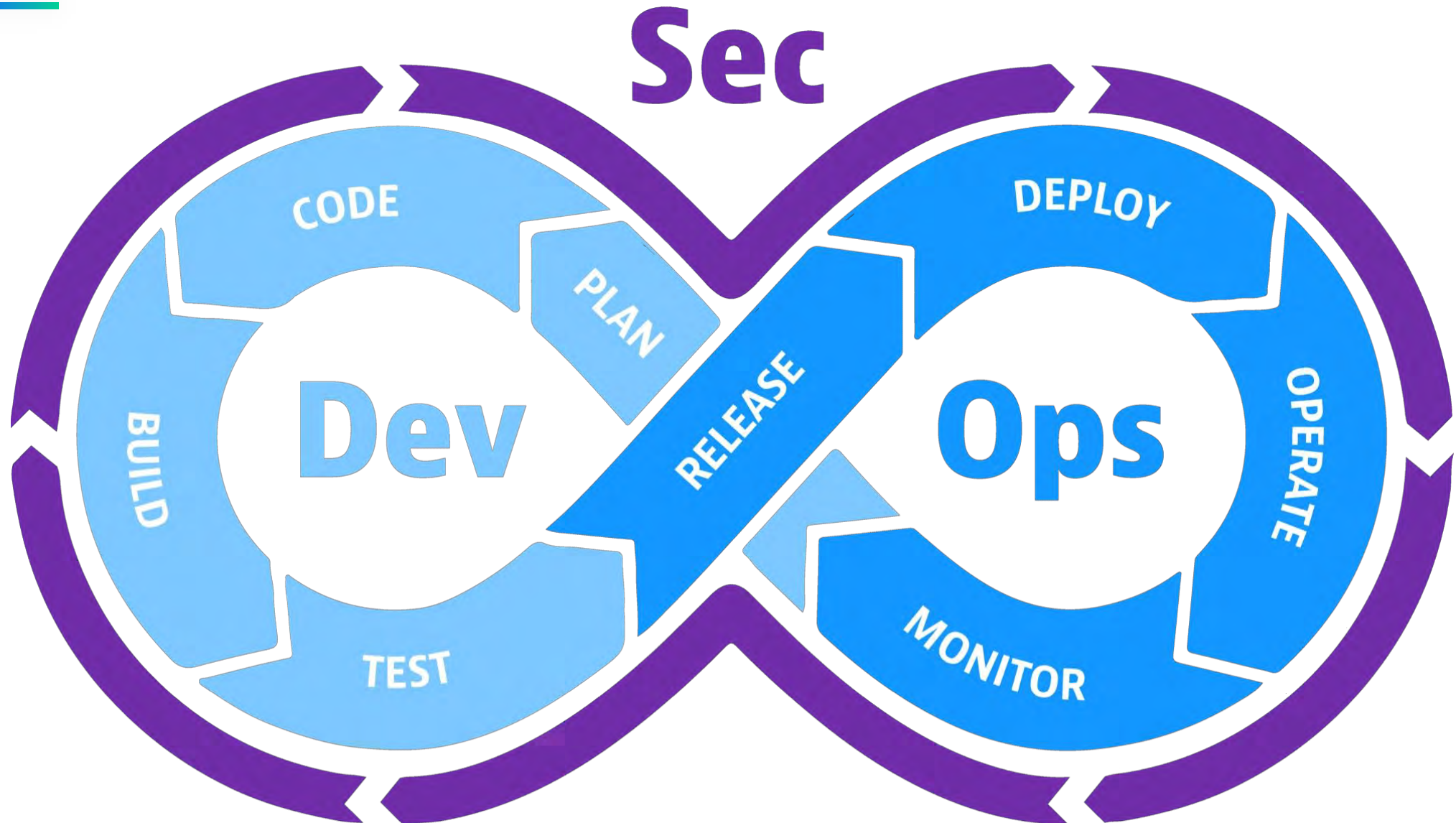


**Cost**

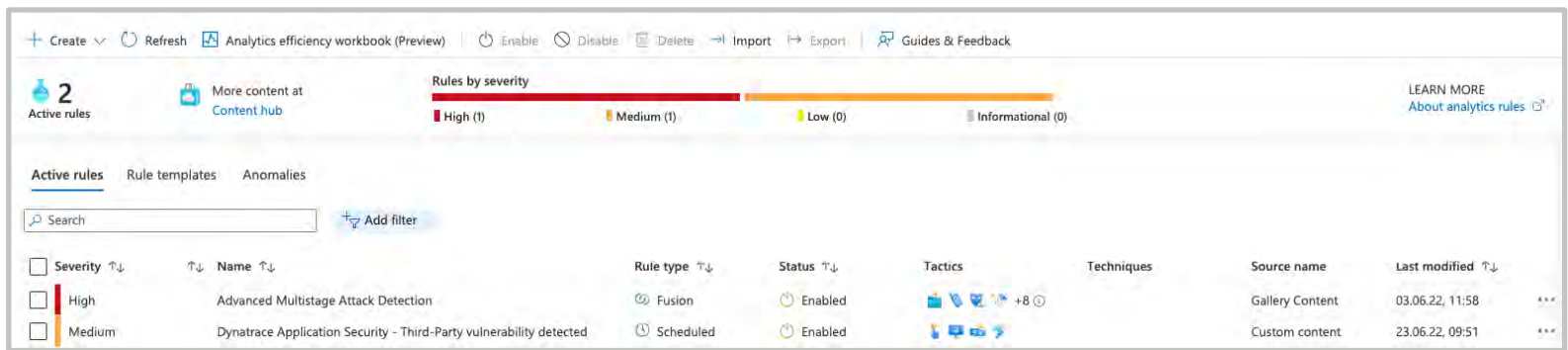


**Correlation**

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

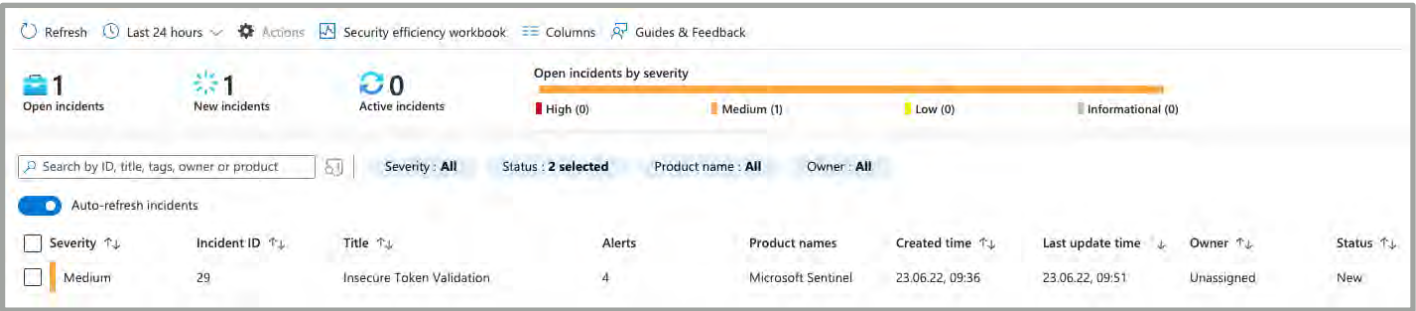


# Sentinel enables SOC teams to perform threat hunting, leverage SOAR capabilities for incident lifecycle; Remediation tasks can also be defined within external systems



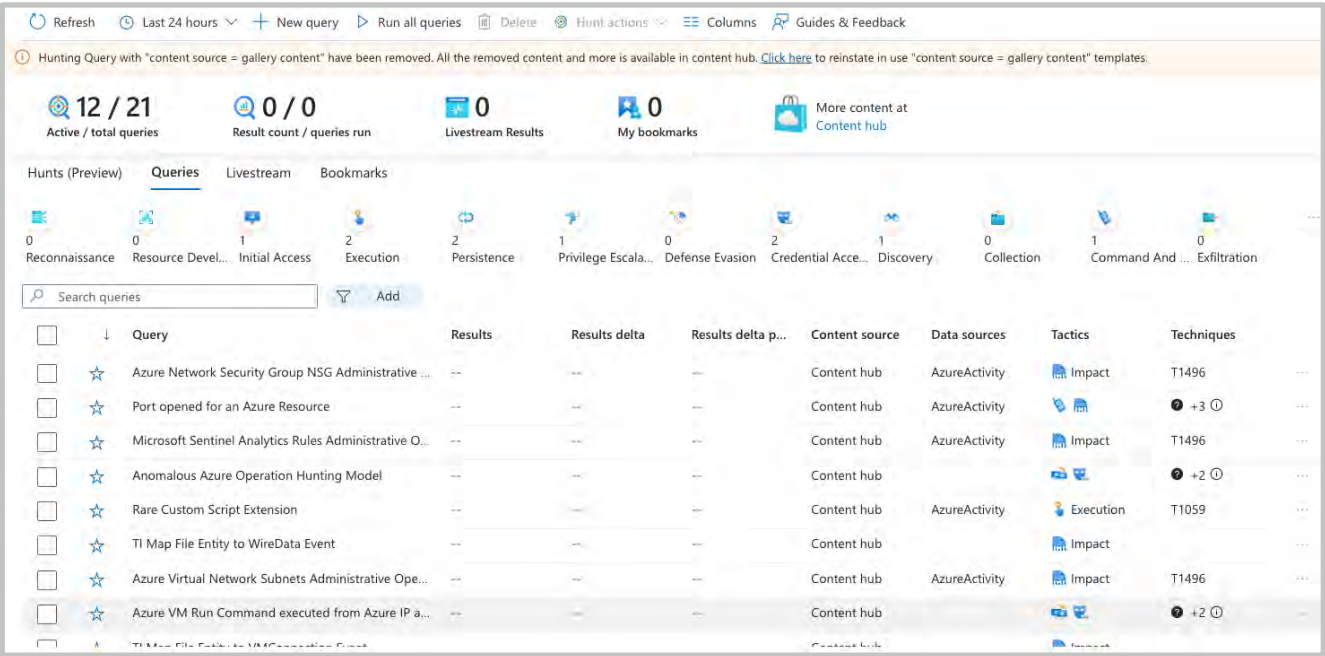
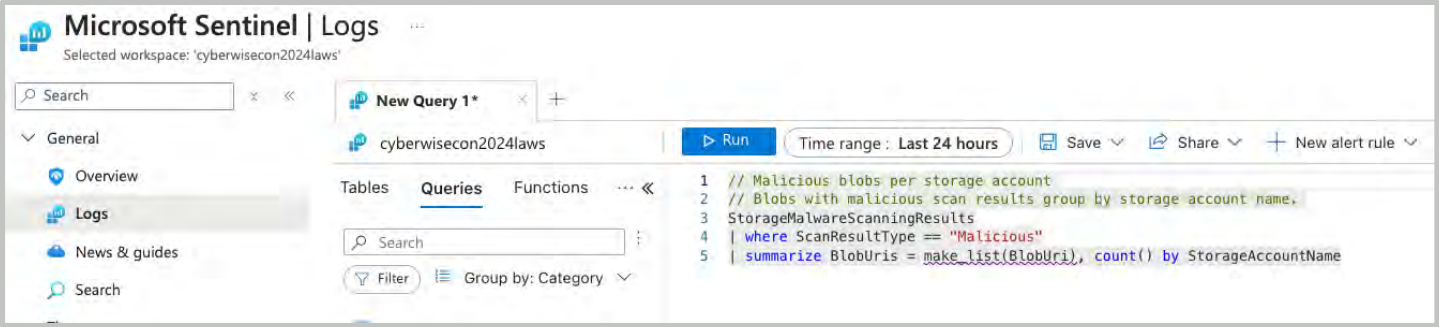
- Define complex analytics rules
- Trigger automated Incident creation

- Manage Incidents centrally
- Trigger remediation tasks



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

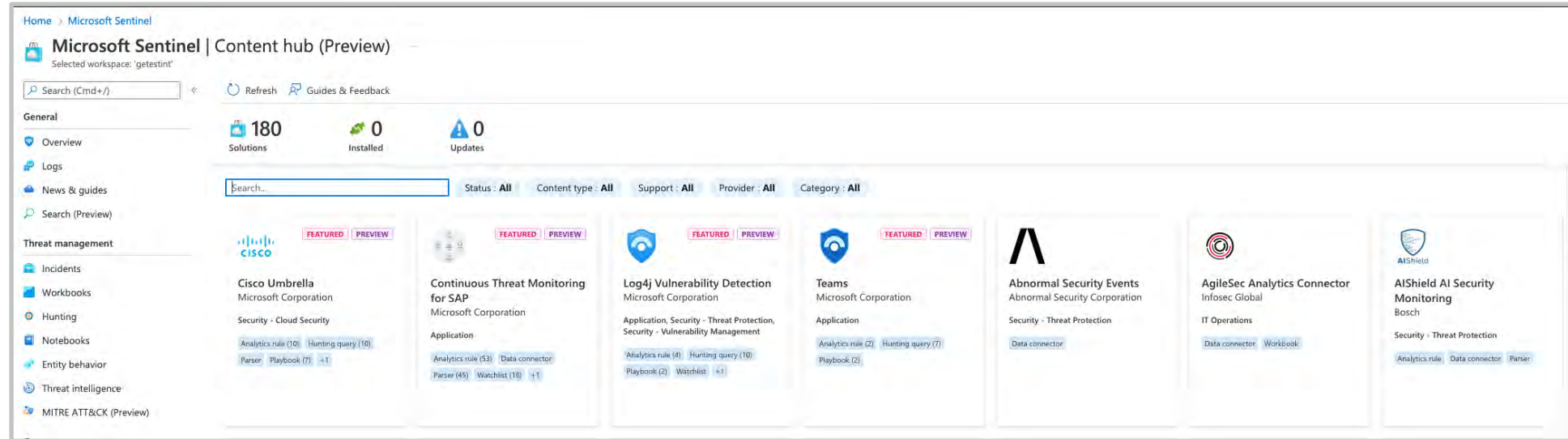
Search and query tools in Microsoft Sentinel to hunt for security threats and tactics throughout your environment



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

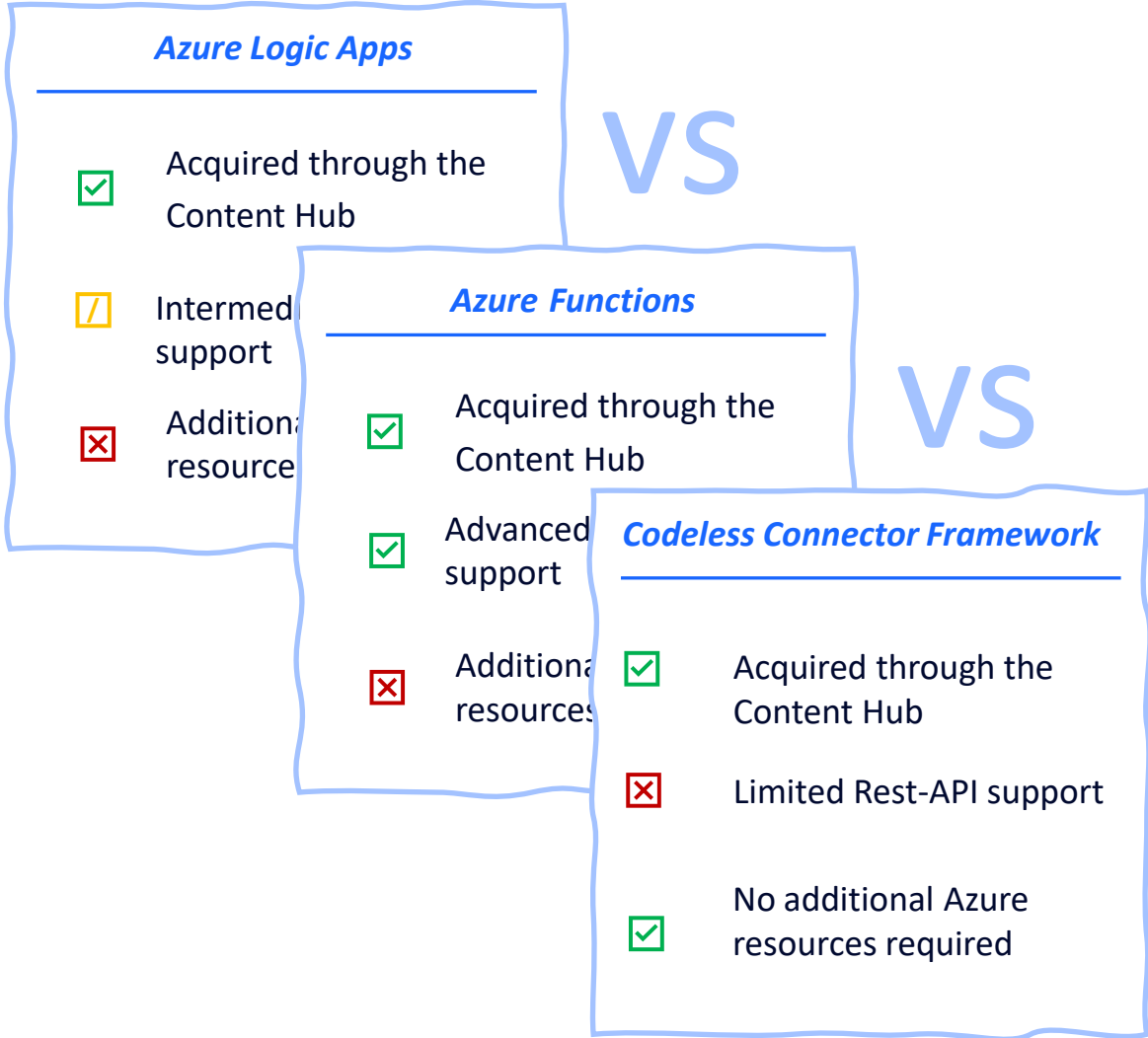


## Dynatrace's Runtime Application Protection

- 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



# Data Connector ingests the raw Json response from a REST API

```
[
  {
    "attackId": "1698405124415_02195243643866821550",
    "displayId": "A-22DAIC",
    "timestamp": 1698405124415,
    "displayName": "javax.servlet.ServletRequestWrapper.getParameterValues()",
    "attackType": "JNDI_INJECTION",
    "technology": "JAVA",
    "state": "EXPLOITED",
    "affectedEntities": {
      "processGroupInstance": {
        "id": "PROCESS_GROUP_INSTANCE-18DCAF348EF31216",
        "name": "SpringBoot org.dynatrace.ssrfservice.Application uguard-proxy-service-* (unguard-)",
      },
      "processGroup": {
        "id": "PROCESS_GROUP-94E74515A8D874B1",
        "name": "SpringBoot org.dynatrace.ssrfservice.Application uguard-proxy-service-*",
      }
    },
    "request": {
      "url": "/",
      "host": null,
      "path": "/",
      "protocolDetails": {
        "http": {
          "requestMethod": "GET",
          "headers": {
            "values": [
              {
                "name": "x-client-ip",
                "value": "192.168.1.1"
              },
              {
                "name": "user-agent",
                "value": "axios/0.20.0"
              },
              {
                "name": "host",
                "value": "unguard-proxy-service"
              },
              {
                "name": "accept",
                "value": "application/json, text/plain, */*"
              },
              {
                "name": "x-dynatrace",
                "value": "Fw4;-1743916453;7;-359533746;498416;2;-860574453;372;d30e;2h02;3h87179aa2;4h0f4988;5h01;0heed8e7bffdd3835c46961d0ded2ae3e75-59eb10f60139ab11-01"
              },
              {
                "name": "traceparent",
                "value": "00-eed8e7bffdd3835c46961d0ded2ae3e75-59eb10f60139ab11-01"
              }
            ]
          }
        }
      }
    }
  }
]
```

HTTP Data Collector API

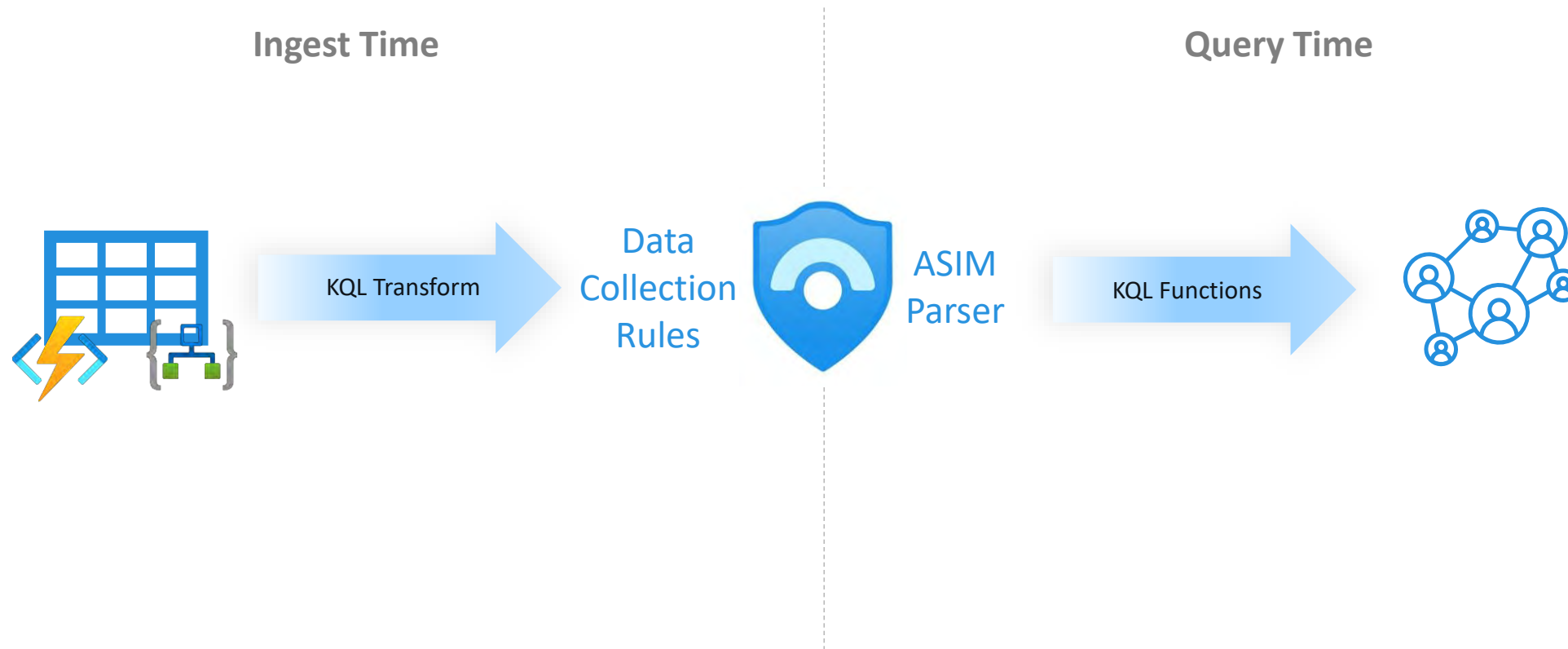
- Table schema was automagically defined on ingest
- Fields were suffixed with type, i.e. “\_s” for string and tables with “\_CL”



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

TimeGenerated [UTC] ↑↓	affectedEntities
04/12/2025, 11:43:55.422	{ "p
> affectedEntities	
> attacker	
attackId	
attackType	
displayId	
displayName	
> endpoint	
> managementZones	
> request	
state	
technology	
timestamp	
> vulnerability	

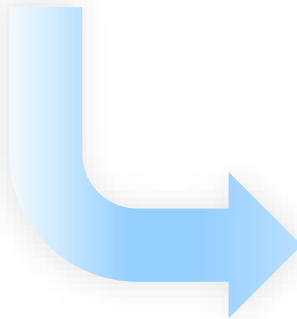




## Data Collection Rules allow us to define the ingestion pipeline upfront

```
"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



DynatraceAttacksV2...

Time range : Last 24 hours

Show : 1000 results

Add

Simple mode

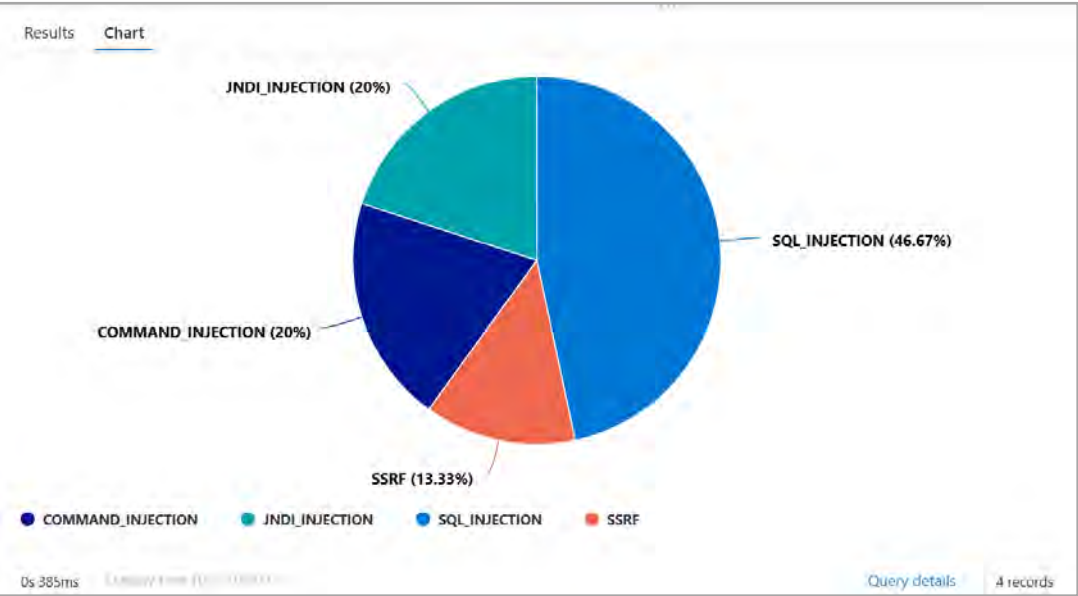
Results

Chart

TimeGenerated [UTC]	attackId	displayId	displayName	attackType	technology	state	request
02/12/2025, 09:20:00.227	1764666948657_14961652827515836252	A-2YXLKKB5	javax.servlet.ServletRequestWrapper.getParameterValu...	SSRF	JAVA	EXPLOITED	{\"url\":\"/\", \"path\":\"/\",
TimeGenerated [UTC]	2025-12-02T09:20:00.2279781Z						
attackId	1764666948657_14961652827515836252						
displayId	A-2YXLKKB5						
displayName	javax.servlet.ServletRequestWrapper.getParameterValues()						
attackType	SSRF						
technology	JAVA						
state	EXPLOITED						
> request	{\"url\":\"/\", \"path\":\"/\", \"protocolDetails\":{\"http\":{\"requestMethod\":\"GET\", \"headers\":{\"values\":{\"name\":\"x-client-ip\", \"value\":\"172.31.0.57\"}, {\"name\":\"user-agent\", \"value\":\"axios/0.20.0\"}, {\"name\":\"host\", \"value\":\"unguard-proxy						
> endpoint	{\"codeLocation\":null, \"entrypointFunction\":{\"displayName\":\"javax.servlet.ServletRequestWrapper.getParameterValues(String)\", \"className\":\"javax.servlet.ServletRequestWrapper\", \"functionName\":\"getParameterValues\",						
> vulnerability	{\"vulnerabilityId\":\"-7766815865420462242\", \"displayName\":\"ProxyController.proxyUrlWithHttpClient():89\", \"codeLocation\":{\"displayName\":\"org.dynatrace.ssrfservice.ProxyController.proxyUrlWithHttpClient(String, Stor						
> attacker	{\"sourceIp\":\"172.31.0.57\", \"location\":{\"}}						
> managementZones	{\"id\":\"-3346355534222956202\", \"name\":\"AppSec: Unguard\"}, {\"id\":\"-4279023605659327282\", \"name\":\"Cloud: AWS\"}]						
TenantId	78bd761b-f05a-4bdc-8ac1-9e5d8d575c40						
Type	DynatraceAttacksV2_CL						

# KQL your language for turning security relevant telemetry into insights

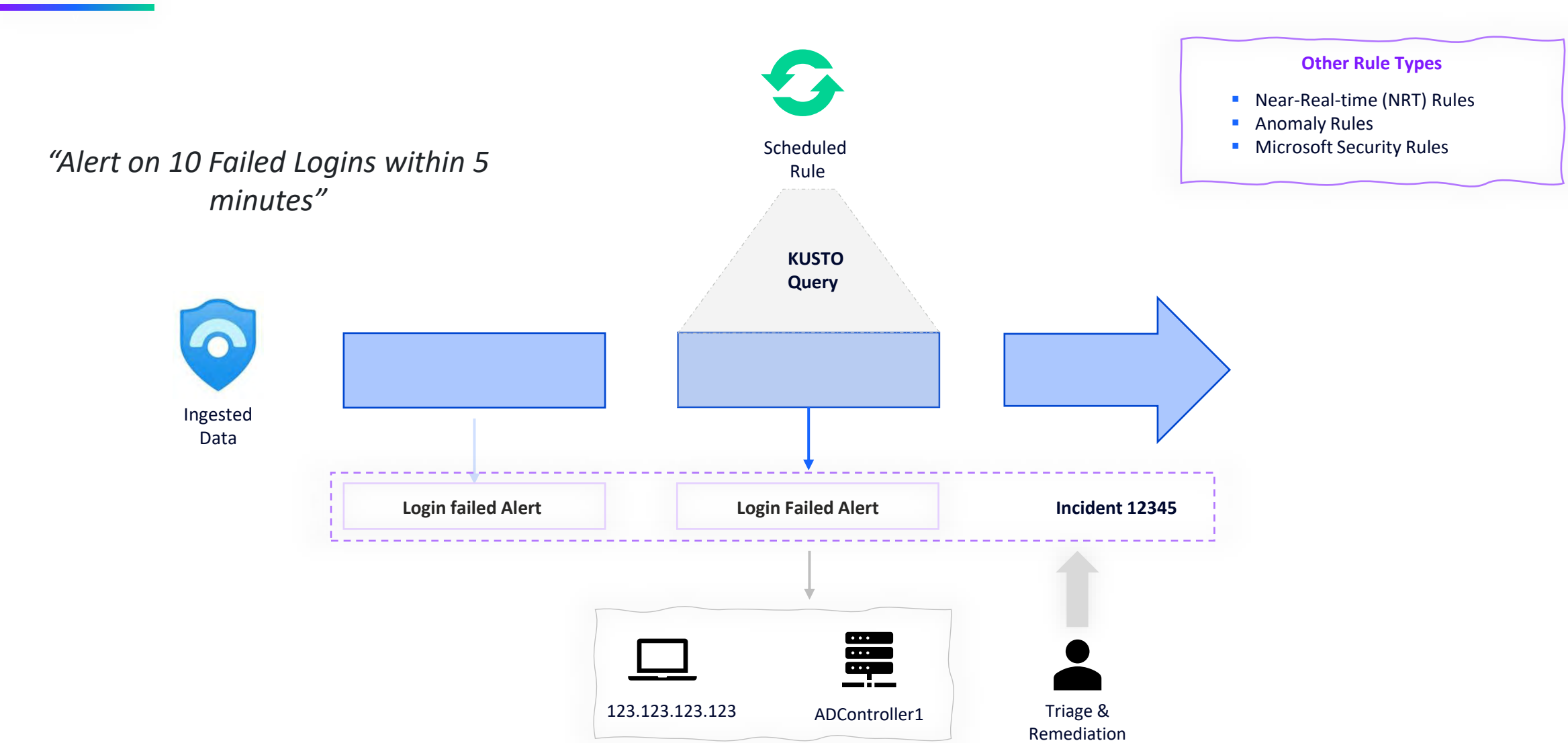
```
DynatraceAttacksV2_CL
| where state != 'ALLOWLISTED'
| summarize Count=count() by attackType
```



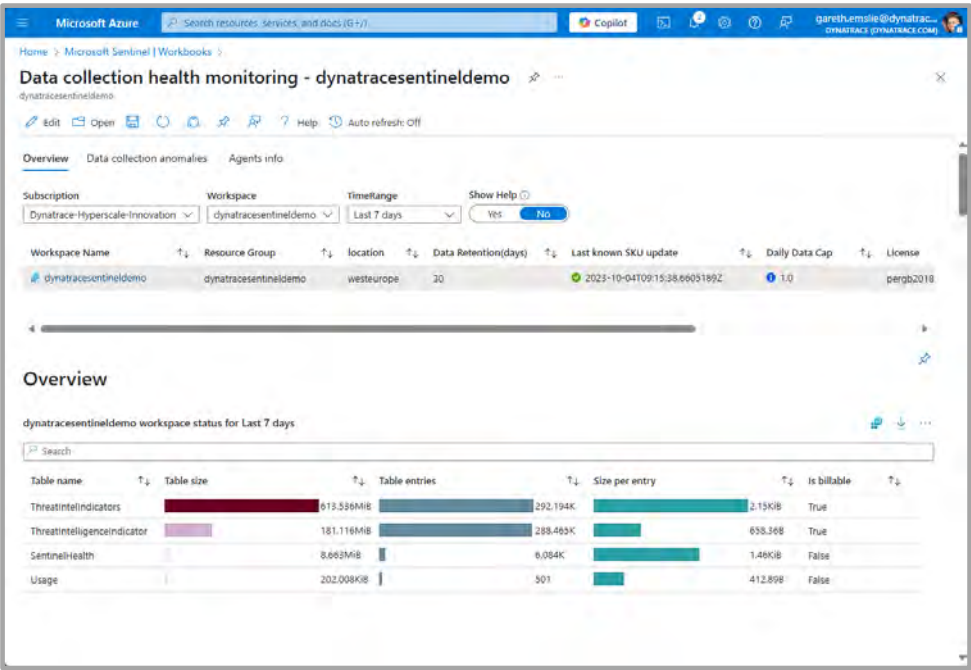
```
DynatraceAttacksV2_CL
| where state != 'ALLOWLISTED'
| summarize Count=count() by toString(attacker.sourceIp)
| order by Count
| limit 10
```

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

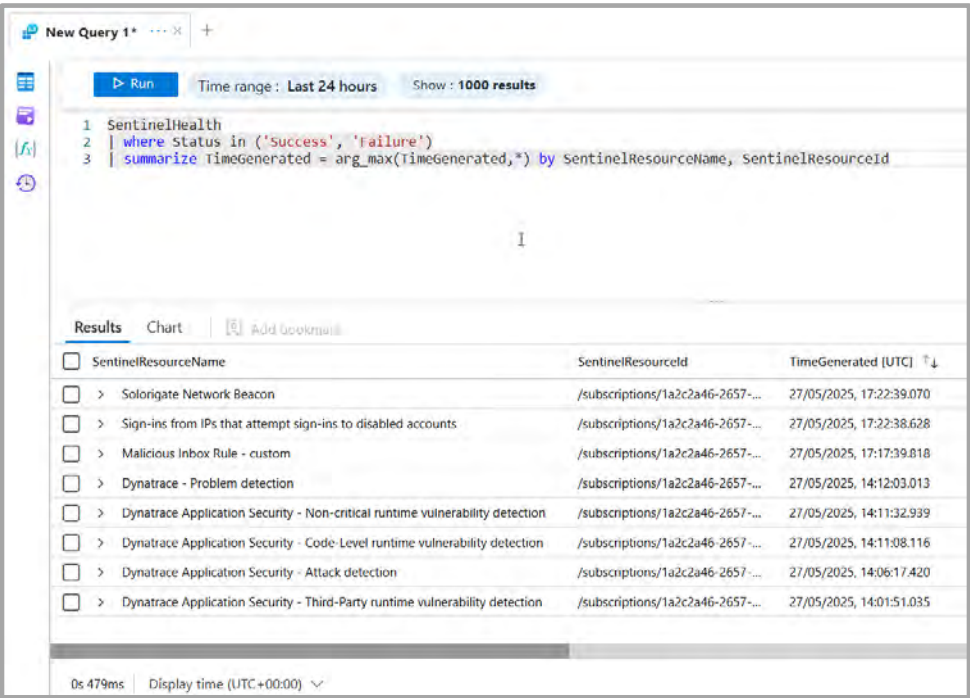
# Reduce human error & increase accuracy by automating threat detection



# 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



Gareth Emslie  
Product Manager &  
Tech Evangelist