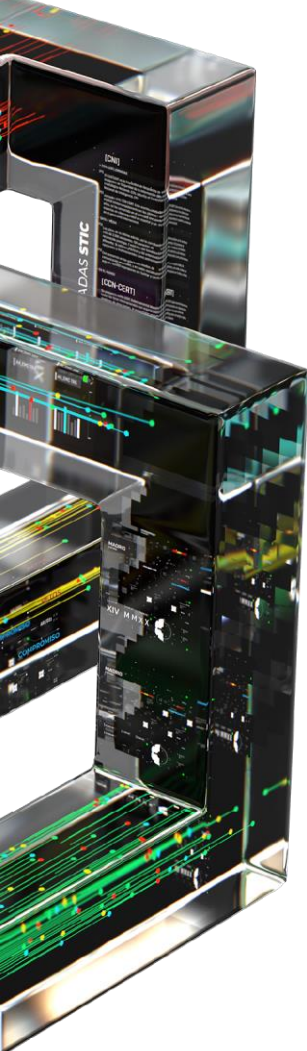




#XIVJORNADASCCNCERT

Modern SOC



Alberto Pinedo Lapeña

National Technology Officer, Microsoft

Alberto.pinedo@microsoft.com



Fernando Rubio Román

Cybersecurity Digital Advisor, Microsoft

Fernando.rubio@microsoft.com



Nube: cambio en el paradigma de la seguridad

MODELO DE SEGURIDAD DIFERENTE

BENEFICIOS

- *Plataforma segura y consistente*
- *Mejora la visibilidad, el control y la detección de amenazas*
- *Existe una responsabilidad menos directa*
- *Funciones de higiene automatizadas*
- *Gestión / informes de cumplimiento más fáciles*



REQUIERE

- *Aprender nuevos controles y plataformas*
- *Aprender sobre el modelo de responsabilidad compartida*
- *Aumentar la "higiene" en los controles de acceso y la identidad*

BIG CHANGES

LA IDENTIDAD Y EL ACCESO ES LA PRIMERA LÍNEA DE DEFENSA

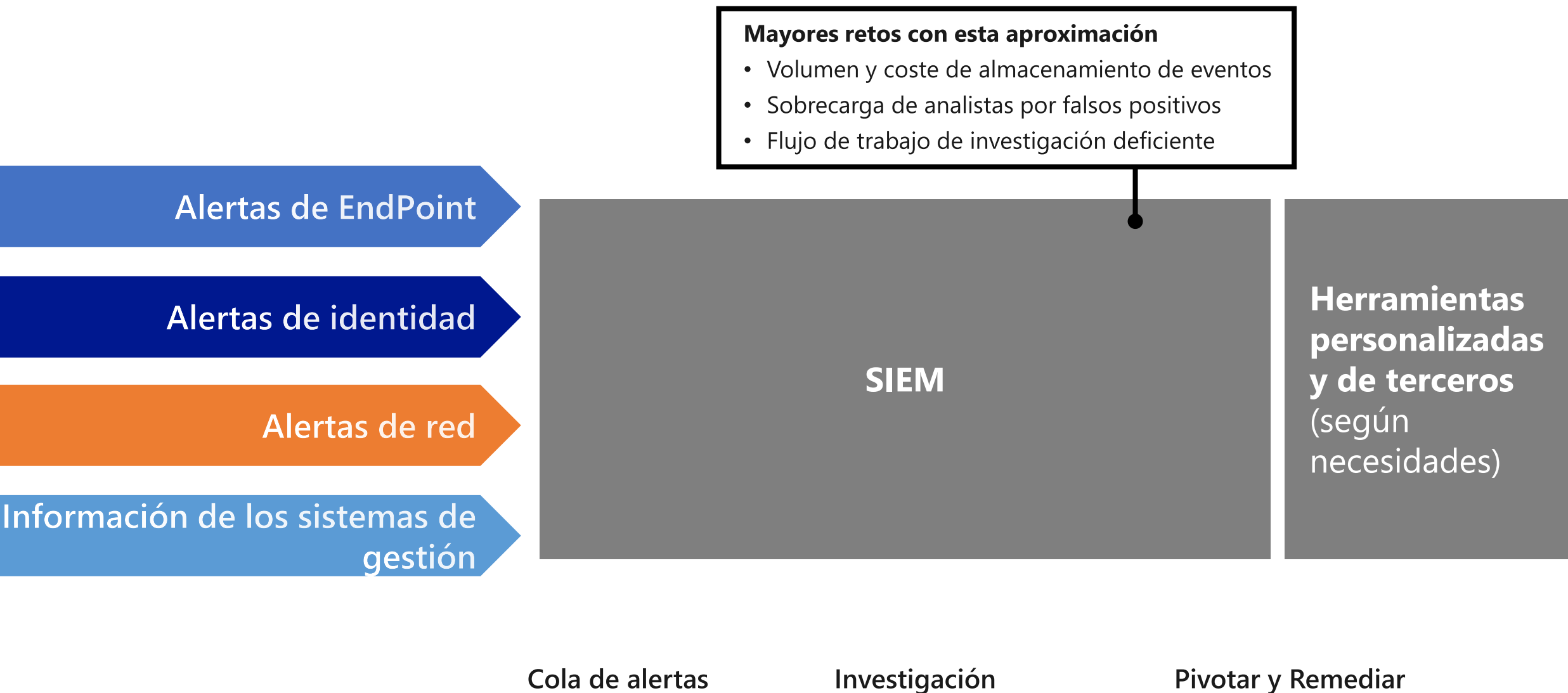
- Es el perímetro de seguridad principal para todas las cargas de trabajo
- Aún se requieren firewalls / red para cargas de trabajo heredadas



SIN PRIVILEGIOS PERMANENTES

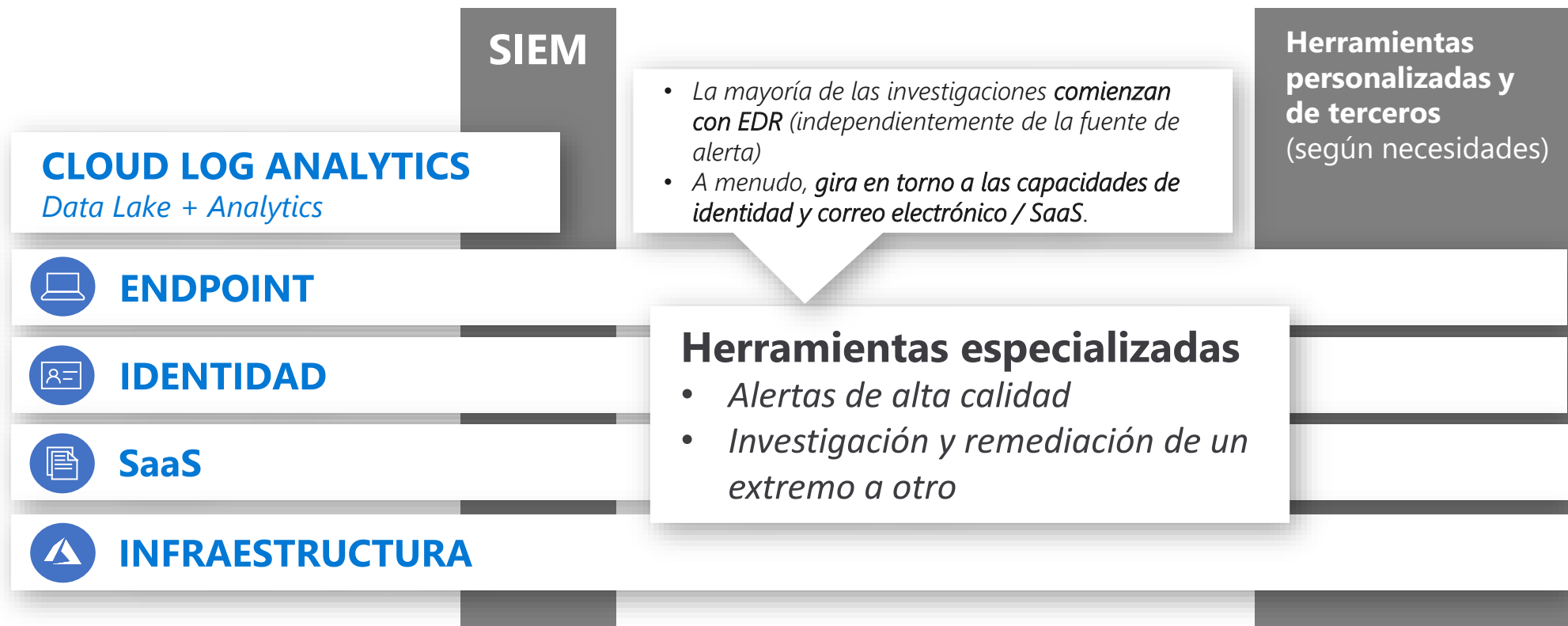
- Acceso puntual para todos los recursos
- Se utiliza para proteger la plataforma en la nube

SOC – Modelo clásico de SIEM



SOC – Evolución

Adoptar herramientas especializadas + Analítica nativa en la nube



Generación de alertas

Cola de alertas

Investigación

Pivotar y Remediar

La aproximación de nuestro propio SOC

- Forzar calidad + aplicar tecnología + amplificar las capacidades de los analistas

Detectar

Responder

Billones de eventos por mes



Machine Learning
(Inteligencia artificial)



Analíticas de comportamiento
(UEBA)
(Usuarios y entidades)

C+AI SOC Triage Dashboard

Redmond Hyderabad MSRC Cases Queue Counts Cases w/o Tasks

Redmond Queue (Excludes MSRC, Master Cases, and XR migrations)

Number	Name	State	Substate	Date created	Severity	Last modified	Date occurred
① SIRO555016	20190515 - CSIRP Mailbox - Malware - qiluio [Autocreated]	Analysis	Email response received	2019-05-15 11:16:47	1 - High	2019-05-16 10:22:13	2019-05-15 11:08:09
① SIRO555849	GLOBAL - 4728 - Global Group Addition - bizamevd:11.AME.CBL - 5/16/2019 4:03:29 PM	Contain	Email sent awaiting response	2019-05-16 09:05:10	1 - High	2019-05-16 10:05:39	2019-05-16 09:03:29
① SIRO546474	[CDG] Scuba NRT - CIS-ForensicsEvent: Forensics-DefenderScan	Review		2019-05-02 18:53:23	2 - Medium	2019-05-14 10:19:56	2019-05-02 18:01:38
① SIRO546692	Scuba NRT - CIS-ForensicsEvent: Forensics-DefenderScan	Review		2019-05-03 02:27:18	2 - Medium	2019-05-10 00:35:54	2019-05-03 02:13:26
① SIRO545038	Scuba NRT - CIS-ForensicsEvent: Forensics-DefenderScan			2019-05-10 00:37:05	2 - Medium	2019-05-10 00:37:05	2019-05-01 03:45:58
① SIRO546610	Scuba NRT - CIS-ForensicsEvent: Forensics-DefenderScan			2019-05-10 00:37:44	2 - Medium	2019-05-10 00:37:44	2019-05-02 22:33:21
① SIRO544868	[AI & Research Group] Scuba NRT - CIS-ForensicsEvent: Forensics-DefenderScan			2019-05-15 20:37:09	2 - Medium	2019-05-15 20:37:09	2019-04-30 20:52:58

Forzar un 90% de verdaderos positivos en todas las alertas



Foco en el tiempo de aceptación y remediación

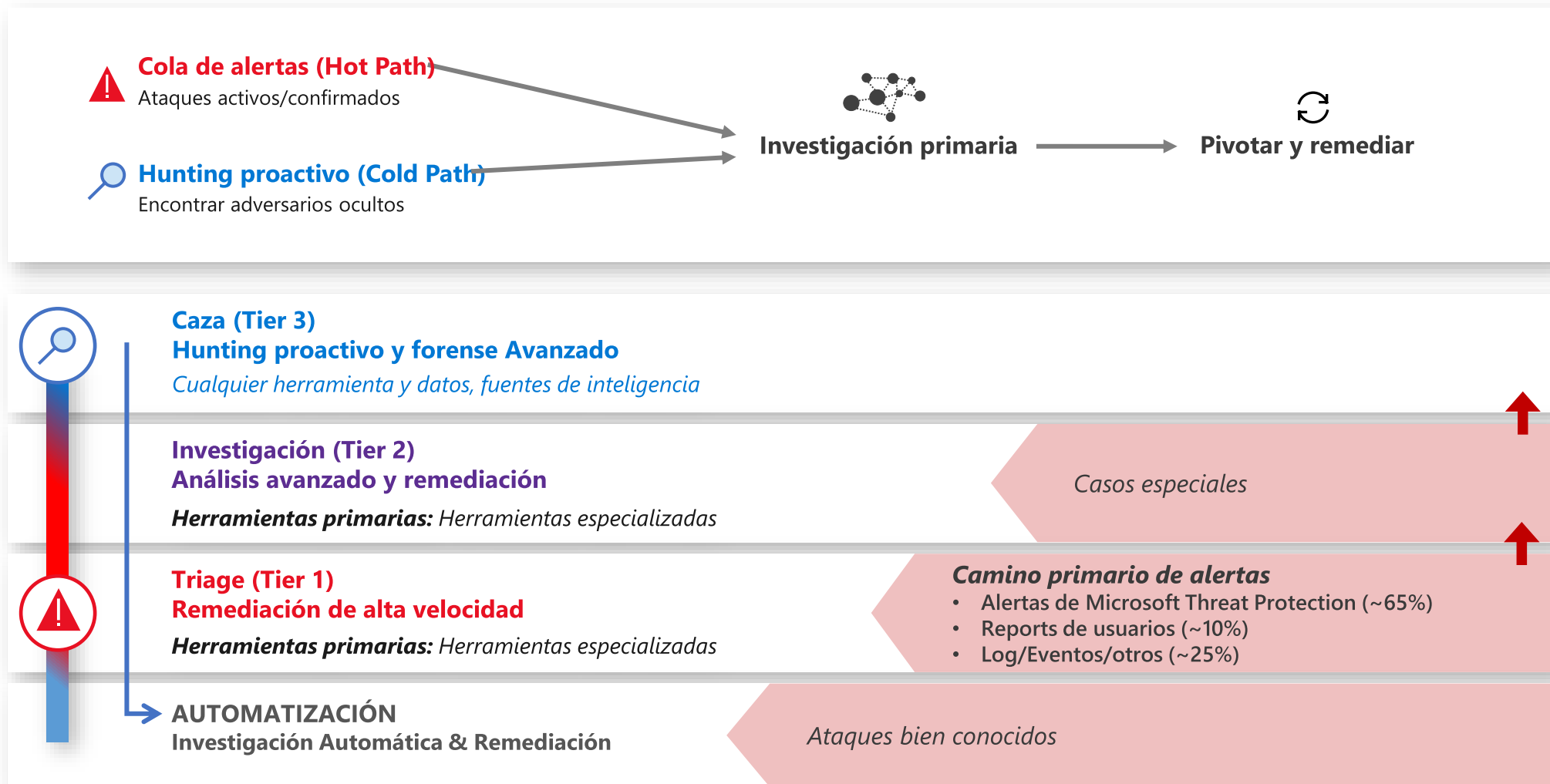
Orquestación de Seguridad, Automatización, y Remediación (SOAR)

Billones de eventos por mes

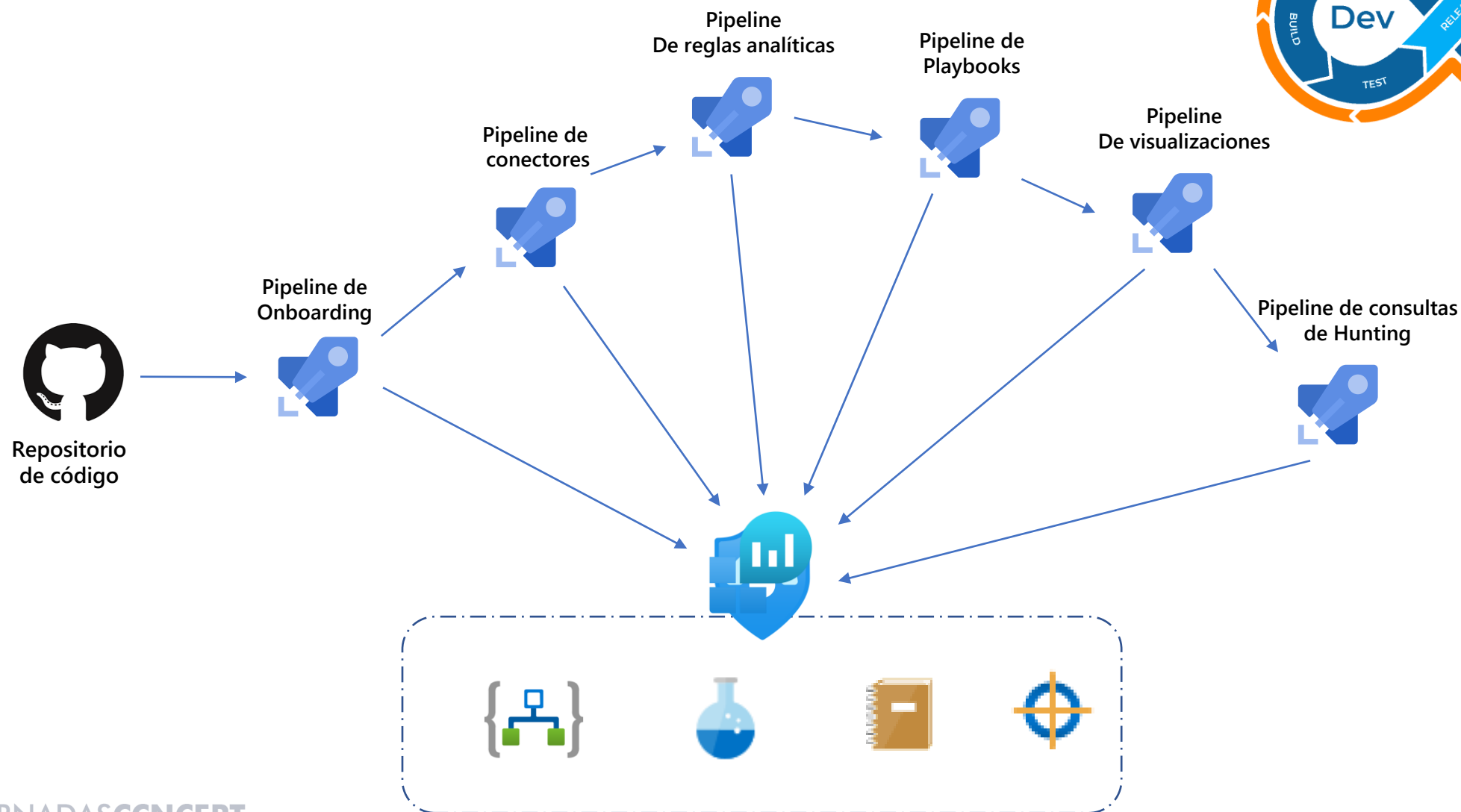
Cientos de investigaciones

Decenas de investigaciones

Microsoft 's IT SOC Corporativo – Tiers y herramientas



SIEM como infraestructura como código



El camino del ML para SecOp

Tres sabores de machine learning

Modelos Built-In

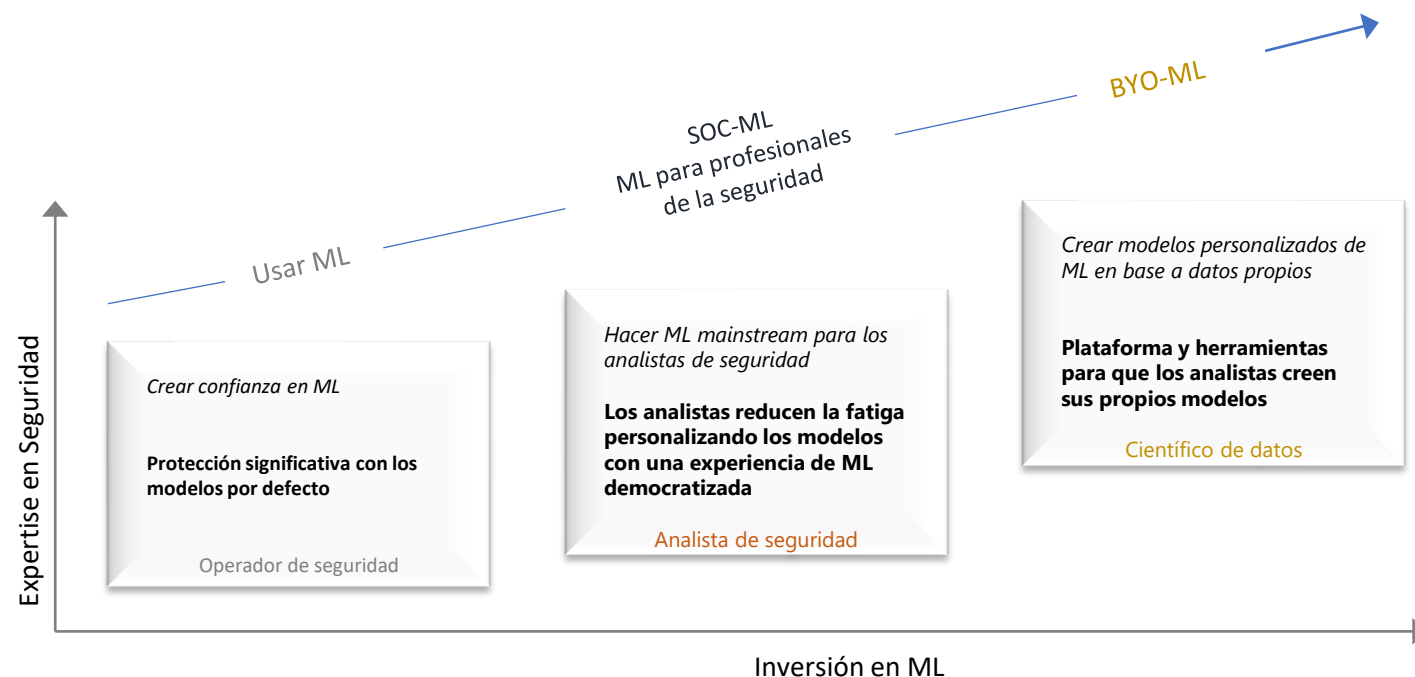
- Detecciones de amenazas "Out-of-the- box" para quien no invierte en ML

SOC-ML

- Permite a los analistas de seguridad, sin conocimientos de ML, afinar los modelos para mejorar el ratio señal ruido

BYO-ML

- Proporciona una plataforma simplificada para los científicos de datos para crear detecciones usando un entorno de ML que les sea familiar e integrar las detecciones en Sentinel



Demo ML personalizado: Acceso anónimo a servidores de ficheros





Search or jump to...



Pull requests

Issues

Marketplace

Explore



Azure / Azure-Sentinel

 Watch ▾

184

 Star

880

 Fork

509

<> Code

! Issues 32

 Pull requests 31

▶ Actions

 Projects

 Wiki

 Security

 Insights

 master ▾

Azure-Sentinel / BYOML /

Go to file

Add file ▾



fafadavi Update README.md

✓ db8fac1 6 days ago

 History

..



Libraries

Update README.md

6 days ago



Notebooks

Add files via upload

27 days ago



README.md

Update README.md

6 days ago

README.md

Build-Your-Own Machine Learning(BYO ML) package, currently in public preview, is provided by Azure Sentinel team to help organizations build or bring your own ML to tackle security problems specifically for your business. This folder contains the BYO ML package including the first ML algorithm Azure Sentinel team shares.

The package includes:

Azure Sentinel | Logs

Selected workspace: 'anilth-ngs-la'

Search (Ctrl+/)

General

- Overview
- Logs**
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks (Preview)
- Entity behavior (Preview)
- Threat intelligence (Preview)

Configuration

- Data connectors
- Analytics
- Playbooks
- Community
- Settings

New Query 1*

AnilTh-NGS-LA

Run Time range : Last 24 hours Save Copy link New alert rule Export Pin to dashboard Format query

Tables Queries Filter

Search

Group by: Solution Filters: not selected

Favorites

You can add favorites by clicking on the ☆ icon

- Azure Sentinel
- LogManagement
- Custom Logs
- Functions

1 SecurityEvent

2

Results Chart Columns Add bookmark Display time (UTC+00:00) Group columns

Completed. Showing results from the last 24 hours. 00:02.2 8 records

	TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName	Channel	Task	Level	EventData
>	9/23/2020, 3:41:49.077 PM	NT AUTHORITY\SYSTEM	Machine	laexportvm1	Microsoft-Windows-Security-Auditing	Security	12,548	8	
>	9/23/2020, 3:41:49.077 PM	NT AUTHORITY\SYSTEM	Machine	laexportvm1	Microsoft-Windows-Security-Auditing	Security	12,544	8	
>	9/23/2020, 3:41:51.267 PM	WORKGROUP\laexportvm1\$	Machine	laexportvm1	Microsoft-Windows-Security-Auditing	Security	13,826	8	<EventData xmlns="http://s
>	9/23/2020, 3:41:51.267 PM	WORKGROUP\laexportvm1\$	Machine	laexportvm1	Microsoft-Windows-Security-Auditing	Security	13,826	8	<EventData xmlns="http://s
>	9/23/2020, 3:41:51.420 PM	NT AUTHORITY\SYSTEM	Machine	laexportvm1	Microsoft-Windows-Security-Auditing	Security	12,548	8	
>	9/23/2020, 3:41:51.420 PM	NT AUTHORITY\SYSTEM	Machine	laexportvm1	Microsoft-Windows-Security-Auditing	Security	12,544	8	
>	9/23/2020, 3:42:20.253 PM			laexportvm1	Microsoft-Windows-Security-Auditing	Security	12,292	8	<EventData xmlns="http://s
>	9/23/2020, 3:42:20.253 PM			laexportvm1	Microsoft-Windows-Security-Auditing	Security	12,290	8	<EventData xmlns="http://s

Page 1 of 1 50 items per page 1 - 8 of 8 items

ms.portal.azure.com/#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/7/subscriptionId/d2a2f3a4-3e6f-4948-ac7a-52a2986fc982/resourceGroup/asi_rsa2019_anil/workspaceName/anilth-ngs-la

Microsoft Azure (Preview) Report a bug Search resources, services, Command Prompt

Home >

Azure Sentinel | Logs

Selected workspace: 'anilth-ngs-la'

Search (Ctrl+ /)

General

Overview

Logs

News & guides

Threat management

Incidents

Workbooks

Hunting

Notebooks (Preview)

Entity behavior (Preview)

Threat intelligence (Preview)

Configuration

Data connectors

Analytics

Playbooks

Community

Settings

New Query 1*

AnilTh-NGS-LA

Run

Time range

Tables

Queries

Filter

Search

Group by: Solution Filters: not selected

Favorites

You can add favorites by clicking on the ☆ icon

Azure Sentinel

LogManagement

Custom Logs

Functions

Results

Chart

Completed. Showing results

TimeGenerated

9/23/2020, 3:4

9/23/2020, 3:4

9/23/2020, 3:4

9/23/2020, 3:4

9/23/2020, 3:4

9/23/2020, 3:4

9/23/2020, 3:4

9/23/2020, 3:4

9/23/2020, 3:4

02.2

8 records

EventData

<EventData xmlns="http://s

<EventData xmlns="http://s

<EventData xmlns="http://s

<EventData xmlns="http://s

Page 1 of 1

50

Items per page

1 - 8 of 8 items

ms.portal.azure.com/#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/7/subscriptionId/d2a2f3a4-3e6f-4948-ac7a-52a2986fc982/resourceGroup/asi_rsa2019_anil/workspaceName/aniith-ngs-la

Apps ASI-RSA New Tab Office 365 Login weather seattle MSTIC-Sentinel Wo...

Microsoft Azure (Preview) Report a bug Search resources, services, Select Command Prompt

Home >

Azure Sentinel | Logs

Selected workspace: 'aniith-ngs-la'

Search (Ctrl+/)

General

Overview

Logs

News & guides

Threat management

Incidents

Workbooks

Hunting

Notebooks (Preview)

Entity behavior (Preview)

Threat intelligence (Preview)

Configuration

Data connectors

Analytics

Playbooks

Community

Settings

New Query 1*

Aniith-NGS-LA

Run

Time range

Tables

Queries

Filter

Search

Group by: Solution Filters: not selected

Favorites

You can add favorites by clicking on the ☆ icon

Azure Sentinel

LogManagement

Custom Logs

Functions

Results

Chart

Completed. Showing results

TimeGenerated

9/23/2020, 3:4

9/23/2020, 3:4

9/23/2020, 3:4

9/23/2020, 3:4

9/23/2020, 3:4

9/23/2020, 3:4

9/23/2020, 3:4

9/23/2020, 3:4

9/23/2020, 3:4

9/23/2020, 3:4

0:\>az monitor log-analytics workspace data-export list --resource-group "asi_rsa2019_anil" --workspace-name "Aniith-NGS-LA"

{

"allTables": null,

"createdDate": "Tue, 21 Jul 2020 00:32:54 GMT",

"dataExportId": "da739135-9bb1-45a9-572d-08d82cffb6aa",

"dataExportType": "StorageAccount",

"enable": true,

"eventHubName": null,

"id": "/subscriptions/d2a2f3a4-3e6f-4948-ac7a-52a2986fc982/resourcegroups/asi_rsa2019_anil/providers/microsoft.operationalinsights/workspaces/aniith-ngs-la/dataexports/laexportclistr",

"lastModifiedDate": "Tue, 22 Sep 2020 15:42:07 GMT",

"name": "LAExportCLIStr",

"resourceGroup": "asi_rsa2019_anil",

"resourceId": "/subscriptions/d2a2f3a4-3e6f-4948-ac7a-52a2986fc982/resourceGroups/ASI_RSA2019_Anil/providers/Microsoft.Storage/storageAccounts/clilaexporteus",

"tableNames": [

"SecurityEvent",

"Heartbeat"

],

"type": "Microsoft.OperationalInsights/workspaces/export"

}

0:\>

aniith@microsoft.com

MICROSOFT

Query explorer

02.2 8 records

EventData

<EventData xmlns="http://s

<EventData xmlns="http://s

<EventData xmlns="http://s

<EventData xmlns="http://s

1 - 8 of 8 items

Home > clilaexporteus | Storage Explorer (preview) ✕

Storage account Directory: Microsoft

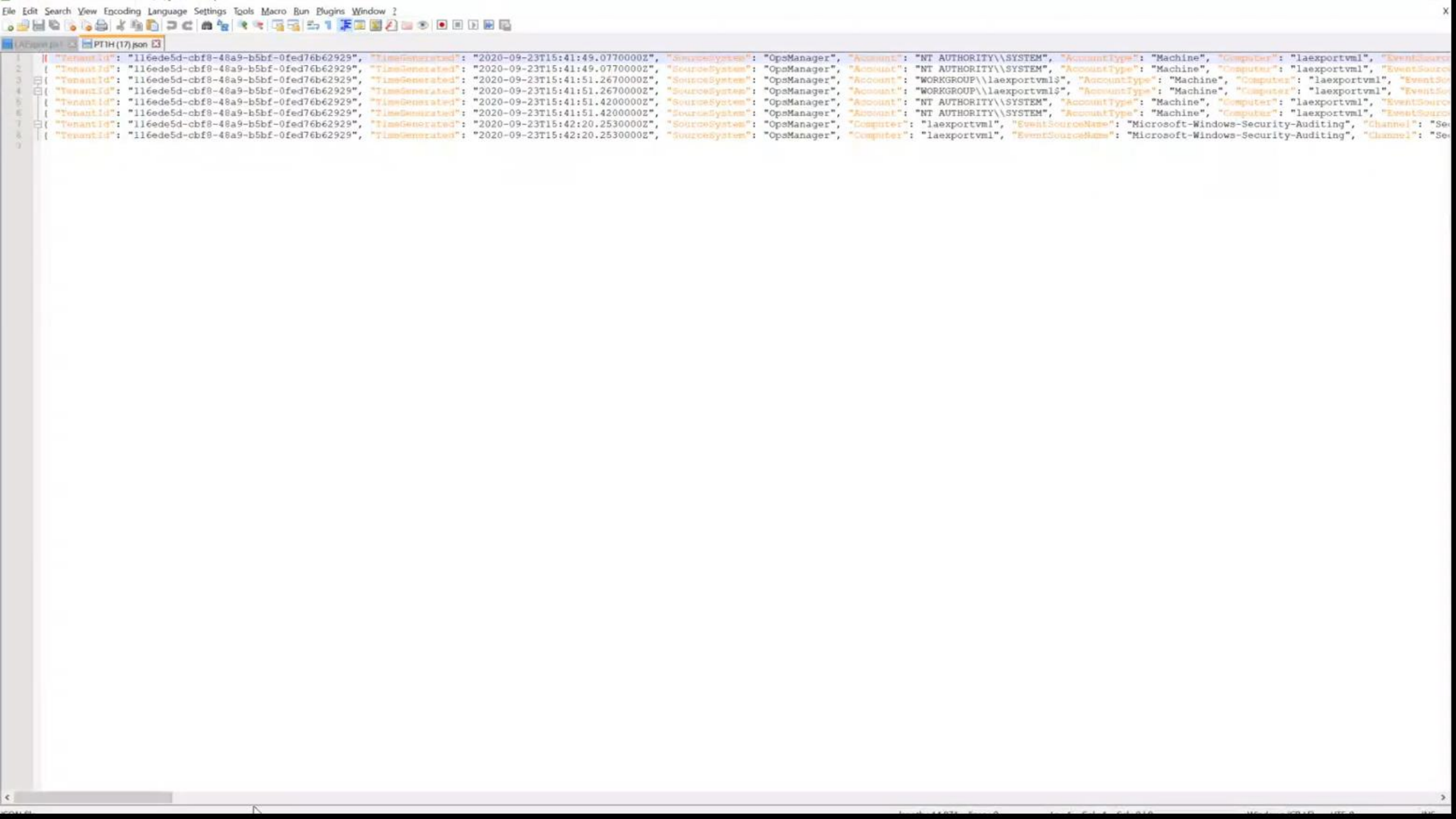
Search

Upload Download Open New Folder Copy URL Select All Copy Paste Rename Delete Undo Create Snapshot Manage Snapshots More

Active blobs (default) resourcegroups > asi_rsa2019_anil > providers > microsoft.operationalinsights > workspaces > anilh-ngs-la > y=2020 > m=09 > d=23 > h=18 > m=00 Search by prefix (case-sensitive)

NAME	ACCESS TIER	ACCESS TIER LAST MODIFIED	LAST MODIFIED	BLOB TYPE	CONTENT TYPE	SIZE	STATUS	REMAINING DAYS	DELETED TIME	LEASE STATE	DISK NAME	VM NAME	DISK TYPE	RESOURCE GROUP NAME
PTTH.json			9/23/2020, 11:10:33 AM	Append Blob	application/octet-stream	7.3 KB	Active							

Showing 1 to 1 of 1 cached items





Home



Workspace



Recents



Data



Clusters



Jobs



Models



Search

AnomalousRATraining-MMLSPARK-SDKv12 (Python)

anildatabricks

BYO-ML-AzureSDKv12 File Edit View: Standard Permissions Run All Clear

Schedule Comments Experiment Revision history

Cmd 5

```
1 from pyspark.sql import functions as f, types as t
2 from pyspark.sql.functions import udf
3 from mmlspark.cyber.anomaly.collaborative_filtering import AccessAnomaly
4 from azure_sentinel_utilities.azure_storage import storage_blob_manager
```

Command took 0.02 seconds -- by anilth@microsoft.com at 9/22/2020, 3:09:21 PM on BYO-ML-AzureSDKv12

Cmd 6

```
1 checkpoint_dir = mount_point_name + 'cache/{0}/checkpoints'.format(project)
2 dbutils.fs.mkdirs(checkpoint_dir)
3 spark.sparkContext.setCheckpointDir(checkpoint_dir)
```

Command took 0.33 seconds -- by anilth@microsoft.com at 9/22/2020, 3:09:21 PM on BYO-ML-AzureSDKv12

Cmd 7

Load Dataset

Cmd 8

```
1 #
2 # This class is used to process 'file share access' related events from Security Events
3 #
4 class FileShareDataset:
5
6     def __init__(self, storage_conn_str):
7         self.storage_conn_str = storage_conn_str
8         self.storage_blob_manager = storage_blob_manager(storage_conn_str)
9
10    @staticmethod
11    def _make_days_delta():
12        @udf('double')
13        def days_delta(d2, d1):
14            return 1.0 + (d2 - d1).days
15        return days_delta
16
17    # NOTE that there are a lot more fields for security events. Below we are picking up only a subset of fields
18    @staticmethod
19    def _security_event_schema():
20        return t.StructType([
21            t.StructField(name = "Account", dataType = t.StringType(), nullable = True),
22            t.StructField(name = "ShareName", dataType = t.StringType(), nullable = True),
23            t.StructField(name = "ShareLocalPath", dataType = t.StringType(), nullable = True),
24            t.StructField(name = "AccountType", dataType = t.StringType(), nullable = True),
25            t.StructField(name = "Computer", dataType = t.StringType(), nullable = True),
```



Search

AnomalousRATraining-MMLSPARK-SDKv12 (Python)



anilth@microsoft.com

BYO-ML-AzureSDKv12

File

Edit

View: Standard

Permissions

Run All

Clear



Schedule



Comments



Experiment



Revision history

Command took 13.97 seconds -- by anilth@microsoft.com at 9/22/2020, 3:09:21 PM on BYO-ML-AzureSDKv12

Cmd 14

Build Model

Cmd 15

```

1 # Model building
2 access_anomaly = AccessAnomaly(
3     tenantCol='tenant_id',
4     userCol='user',
5     resCol='res',
6     likelihoodCol='likelihood',
7     maxIter=100
8 )
9 access_anomaly_model = access_anomaly.fit(pttraining)
    
```

▶ (40) Spark Jobs

Command took 1.48 minutes -- by anilth@microsoft.com at 9/22/2020, 3:09:21 PM on BYO-ML-AzureSDKv12

Cmd 16

Save Model

Cmd 17

```

1 model_output = '{root}/{project}/model_output'.format(root=mount_point_name + 'models', project=project)
2 print(model_output)
    
```

/mnt/rootFSApp/models/ResourceAccessAppend5/model_output

Command took 0.02 seconds -- by anilth@microsoft.com at 9/22/2020, 3:09:21 PM on BYO-ML-AzureSDKv12

Cmd 18

```

1 access_anomaly_model.save(
2     '{model_output}/access_anomaly_model'.format(model_output=model_output)
3 )
    
```

▶ (7) Spark Jobs

Command took 18.70 seconds -- by anilth@microsoft.com at 9/22/2020, 3:09:21 PM on BYO-ML-AzureSDKv12

Cmd 19

```

1 # Mount point for the model
    
```



AnomalousRAScoring-MMLSPARK-SDKv12 (Python)

anilth@microsoft.com

BYO-ML-AzureSDKv12 File Edit View: Standard Permissions Run All Clear

Schedule Comments Experiment Revision history

notebook: /Users/anilth@microsoft.com

Write top anomalous scores to Sentinel

Cmd 29

```
1 @udf
2 def escape_str(str):
3     return str.replace('\\', '\\\\')
4
5 def send_results_to_log_analytics(df_to_la):
6     # The log type is the name of the event that is being submitted. This will show up under "Custom Logs" as log_type + '_CL'
7     log_type = 'AnomalousResourceAccessResult'
8
9     # concatenate columns to form one json record
10    json_records = df_to_la.withColumn('json_field', f.concat(f.lit('{}',
11        f.lit(' \"Timestamp\": '), f.from_unixtime(f.unix_timestamp(f.col('timestamp')), "y-MM-dd'T'hh:mm:ss.SSS'Z'"), f.lit('\"'),
12        f.lit(' \"User\": '), escape_str(f.col('user')), f.lit('\"'),
13        f.lit(' \"Resource\": '), escape_str(f.col('res')), f.lit('\"'),
14        f.lit(' \"AnomalyScore\": '), f.col('anomaly_score'),
15        f.lit('{}')
16    ))
17
18    # combine json record column to create the array
19    json_body = json_records.agg(f.concat_ws(" ", f.collect_list('json_field')).alias('body'))
20
21    if len(json_body.first()) > 0:
22        json_payload = json_body.first()['body']
23        json_payload = '[' + json_payload + ']'
24
25        payload = json_payload.encode('utf-8') #json.dumps(json_payload)
26        print(payload)
27        return log_analytics_client(workspace_id, workspace_shared_key).post_data(payload, log_type)
28    else:
29        return "No json data to send to LA"
30
31 count = results_to_la.count()
32 if count > 0:
33     print ('Results count = ', count)
34     result = send_results_to_log_analytics(results_to_la)
35     print("Writing to Log Analytics result: ", result)
36 else:
37     print ('No results to send to LA')
```

▶ (3) Spark Jobs

Results count = 3

b'[{ "TimeStamp": "2020-09-03T12:00:00.000Z", "User": "exportvm1\\\\\\\\ryan", "Resource": "\\ShareFolder2", "AnomalyScore":0.986343279566988}, { "TimeStamp": "2020-09-03T12:00:00.000Z", "User": "exportvm1\\\\\\\\\\\\\\\\anil", "Res

Home >

Azure Sentinel | Logs

Selected workspace: 'anilth-ngs-la'

Search (Ctrl+/)

General

Overview

Logs

News & guides

Threat management

Incidents

Workbooks

Hunting

Notebooks (Preview)

Entity behavior (Preview)

Threat intelligence (Preview)

Configuration

Data connectors

Analytics

Playbooks

Community

Settings

New Query 1*

AnilTh-NGS-LA

Tables

Queries

Filter

Search

Group by: Solution Filters: not selected

Favorites

You can add favorites by clicking on the ☆ icon

Azure Sentinel

LogManagement

Custom Logs

Functions

Run

Time range: Last 24 hours

Save

Copy link

New alert rule

Export

Pin to dashboard

Format query

1 AnomalousResourceAccessResult_CL | take 10

Results

Chart

Columns

Add bookmark

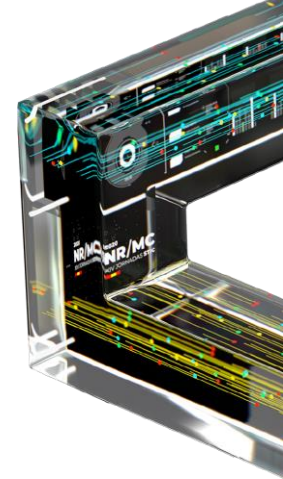
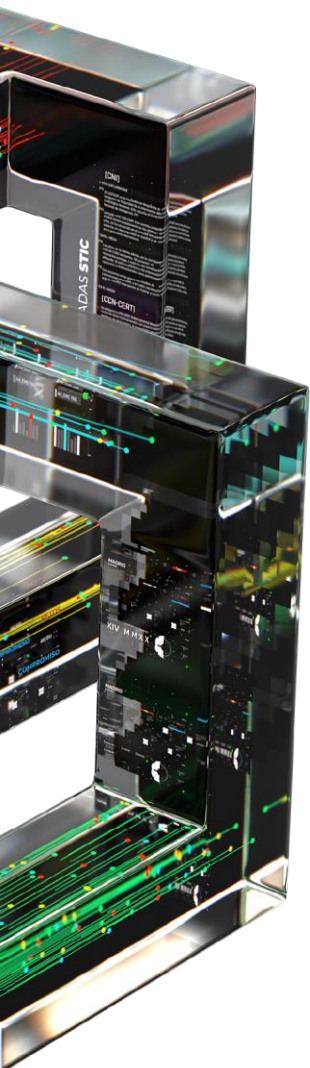
Display time (UTC+00:00)

Group columns

Completed. Showing results from the last 24 hours.

00:00.8 3 records

☐	TimeGenerated [UTC]	Computer	RawData	User_s	AnomalyScore_d	TimeStamp_t [UTC]	TimeStamp_s	Actor_s	Resource	Pre
> ☐	9/22/2020, 10:15:29.586 PM			exportvm1ryan	0.986	9/3/2020, 12:00:00.000 PM			*\ShareFolder2	
> ☐	9/22/2020, 10:15:29.586 PM			exportvm1anil	0.939	9/3/2020, 12:00:00.000 PM			*\IPC\$	
> ☐	9/22/2020, 10:15:29.586 PM			WORKGROUP\exportvm1\$	0.759	9/3/2020, 12:00:00.000 PM			*\ShareFolder2	



MUCHAS GRACIAS

#XIVJORNADASCCNCERT