

From Zero to a DevSecOps Hero: Extending Microsoft Sentinel



Gareth Emslie
Product Manager &
Tech Evangelist



Disclaimer

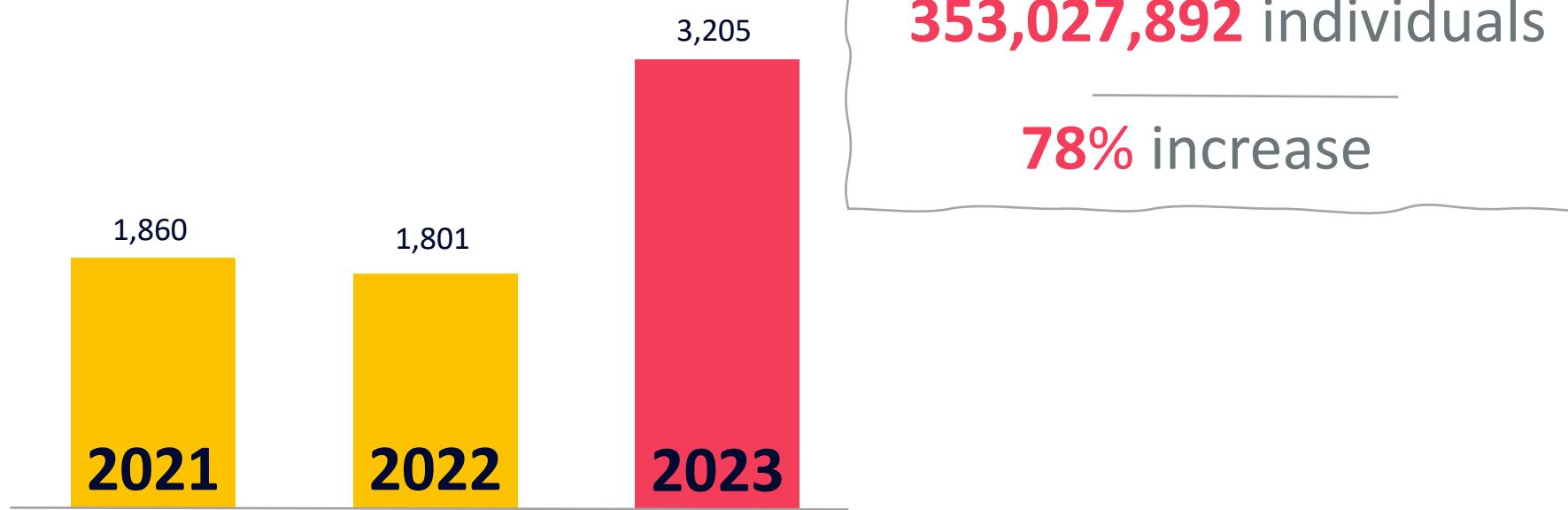
- The information presented in this session is based on my personal experience and opinions and not those of my employer
- Mention of any specific product or service does not imply endorsement
- I don't claim to be an expert in ***all | any*** the areas we will talk about today 😊

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

The
Economist

6th 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

18.5%

Social engineering

10.4%

Ransomware

4.9%

Malware

4.6%

Zero-Day

74% of all breaches included a
human element

Today's operations teams are not only challenged by attackers



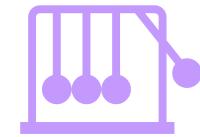
Complexity



Volume

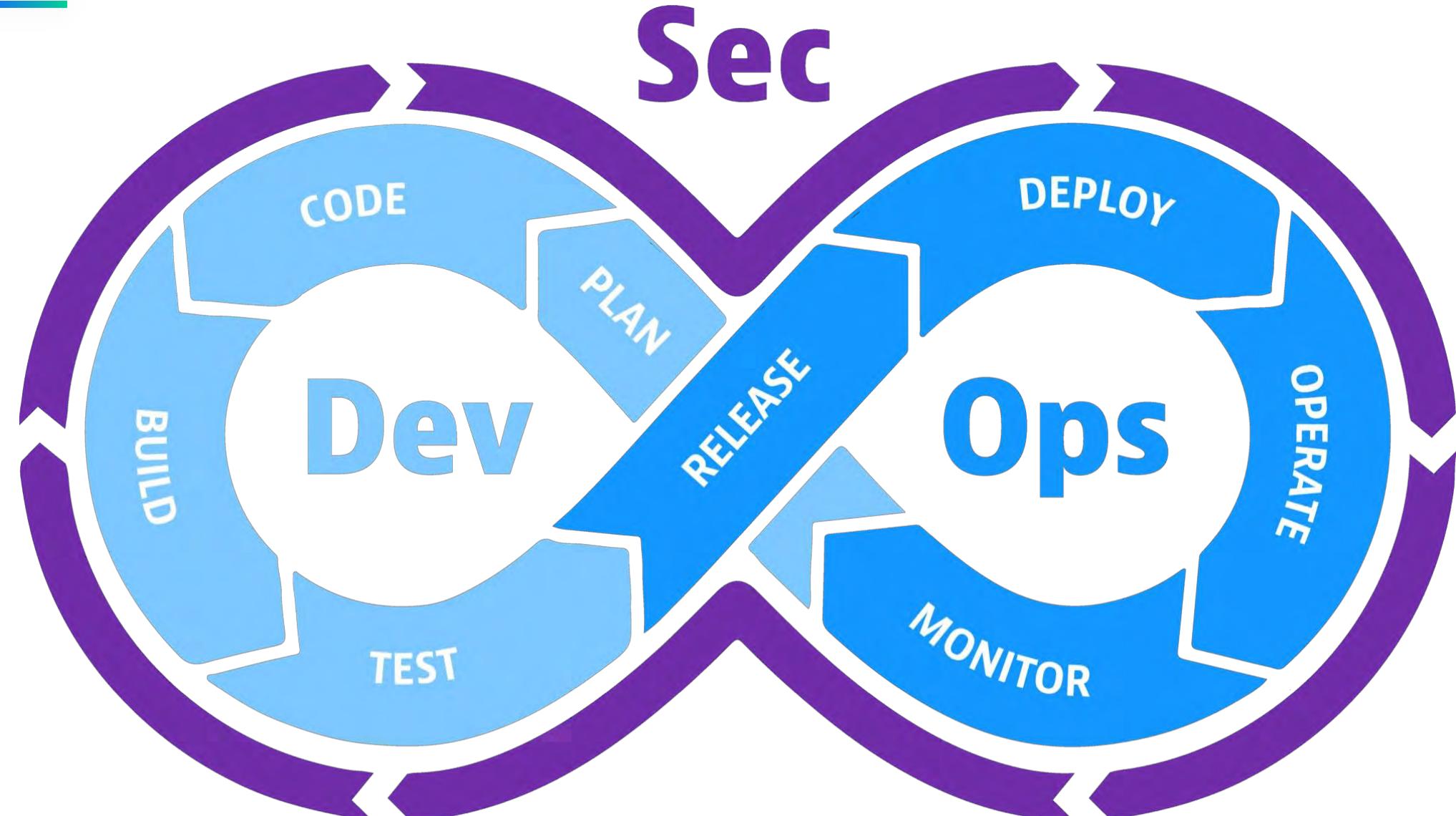


Cost



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

The screenshot shows the Microsoft Sentinel Analytics efficiency workbook interface. At the top, there are buttons for Create, Refresh, Enable, Disable, Delete, Import, Export, and Guides & Feedback. Below this is a header with '2 Active rules' and a 'Rules by severity' bar showing 1 High, 1 Medium, and 0 Low and Informational rules. The main area displays two active rules:

Severity	Name	Rule type	Status	Tactics	Techniques	Source name	Last modified
High	Advanced Multistage Attack Detection	Fusion	Enabled	+8		Gallery Content	03.06.22, 11:58
Medium	Dynatrace Application Security - Third-Party vulnerability detected	Scheduled	Enabled			Custom content	23.06.22, 09:51

- Define complex analytics rules
- Trigger automated Incident creation

The screenshot shows the Microsoft Sentinel Security efficiency workbook interface. At the top, there are buttons for Refresh, Last 24 hours, Actions, Security efficiency workbook, Columns, and Guides & Feedback. Below this is a header with counts for Open incidents (1), New incidents (1), and Active incidents (0). A 'Open incidents by severity' bar shows 0 High, 1 Medium, 0 Low, and 0 Informational incidents. The main area displays one open incident:

Severity	Incident ID	Title	Alerts	Product names	Created time	Last update time	Owner	Status
Medium	29	Insecure Token Validation	4	Microsoft Sentinel	23.06.22, 09:36	23.06.22, 09:51	Unassigned	New

- 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

The screenshot shows the Microsoft Sentinel Logs interface. On the left, there's a navigation sidebar with 'General' (Overview, Logs, News & guides, Search), 'Tables' (selected), 'Queries' (selected), and 'Functions'. A search bar at the top has 'cyberwisecon2024laws' typed into it. Below the search bar are 'Run' and 'Time range: Last 24 hours' buttons. The main area displays a query editor with the following code:

```
1 // Malicious blobs per storage account
2 // Blobs with malicious scan results group by storage account name,
3 StorageMalwareScanningResults
4 | where ScanResultType == "Malicious"
5 | summarize BlobUris = make_list(BlobUri), count() by StorageAccountName
```

The screenshot shows the Microsoft Sentinel Queries interface. At the top, there are summary statistics: 12 / 21 Active / total queries, 0 / 0 Result count / queries run, 0 Livestream Results, 0 My bookmarks, and a 'More content at Content hub' button. Below this is a navigation bar with 'Hunts (Preview)', 'Queries' (selected), 'Livestream', and 'Bookmarks'. A 'Search queries' input field and an 'Add' button are also present. The main area is a table listing hunting queries:

	Query	Results	Results delta	Results delta p...	Content source	Data sources	Tactics	Techniques
1	Azure Network Security Group NSG Administrative ...	--	--	--	Content hub	AzureActivity	Impact	T1496
2	Port opened for an Azure Resource	--	--	--	Content hub	AzureActivity	Impact	+3 ⓘ
3	Microsoft Sentinel Analytics Rules Adminstrative O...	--	--	--	Content hub	AzureActivity	Impact	T1496
4	Anomalous Azure Operation Hunting Model	--	--	--	Content hub	AzureActivity	Impact	+2 ⓘ
5	Rare Custom Script Extension	--	--	--	Content hub	AzureActivity	Execution	T1059
6	T1 Map File Entity to WireData Event	--	--	--	Content hub	AzureActivity	Impact	
7	Azure Virtual Network Subnets Adminstrative Ope...	--	--	--	Content hub	AzureActivity	Impact	T1496
8	Azure VM Run Command executed from Azure IP a...	--	--	--	Content hub	AzureActivity	Impact	+2 ⓘ

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

The screenshot shows the Microsoft Sentinel Content hub (Preview) interface. At the top, there are statistics: 180 Solutions, 0 Installed, and 0 Updates. Below this is a search bar and filter options for Status (All), Content type (All), Support (All), Provider (All), and Category (All). The main area displays a grid of connectors:

- Cisco Umbrella** (Microsoft Corporation): Security - Cloud Security. Features: Analytics rule (10), Hunting query (10), Parser (1), Playbook (7).
- Continuous Threat Monitoring for SAP** (Microsoft Corporation): Application. Features: Analytics rule (53), Data connector (1), Parser (45), Watchlist (15).
- Log4j Vulnerability Detection** (Microsoft Corporation): Application, Security - Threat Protection, Security - Vulnerability Management. Features: Analytics rule (4), Hunting query (10), Playbook (2), Watchlist (1).
- Teams** (Microsoft Corporation): Application. Features: Analytics rule (2), Hunting query (7), Playbook (2).
- Abnormal Security Events** (Abnormal Security Corporation): Security - Threat Protection. Features: Data connector (1).
- AgileSec Analytics Connector** (Infosec Global): IT Operations. Features: Data connector (1), Workbook (1).
- AIShield AI Security Monitoring** (Bosch): Security - Threat Protection. Features: Analytics rule (1), Data connector (1), Parser (1).

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

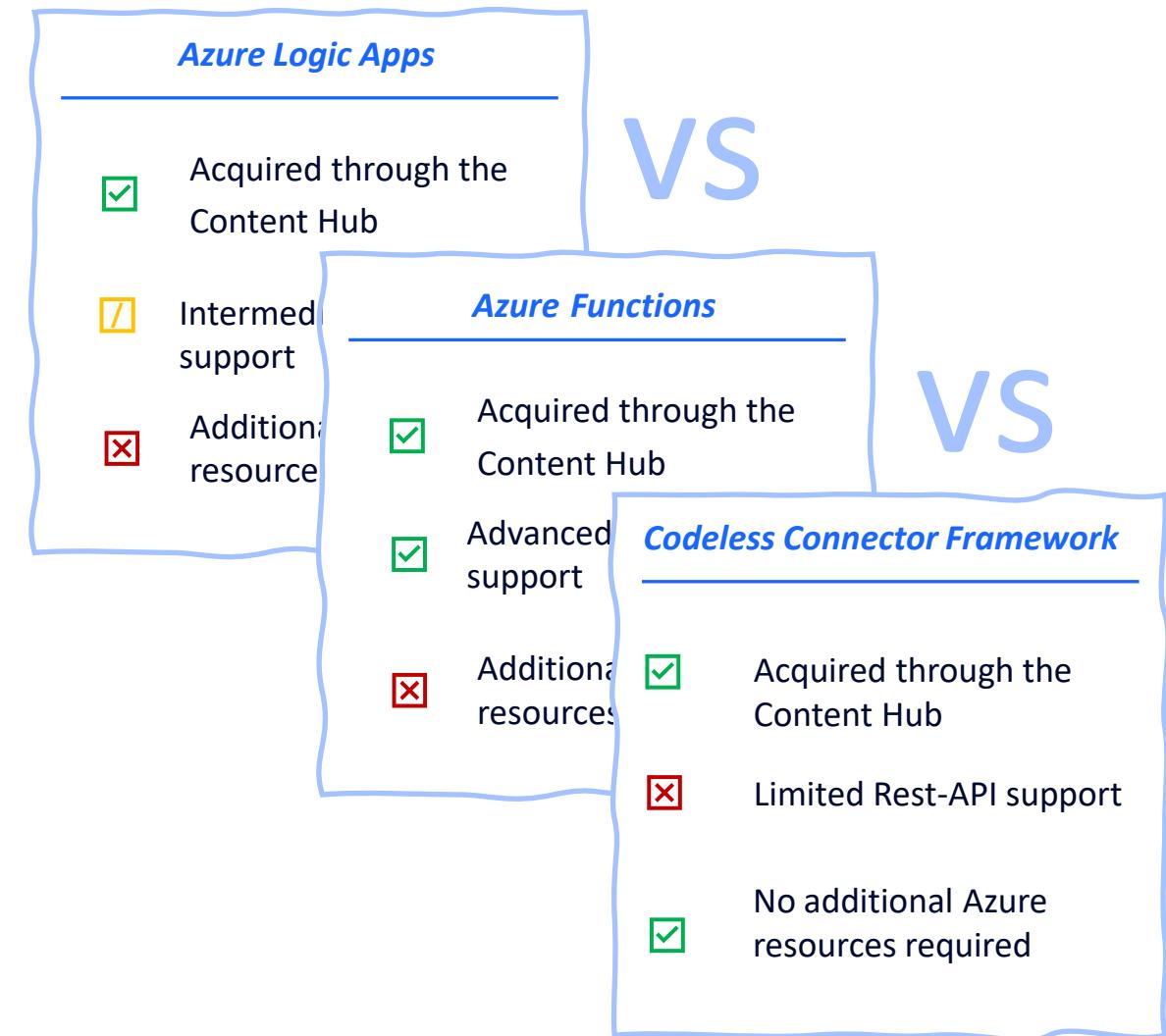
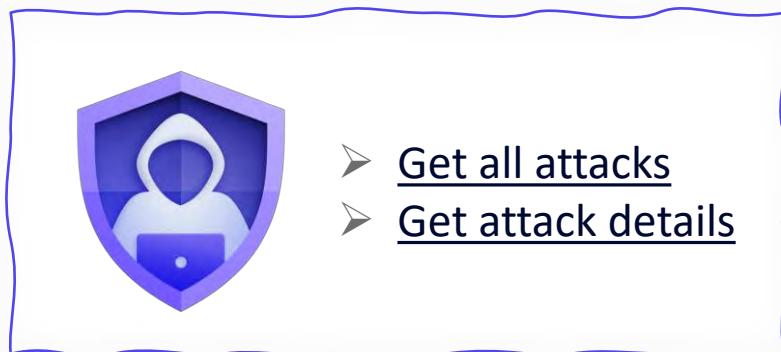


Choose a vendor who has important insights that we could add to our DevSecOps lifecycle



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



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": "ONI_INJECTION",  
  "technology": "JAVA",  
  "state": "EXPLOITED",  
  "affectedEntities": [  
    "processGroupInstance": [  
      {"id": "PROCESS_GROUP_INSTANCE_1BDCAF348EF31216",  
       "name": "Springboot org.dynatrace.ssrfservice.Application unguard-proxy-service-* (unguarded)"},  
    ],  
    "processGroup": [  
      {"id": "PROCESS_GROUP-94E74515A8D874B1",  
       "name": "Springboot org.dynatrace.ssrfservice.Application unguard-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;3h87379aa2;4h0f4988;5h01;6heed8e7bffd3835c46961d6dedd  
            },  
            {  
              "name": "traceparent",  
              "value": "00-eed8e7bffd3835c46961d6ded2ae3e75-59eb10f60139ab11-01"  
            }  
          ]  
        }  
      }  
    }  
  }  
}
```

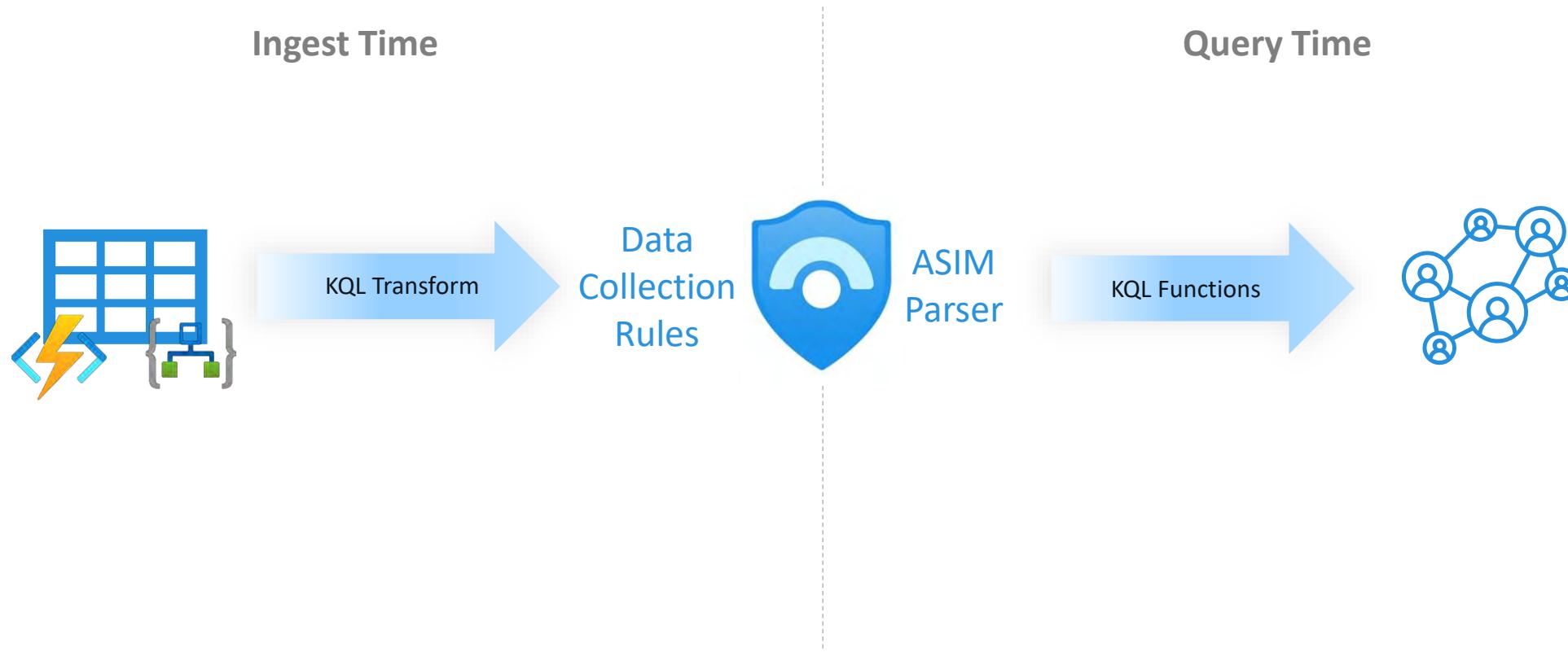
HTTP Data Collector API

- 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_16
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

```
{  
    "attackId": "1698405124415_02195243643866821550",  
    "displayId": "A-22DAIC",  
    "timestamp": 1698405124415,  
    "displayName": "javax.servlet.ServletRequestWrapper.getParameterValues()",  
    "attackType": "ONI_INJECTION",  
    "technology": "JAVA",  
    "state": "EXPLOITED",  
    "affectedEntities": {  
        "processGroupInstance": [  
            {"id": "PROCESS_GROUP_INSTANCE-1BDCAF348EF31216",  
            "name": "Springboot org.dynatrace.ssrfservice.Application unguard-proxy-service-* (unguard-proxy)"},  
            {"id": "PROCESS_GROUP-94E74515A8D874B1",  
            "name": "Springboot org.dynatrace.ssrfservice.Application unguard-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;bheed8e7bffd3835c46961d6ded"},  
                            {"name": "traceparent",  
                            "value": "00-eed8e7bffd3835c46961d6ded2ae3e75-59eb10f60139ab11-01"}  
                        ]  
                    }  
                }  
            }  
        }  
    }  
}
```

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] ↑↓	aff
04/12/2025, 11:43:55.422	{"p"}
>	affectedEntities
>	attacker
	attackId
	attackType
	displayId
	displayName
>	entrypoint
>	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"  
}]
```

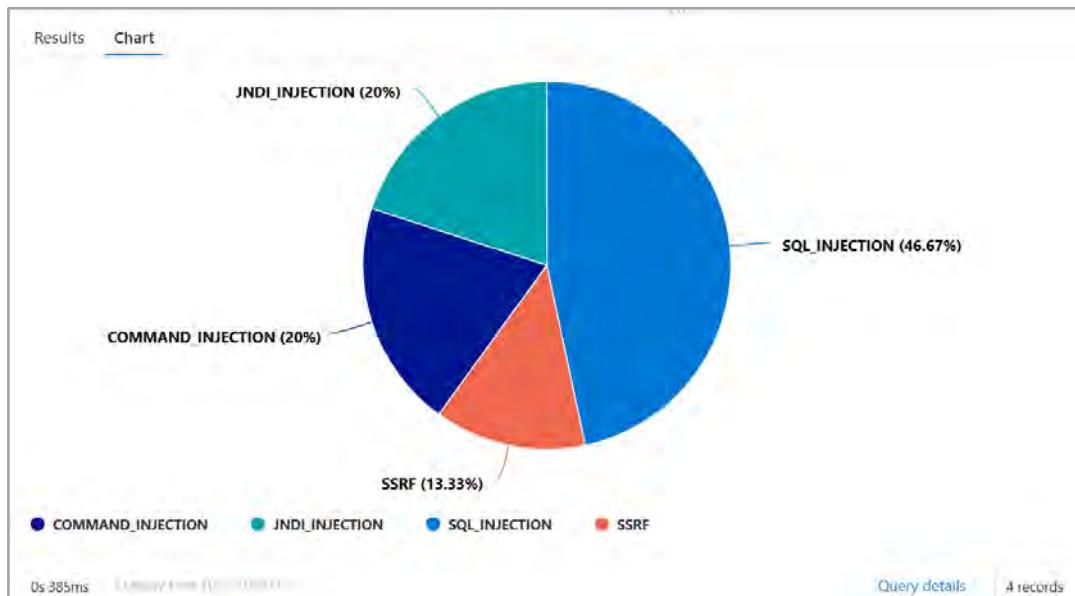
- Define the Table Schema
 - Apply transformations i.e., filtering
 - Send data to multiple destinations

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-2YXLKKBS	javax.servlet.ServletRequestWrapper.getParameterValue...	SSRF	JAVA	EXPLOITED	{"url":"/","path":"/",
TimeGenerated [UTC]	2025-12-02T09:20:00.2279781Z						
attackId	1764666948657_14961652827515836252						
displayId	A-2YXLKKBS						
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"}]}						
> entrypoint	{"codeLocation":null,"entrypointFunction":{"displayName":"javax.servlet.ServletRequestWrapper.getParameterValues(String)"}}						
> vulnerability	{"vulnerabilityId":-7766815865420462242,"displayName":"ProxyController.proxyUrlWithHttpClient():89","codeLocation":{"displayName":"org.dynatrace.ssrfservice.ProxyController.proxyUrlWithHttpClient(String, String)"}}						
> attacker	{"sourceIp":"172.31.0.57","location":{}}						
> managementZones	[{"id":-334635534222956202,"name":"AppSec: Unguard"}, {"id":-4279023605659327282,"name":"Cloud: AWS"}]						
TenantId	78bd761b-f05a-4bdc-8ac1-9e5d8d75c40						
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.sourcelp)  
| order by Count  
| limit 10
```

Results Chart

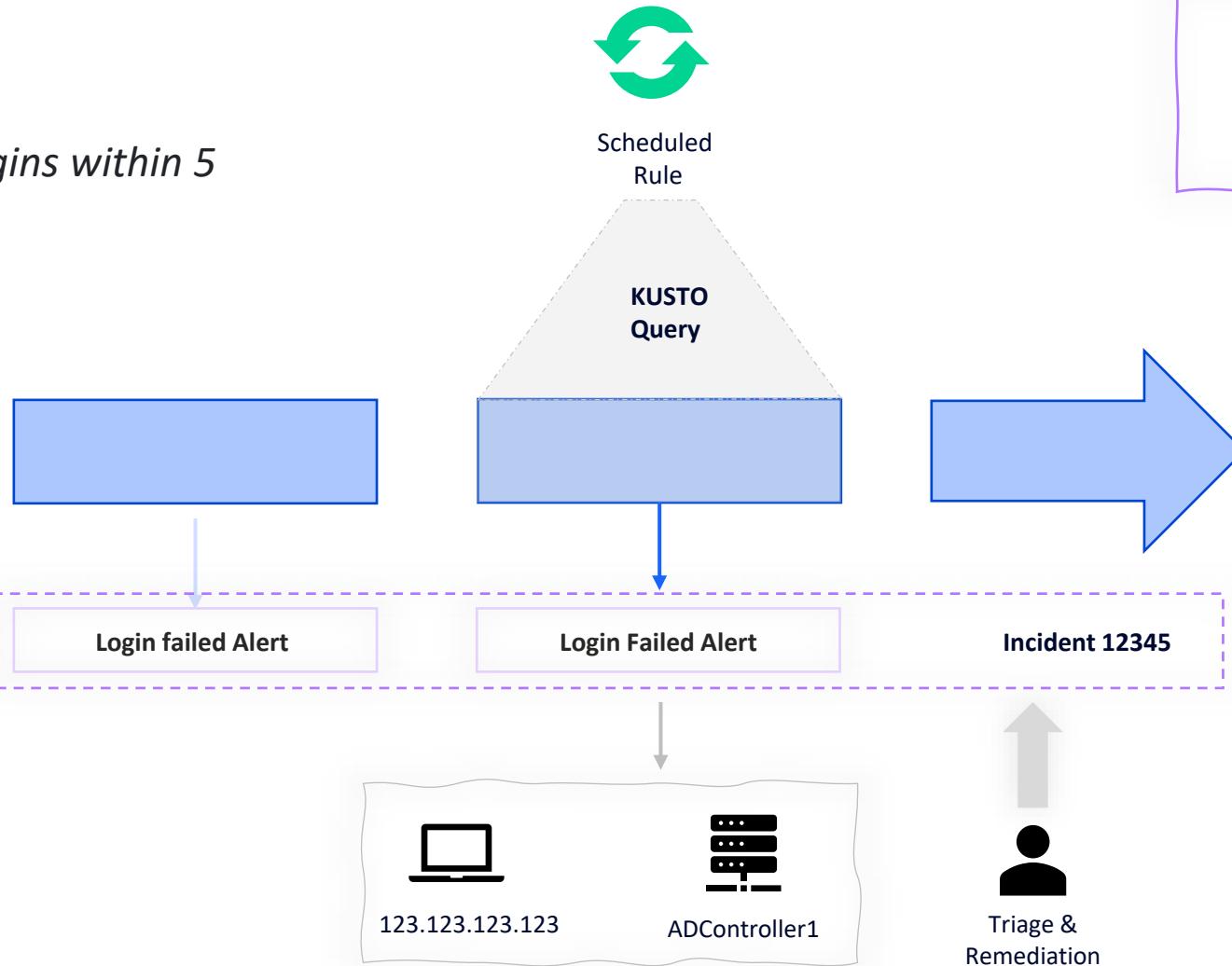
attacker_sourcelp	Count
> 172.31.0.57	3
> 184.195.3.131	3
> 19.21.221.83	2
> 182.7.180.66	2
> 101.58.202.167	2
> 66.96.37.30	1
> 113.167.100.35	1
> 35.183.42.70	1
> 172.175.183.17	1
> 48.130.188.78	1

Reduce human error & increase accuracy by automating threat detection

"Alert on 10 Failed Logins within 5 minutes"



Ingested Data



Other Rule Types

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

Monitoring the Health of your sentinel ingestion

The screenshot shows the Microsoft Azure Data collection health monitoring interface for the workspace 'dynatrace sentinel demo'. It includes a navigation bar with 'Copilot' and user info, and a top bar with 'Search resources, services, and docs (G+)', 'Auto refresh: Off', and a 'Help' link. The main area has tabs for 'Overview', 'Data collection anomalies', and 'Agents info'. The 'Overview' tab displays workspace status for the last 7 days, showing table sizes and entry counts for 'ThreatIntelligenceIndicators', 'ThreatIntelligenceIndicator', 'SentinelHealth', and 'Usage'. A 'Results' table at the bottom provides detailed information about each table.

Table name	Table size	Table entries	Size per entry	Is billable
ThreatIntelligenceIndicators	615.536MB	292.194K	2.15KB	True
ThreatIntelligenceIndicator	181.116MB	288.465K	658.368	True
SentinelHealth	8.683MB	6.084K	1.46KB	False
Usage	202.009KB	501	412.898	False

Data collection health monitoring workbook

The screenshot shows the Microsoft Sentinel 'New Query 1' results table. The query is: `1 SentinelHealth
2 | where Status in ('Success', 'Failure')
3 | summarize TimeGenerated = arg_max(TimeGenerated, *) by SentinelResourceName, SentinelResourceId`. The results table lists various sentinel events with their names, resource IDs, and generation times. The table is sorted by TimeGenerated in descending order.

SentinelResourceName	SentinelResourceId	TimeGenerated (UTC)
Solorigate Network Beacon	/subscriptions/1a2c2a46-2657-...	27/05/2025, 17:22:39.070
Sign-ins from IPs that attempt sign-ins to disabled accounts	/subscriptions/1a2c2a46-2657-...	27/05/2025, 17:22:38.628
Malicious Inbox Rule - custom	/subscriptions/1a2c2a46-2657-...	27/05/2025, 17:17:39.818
Dynatrace - Problem detection	/subscriptions/1a2c2a46-2657-...	27/05/2025, 14:12:03.013
Dynatrace Application Security - Non-critical runtime vulnerability detection	/subscriptions/1a2c2a46-2657-...	27/05/2025, 14:11:32.939
Dynatrace Application Security - Code Level runtime vulnerability detection	/subscriptions/1a2c2a46-2657-...	27/05/2025, 14:11:08.116
Dynatrace Application Security - Attack detection	/subscriptions/1a2c2a46-2657-...	27/05/2025, 14:06:17.420
Dynatrace Application Security - Third-Party runtime vulnerability detection	/subscriptions/1a2c2a46-2657-...	27/05/2025, 14:01:51.035

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



CLOUD DONE RIGHT



Gareth Emslie
Product Manager &
Tech Evangelist