The art of knowing your SIEM & XDR data

Start 15:25

Bert-Jan Pals

Security MVP, kqlquery.com

Microsoft MVP 2023 Most Valuable Professional

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Agenda

6 points

1. Introduction
2. Why want to know your data?
3. Data theory
4. Preview: SOC Optimization
5. Demo: Investigating XDR & Sentinel Data
6. Q&A

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Why want to know your data?

Data in numbers

	Small 0 – 500	Medium 500 - 5000	Large 5000+	Large Enterprise 100.000+
# Daily Events	5.000.000	150.000.000	500.000.000	1.200.000.000
# Tables	50	75	100	100 – N
# Actions	500	1800	2500	5000

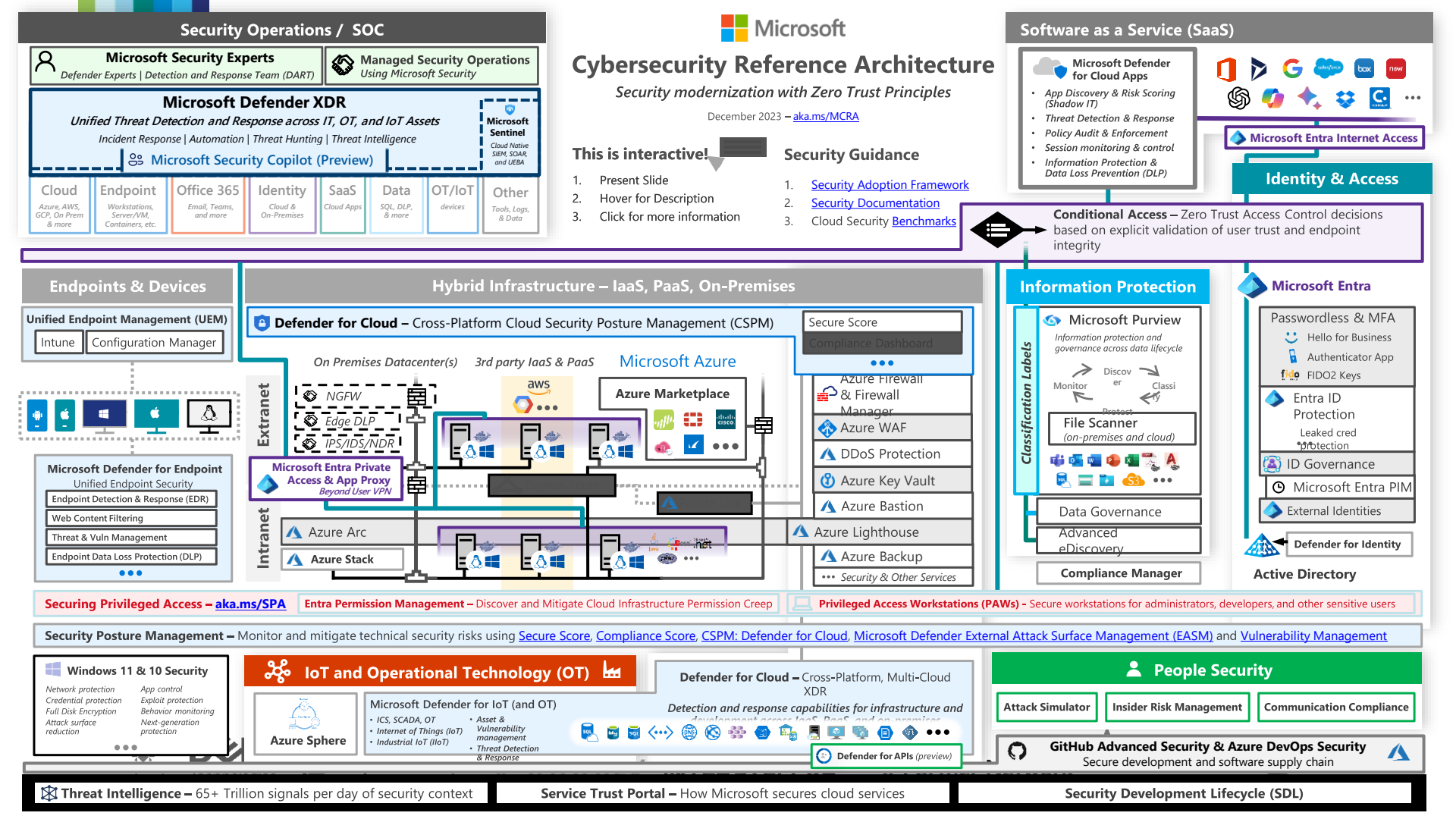
rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Log Data

Security & Audit
- Endpoints
- Server
- Cloud Resources
- Identities
- Network

Operation
- Availability
- Performance
- Incidents
- Troubleshooting

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka


Security Operations / SOC
Microsoft Security Experts
Defender Experts | Detection and Response Team (DART)
Managed Security Operations
Using Microsoft Security
Microsoft Defender XDR
Unified Threat Detection and Response across IT, OT, and IoT Assets
Incident Response | Automation | Threat Hunting | Threat Intelligence
Microsoft Sentinel
Cloud Native SIEM, SOAR, and UEBA
Microsoft Security Copilot (Preview)
Cloud
Azure, AWS, GCP, On Prem & more
Endpoint
Workstations, Server/VM, Containers, etc.
Office 365
Email, Teams, and more
Identity
Cloud & On-Premises
SaaS
Cloud Apps
Data
SQL, DLP, & more
OT/IoT
devices
Other
Tools, Logs, & Data
Microsoft
Cybersecurity Reference Architecture
Security modernization with Zero Trust Principles
December 2023 – aka.ms/MCRA
This is interactive!
1. Present Slide
2. Hover for Description
3. Click for more information
Security Guidance
1. Security Adoption Framework
2. Security Documentation
3. Cloud Security Benchmarks
Software as a Service (SaaS)
Microsoft Defender for Cloud Apps
App Discovery & Risk Scoring (Shadow IT)
Threat Detection & Response
Policy Audit & Enforcement
Session monitoring & control
Information Protection & Data Loss Prevention (DLP)
Microsoft Entra Internet Access
Identity & Access
Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity
Endpoints & Devices
Unified Endpoint Management (UEM)
Intune
Configuration Manager
Microsoft Defender for Endpoint
Unified Endpoint Security
Endpoint Detection & Response (EDR)
Web Content Filtering
Threat & Vuln Management
Endpoint Data Loss Protection (DLP)
Hybrid Infrastructure – IaaS, PaaS, On-Premises
Defender for Cloud – Cross-Platform Cloud Security Posture Management (CSPM)
Secure Score
Compliance Dashboard
On Premises Datacenter(s)
3rd party IaaS & PaaS
Microsoft Azure
Extranet
Intranet
NGFW
Edge DLP
IPS/IDS/NDR
Microsoft Entra Private Access & App Proxy
Beyond User VPN
Azure Marketplace
Azure Arc
Azure Stack
Azure Firewall & Firewall Manager
Azure WAF
DDoS Protection
Azure Key Vault
Azure Bastion
Azure Lighthouse
Azure Backup
Security & Other Services
Information Protection
Classification Labels
Microsoft Purview
Information protection and governance across data lifecycle
Monitor
Discover
Classify
Protect
File Scanner
(on-premises and cloud)
Data Governance
Advanced eDiscovery
Compliance Manager
Microsoft Entra
Passwordless & MFA
Hello for Business
Authenticator App
FIDO2 Keys
Entra ID Protection
Leaked cred protection
ID Governance
Microsoft Entra PIM
External Identities
Defender for Identity
Active Directory
Securing Privileged Access – aka.ms/SPA
Entra Permission Management – Discover and Mitigate Cloud Infrastructure Permission Creep
Privileged Access Workstations (PAWs) - Secure workstations for administrators, developers, and other sensitive users
Security Posture Management – Monitor and mitigate technical security risks using Secure Score, Compliance Score, CSPM: Defender for Cloud, Microsoft Defender External Attack Surface Management (EASM) and Vulnerability Management
Windows 11 & 10 Security
Network protection
Credential protection
Full Disk Encryption
Attack surface reduction
App control
Exploit protection
Behavior monitoring
Next-generation protection
IoT and Operational Technology (OT)
Azure Sphere
Microsoft Defender for IoT (and OT)
ICS, SCADA, OT
Internet of Things (IoT)
Industrial IoT (IIoT)
Asset & Vulnerability management
Threat Detection & Response
Defender for Cloud – Cross-Platform, Multi-Cloud XDR
Detection and response capabilities for infrastructure and
Defender for APIs (preview)
People Security
Attack Simulator
Insider Risk Management
Communication Compliance
GitHub Advanced Security & Azure DevOps Security
Secure development and software supply chain
Threat Intelligence – 65+ Trillion signals per day of security context
Service Trust Portal – How Microsoft secures cloud services
Security Development Lifecycle (SDL)

Why need to know your data?

- Response efficiency
- Knowing when to use which table
- Enrich (security) incidents
- Cost
- Get more value from the ingested data
- Discovery of new hunting/detection potential
- Identify gaps
- Reliability

Data Theory

XDR Tables

Defender For Identity	Defender For Endpoint	Defender For Office 365	Defender Cloud Apps	Entra ID	Exposure Management
• IdentityDirectoryEvents • IdentityInfo • IdentityLogonEvents • IdentityQueryEvents	• DeviceEvents • DeviceFileCertificateInfo • DeviceFileEvents • DeviceImageLoadEvents • DeviceInfo • DeviceLogonEvents • DeviceNetworkEvents • DeviceNetworkInfo • DeviceProcessEvents • DeviceRegistryEvents • DeviceTvm*	• EmailAttachmentInfo • EmailEvents • EmailPostDeliveryEvents • EmailUrlInfo • UrlClickEvents	• BehaviorEntities • BehaviorInfo • CloudAppEvents	• AADSignInEventsBeta • AADSpnSignInEventsBeta	• ExposureGraphEdges • ExposureGraphNodes

Tables contain data if product is installed, no additional cost for storing data.

Sentinel Tables

Azure	Log Analytics	Office 365	Syslog/CommonSecurityEvents	Entra ID	Other
• AzureActivity • Operation • AzureDiagnostics • Heartbeat • SecurityBaseline • SecurityBaselineSummary • AZ Firewall	• Usage • LAQueryLogs	• OfficeActivity	• Network Devices • VPN Devices • Linux Servers	•AuditLogs •SignInLogs •NonInteractiveUserSignInLogs •ServicePrincipalSignInLogs •ManagedIdentitySignInLogs •ProvisioningLogs •ADFSSignInLogs •RiskyUsers •UserRiskEvents •NetworkAccessTrafficLogs •RiskyServicePrincipals •ServicePrincipalRiskEvents •EnrichedOffice365AuditLogs •MicrosoftGraphActivityLogs •RemoteNetworkHealthLogs	• IntuneAuditLogs • IntuneDeviceComplianceOrg • IntuneDevices • ThreatIntelligenceIndicator • AWSCloudTrail • AWSCloudWatch • AWSGuardDuty • GCPAuditLogs • *_CL

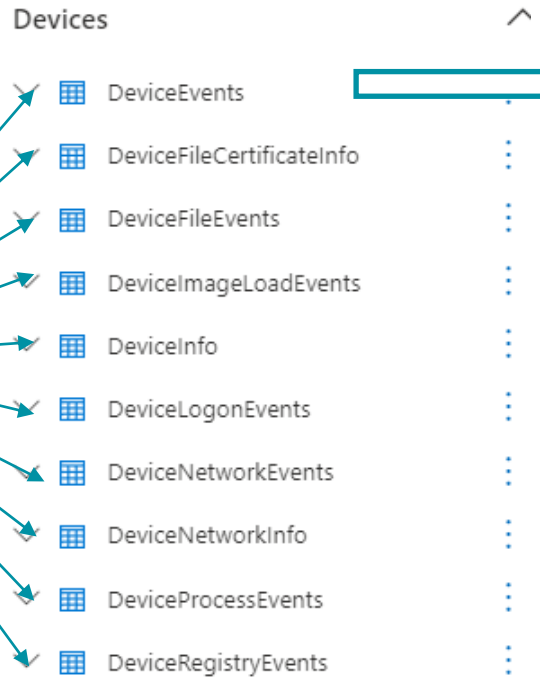
Tables only contain data if configured, additional cost may be involved.

Data Flow

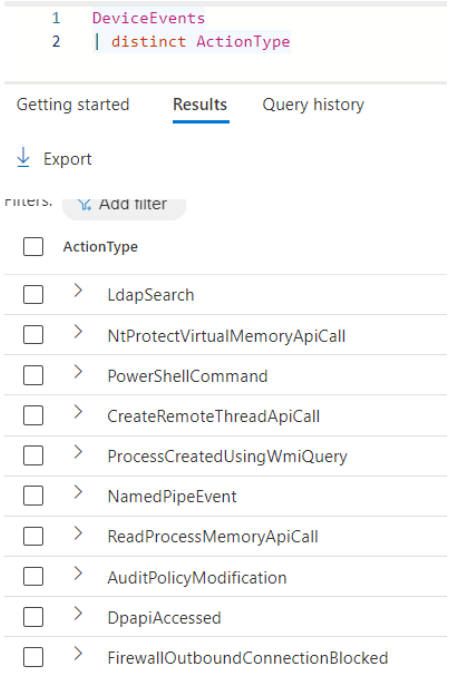
1 Product

Microsoft Defender for Endpoint

10 Tables



50 + Actions (Sub-Tables)



rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Sub-Tables

- DeviceEvents Table ->
- Table != one datasource
- Relation between amount of configuration and ActionTypes

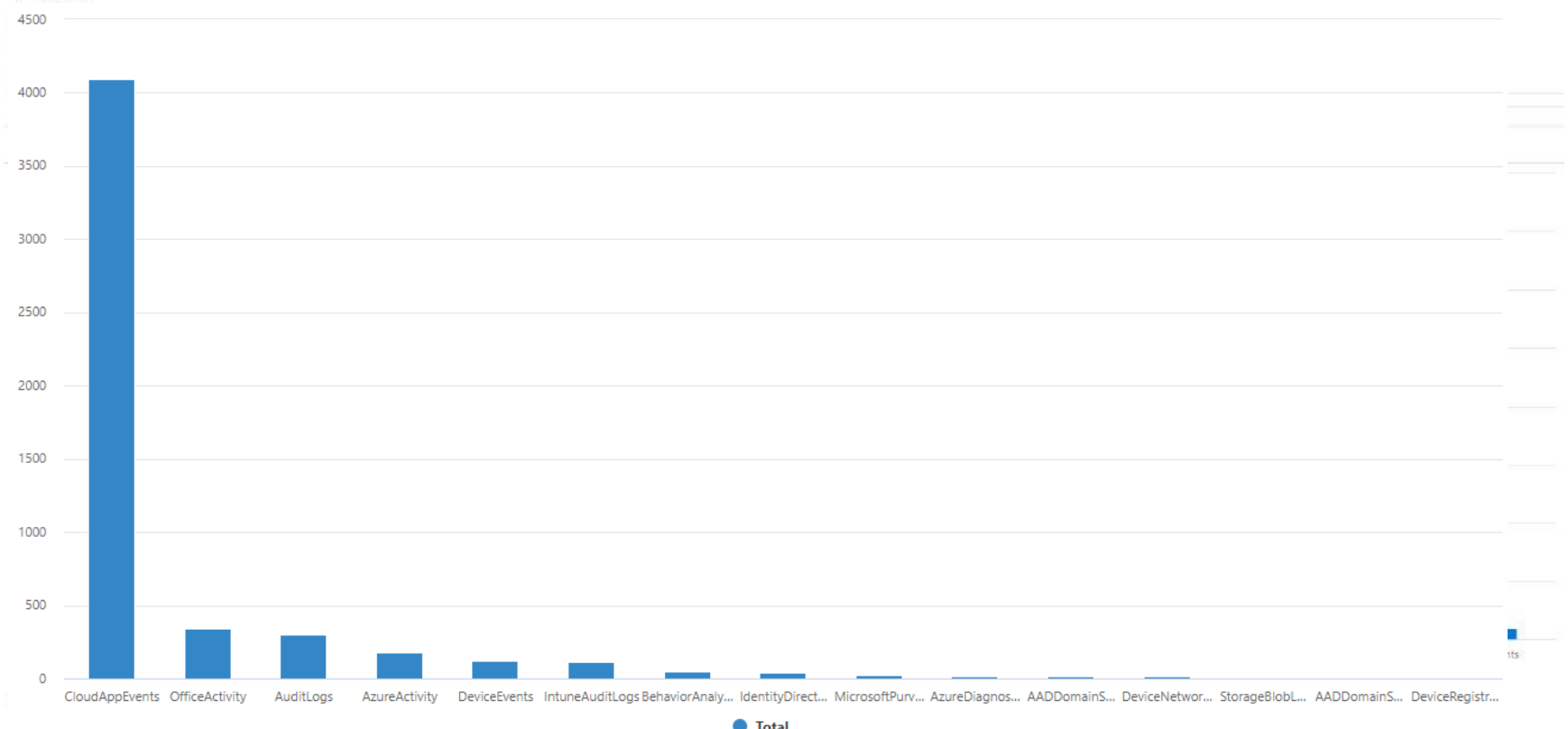
DeviceEvents Sub-Tables	Example ActionType
Attack Surface Reduction Rules	• AsrExecutableOfficeContentBlocked • AsrPsexecWmiChildProcessAudited
Network Activity	• DnsQueryResponse • RemoteDesktopConnection
Identity	• UserAccountAddedToLocalGroup • UserAccountCreated • SecurityGroupCreated • LdapSearch
Antivirus	• AntivirusDetection • AntivirusScanCompleted
Process	• PowerShellCommand • ProcessCreatedUsingWmiQuery

Sub-Tables

- OfficeActivity Table ->
- Table != one datasource

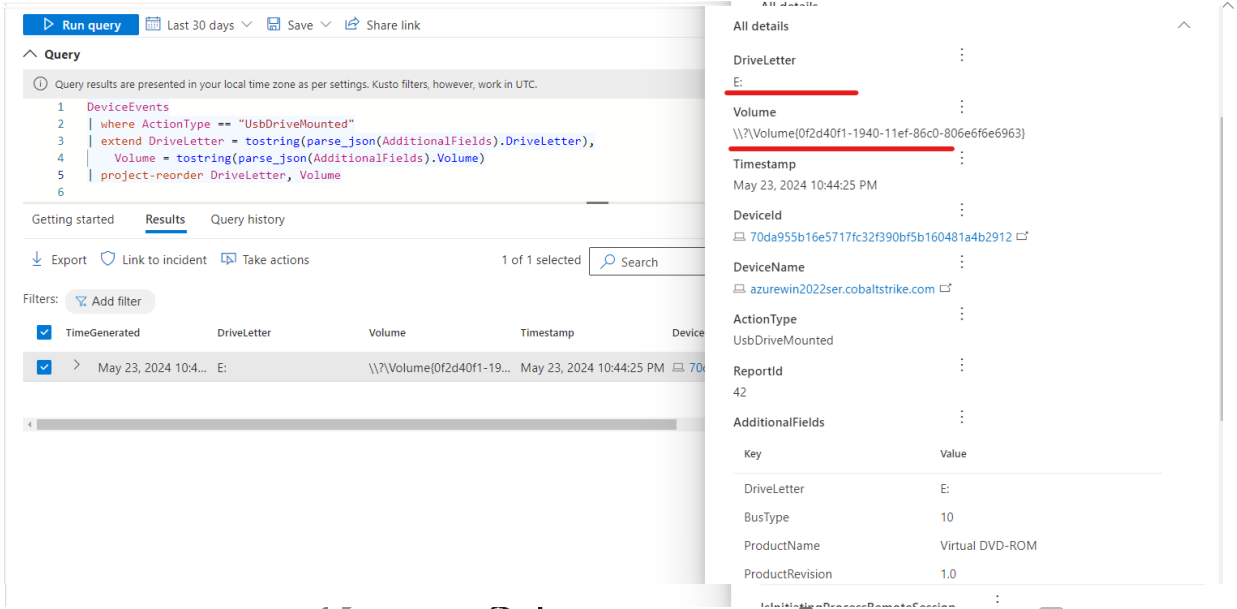
OfficeActivity Sub-Tables	Example Operation
Exchange	• MailItemsAccessed • Add-MailboxPermission
SharePoint	• AddedToGroup • PageViewed • FolderCreated
Microsoft Teams	• MemberRemoved • TeamsSessionStarted • ChannelAdded

Sub-Tables


4500
4000
3500
3000
2500
2000
1500
1000
500
0
CloudAppEvents
OfficeActivity
AuditLogs
AzureActivity
DeviceEvents
IntuneAuditLogs
BehaviorAnaly...
IdentityDirect...
MicrosoftPurv...
AzureDiagnos...
AADDomainS...
DeviceNetwor...
StorageBlobL...
AADDomainS...
DeviceRegistr...
Total

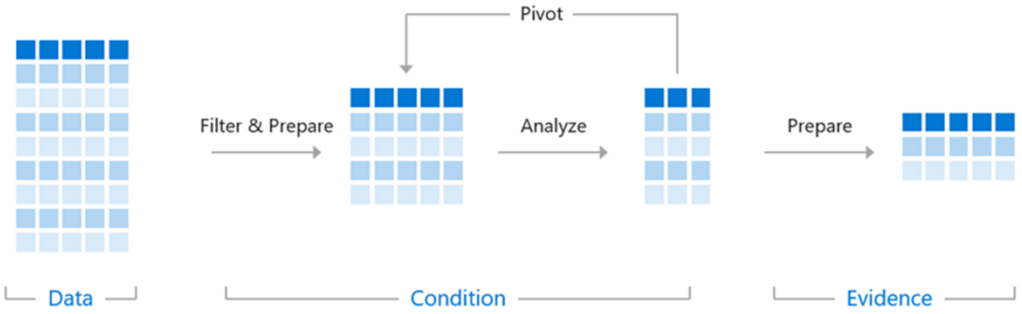
To get to the important data you might need to parse

- The investigation/detection data can be ‘hidden’
- RawData
- AdditionalFields



How to get the data from a table?

```
SecurityEvent | where EventID == "4626" | summarize count() by Account | limit 10
```



Summarize columns
Distinct values
getschema
Take 100
Review AdditionalData & Raw data

Why Learn KQL?

No matter what IT career path you pursue, you'll meet **KQL**

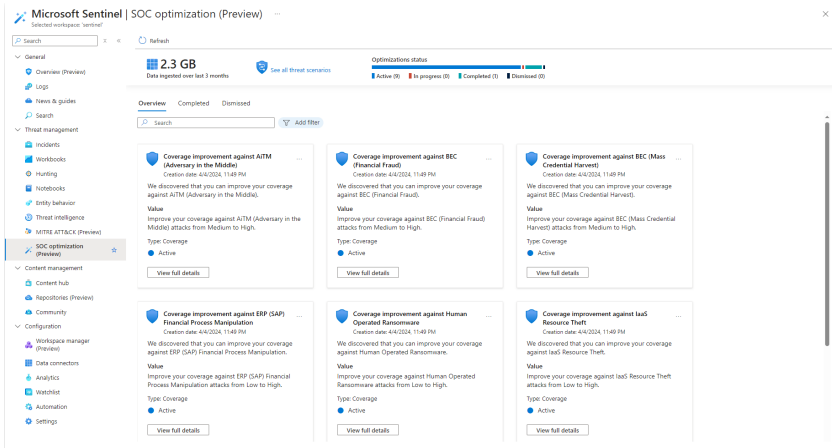
rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Preview: SOC Optimization

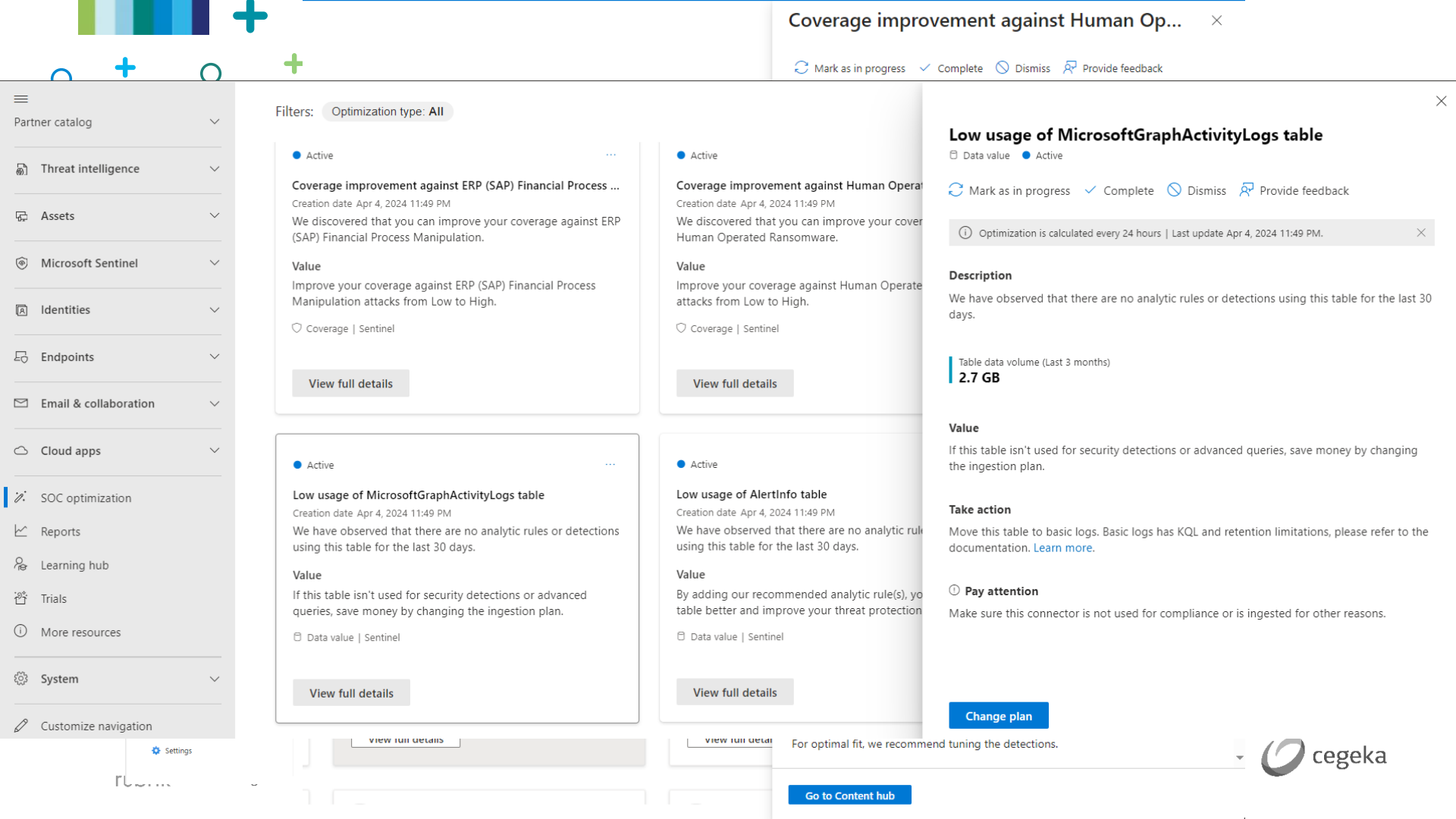
Experts Live Netherlands

New Feature: SOC optimization

- Public preview
- Available for Sentinel and Unfied XDR Customers (no support for only Defender XDR)
- Coverage improvements common attack scenarios
- Recommended Analytics Rules
- Low usage tables



rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka


Coverage improvement against Human Op...
Mark as in progress
Complete
Dismiss
Provide feedback
Partner catalog
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
SOC optimization
Reports
Learning hub
Trials
More resources
System
Customize navigation
Settings
Filters:
Optimization type: All
Active
Coverage improvement against ERP (SAP) Financial Process ...
Creation date Apr 4, 2024 11:49 PM
We discovered that you can improve your coverage against ERP (SAP) Financial Process Manipulation.
Value
Improve your coverage against ERP (SAP) Financial Process Manipulation attacks from Low to High.
Coverage | Sentinel
View full details
Active
Coverage improvement against Human Operat
Creation date Apr 4, 2024 11:49 PM
We discovered that you can improve your cover
Human Operated Ransomware.
Value
Improve your coverage against Human Operate
attacks from Low to High.
Coverage | Sentinel
View full details
Active
Low usage of MicrosoftGraphActivityLogs table
Creation date Apr 4, 2024 11:49 PM
We have observed that there are no analytic rules or detections using this table for the last 30 days.
Value
If this table isn't used for security detections or advanced queries, save money by changing the ingestion plan.
Data value | Sentinel
View full details
Active
Low usage of AlertInfo table
Creation date Apr 4, 2024 11:49 PM
We have observed that there are no analytic rul
using this table for the last 30 days.
Value
By adding our recommended analytic rule(s), yo
table better and improve your threat protection
Data value | Sentinel
View full details
Low usage of MicrosoftGraphActivityLogs table
Data value
Active
Mark as in progress
Complete
Dismiss
Provide feedback
Optimization is calculated every 24 hours | Last update Apr 4, 2024 11:49 PM.
Description
We have observed that there are no analytic rules or detections using this table for the last 30 days.
Table data volume (Last 3 months)
2.7 GB
Value
If this table isn't used for security detections or advanced queries, save money by changing the ingestion plan.
Take action
Move this table to basic logs. Basic logs has KQL and retention limitations, please refer to the documentation. Learn more.
Pay attention
Make sure this connector is not used for compliance or is ingested for other reasons.
Change plan
For optimal fit, we recommend tuning the detections.
Go to Content hub
cegeka

Demo Prep

KQL 101

Declare Variable

Filter Time

Table Name

Add Column

Display Results

Sort Results

```
1  let TimeFrame = 3d;
2  EmailEvents
3  | where TimeGenerated > startofday(ago(TimeFrame))
4  | where EmailDirection == "Intra-org"
5  | extend DKIMValue = tostring(parse_json(AuthenticationDetails).DKIM)
6  | project TimeGenerated, SenderDisplayName, RecipientEmailAddress, Subject, DKIMValue
7  | sort by TimeGenerated desc
```

Results | Chart | Add bookmark

TimeGenerated [UTC]	SenderDisplay...	RecipientEmailAddress	Subject	DKIMValue
2/20/2024, 12:29:29.000 AM	Bert-Jan	bert-jan@kqlquery.com	Sentinel Data Ingestion Report:...	none
2/19/2024, 12:29:30.000 AM	Bert-Jan	bert-jan@kqlquery.com	Sentinel Data Ingestion Report:...	none
2/18/2024, 12:29:28.000 AM	Bert-Jan	bert-jan@kqlquery.com	Sentinel Data Ingestion Report:...	none
2/17/2024, 12:29:31.000 AM	Bert-Jan	bert-jan@kqlquery.com	Sentinel Data Ingestion Report:...	none

KQL 101

Summarize – Statistics
Distinct – Unique values

```
1  DeviceEvents
2  | summarize TotalEvents = count() by ActionType
```

Getting started | Results | Query history

Export

Filters: Add filter

ActionType	TotalEvents
LdapSearch	1692
PowerShellCommand	555
ProcessCreatedUsingWmiQuery	497
NamedPipeEvent	308
NtProtectVirtualMemoryApiCall	300
GetClipboardData	223
ShellLinkCreateFileEvent	133
BrowserLaunchedToOpenUrl	132
DpapiAccessed	127

```
1  DeviceEvents
2  | distinct ActionType
```

Getting started | Results | Query history

Export

Filters: Add filter

ActionType
LdapSearch
PowerShellCommand
ProcessCreatedUsingWmiQuery
NtProtectVirtualMemoryApiCall
NamedPipeEvent
GetClipboardData
ShellLinkCreateFileEvent
BrowserLaunchedToOpenUrl
AuditPolicyModification

Demo

- Analyzing Tables
- Data Workbook
- Entity Workbook
- Automate New Action Notifications
- SOC Optimization

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

XDR vs Sentinel vs Unfied XDR

	Defender XDR	Sentinel	Unfied XDR
Workbooks	✗	✓	✓
Automate new ActionTypes (Logic Apps)	✓ (Defender APT API or Graph API)	✓ (Azure Monitor API)	✓
Table Reference	✓	✓	✓
KQL getschema support	✓	✓	✓
KQL Table Type support (union * | distinct Type)	✗	✓	✓
Preview: SOC Optimization	✗	✓	✓

How to get started?

1. Proactive approach
2. Use distinct & summarize on tables, ActionTypes, entities
3. Run search activities on entities, see what the results are
4. If you expect more logs, check configuration
5. This does apply to all your data, not only security
6. Workbooks and Logic Apps – GitHub
7. Queries – GitHub

Blogs:

LinkedIn:

Please evaluate this session in the App.

THANK YOU

Are there any questions?

KQL & Tools:

Blogs: KQLQuery.com
GitHub: https://github.com/bert-janp

Data Dashboard

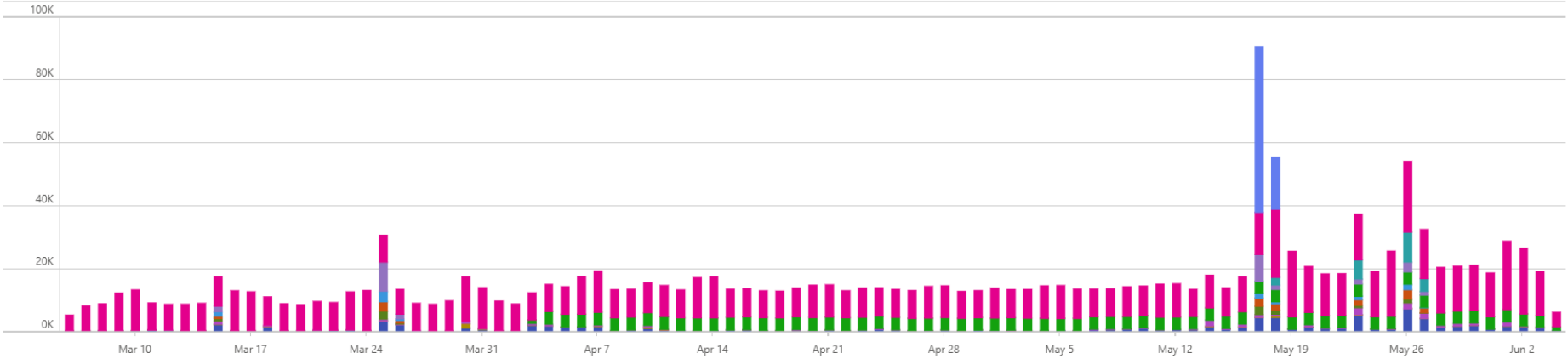
sentinel

Edit | Open | Help | Auto refresh: Off

Sentinel Data Dashboard

Timeframe: **Last 90 days** | DataType: **All**

Data Inflow Tables

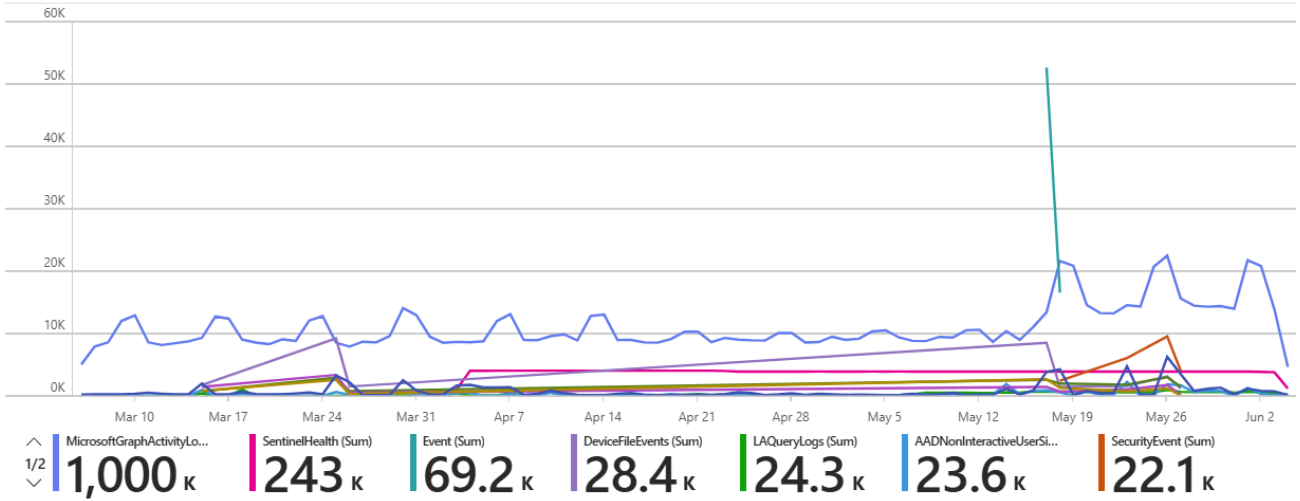


Event	MicrosoftGraphActivityLogs	SecurityEvent	DeviceFileEvents	SentinelHealth	DeviceRegistryEvents	DeviceEvents	DeviceFileCertificateInfo	AADNonInteractiveUserSi...	AzureActivity	Other
69.2 K	1.000 K	22.1 K	28.4 K	243 K	10.4 K	15.3 K	9.64 K	23.6 K	4.64 K	88.5 K

Table Information

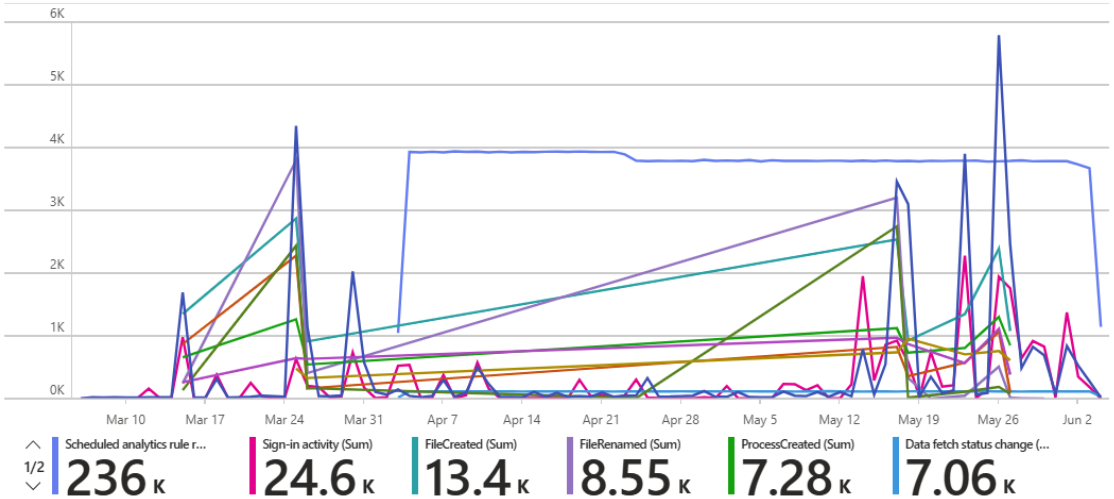
Most Active Tables

DataType	TotalEvents	GB
MicrosoftGraphActivityLogs	999583	
SentinelHealth	242995	
Event	69212	
DeviceFileEvents	28378	
LAQueryLogs	24313	
AADNonInteractiveUserSignInLogs	23646	
SecurityEvent	22055	
DeviceEvents	15334	
DeviceRegistryEvents	10410	
DeviceFileCertificateInfo	9644	



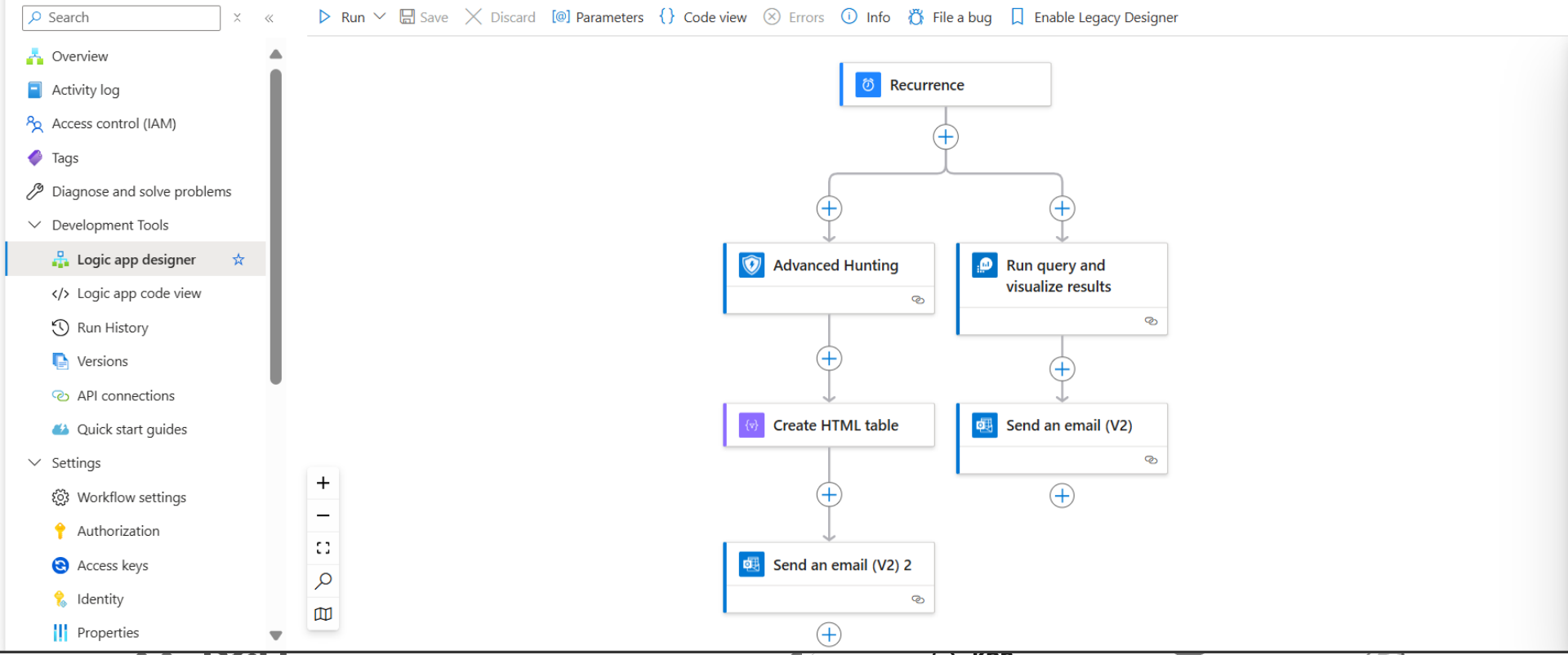
Most Active Action (Sub-Table)

Action	TotalEvents	DataType
Scheduled analytics rule run	235930	SentinelHealth
Sign-in activity	23646	AADNonInteractiveUserSignInLogs
FileCreated	13407	DeviceFileEvents
FileRenamed	8537	DeviceFileEvents
ProcessCreated	7283	DeviceProcessEvents
Data fetch status change	7056	SentinelHealth
RegistryValueSet	6238	DeviceRegistryEvents
FileDeleted	5871	DeviceFileEvents
ImageLoaded	5439	DeviceImageLoadEvents
LdapSearch	4570	DeviceEvents



Report-NewTableActionFound | Logic app designer

Logic app



BP

Bert-Jan Pals

To: Bert-Jan

Mon 6/3/2024 10:45 AM

Hello,

Herby the weekly report of new Actions found in the DataTables.

DataType	Action
SentinelHealth	Automation rule run
SentinelAudit	Microsoft.SecurityInsights/alertRules/Delete
OfficeActivity	SoftDelete
OfficeActivity	SearchQueryPerformed
OfficeActivity	ReactedToMessage
OfficeActivity	New-InboxRule
OfficeActivity	MessageReadReceiptReceived
OfficeActivity	MeetingParticipantDetail
OfficeActivity	MeetingDetail