ITASEC

Security operations modernized: Microsoft unified SIEM/SOAR and XDR approach

Rebecca Travasi & Antonio Formato
Technical Specialist Security & Compliance
Microsoft

April 2021

SIEM

Azure Sentinel

Multi-cloud

Partnerships

Microsoft Defender

XDR

SIEM

Azure Sentinel

Cloud native, any data, any entity

Multi-cloud

Partnerships

Cloud native

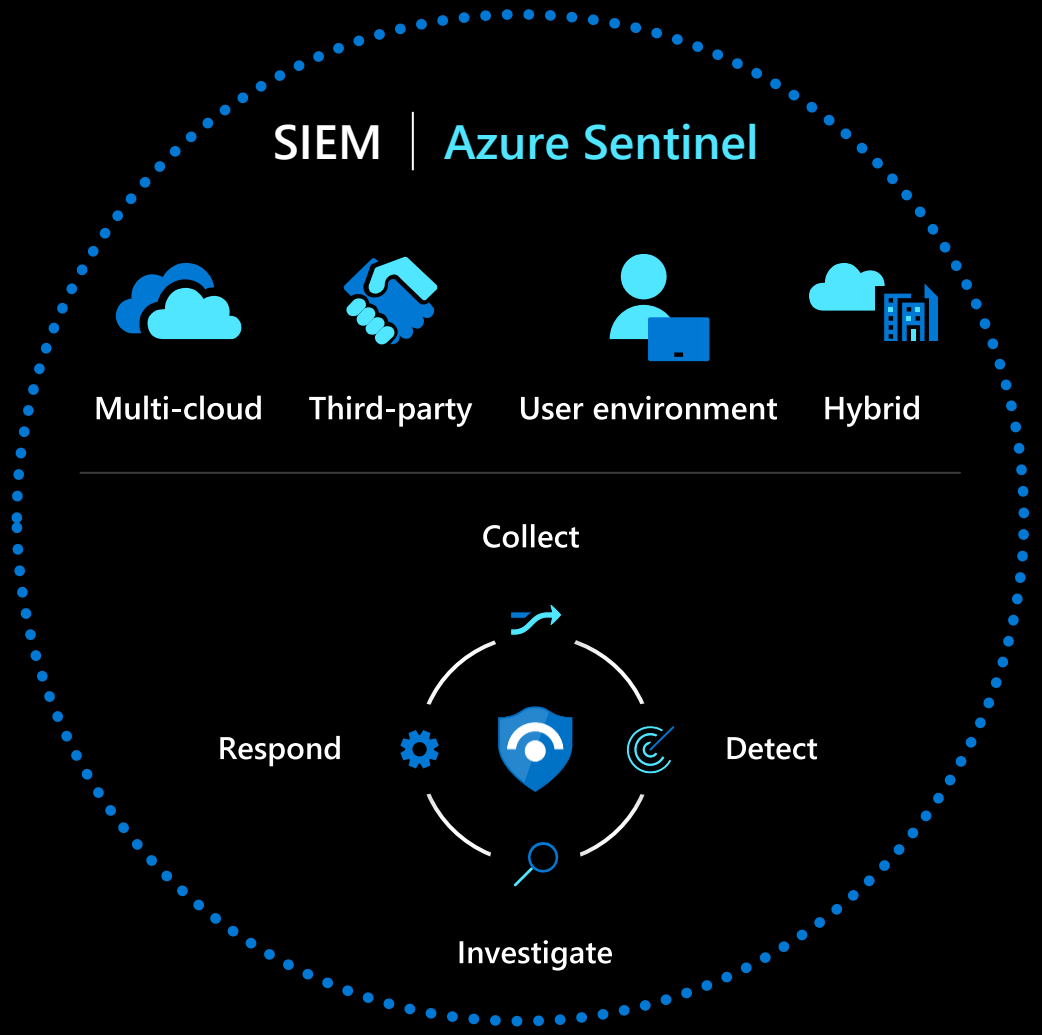
Any data

AI

Automation

Gain insights across your entire enterprise

Visualize and investigate the attack chain with cloud-native SIEM



- Collect security data at cloud scale and integrate with your existing tools
- Leverage AI to detect emergent threats and reduce alert fatigue by 90 percent
- Respond rapidly with built-in orchestration and automation

SIEM

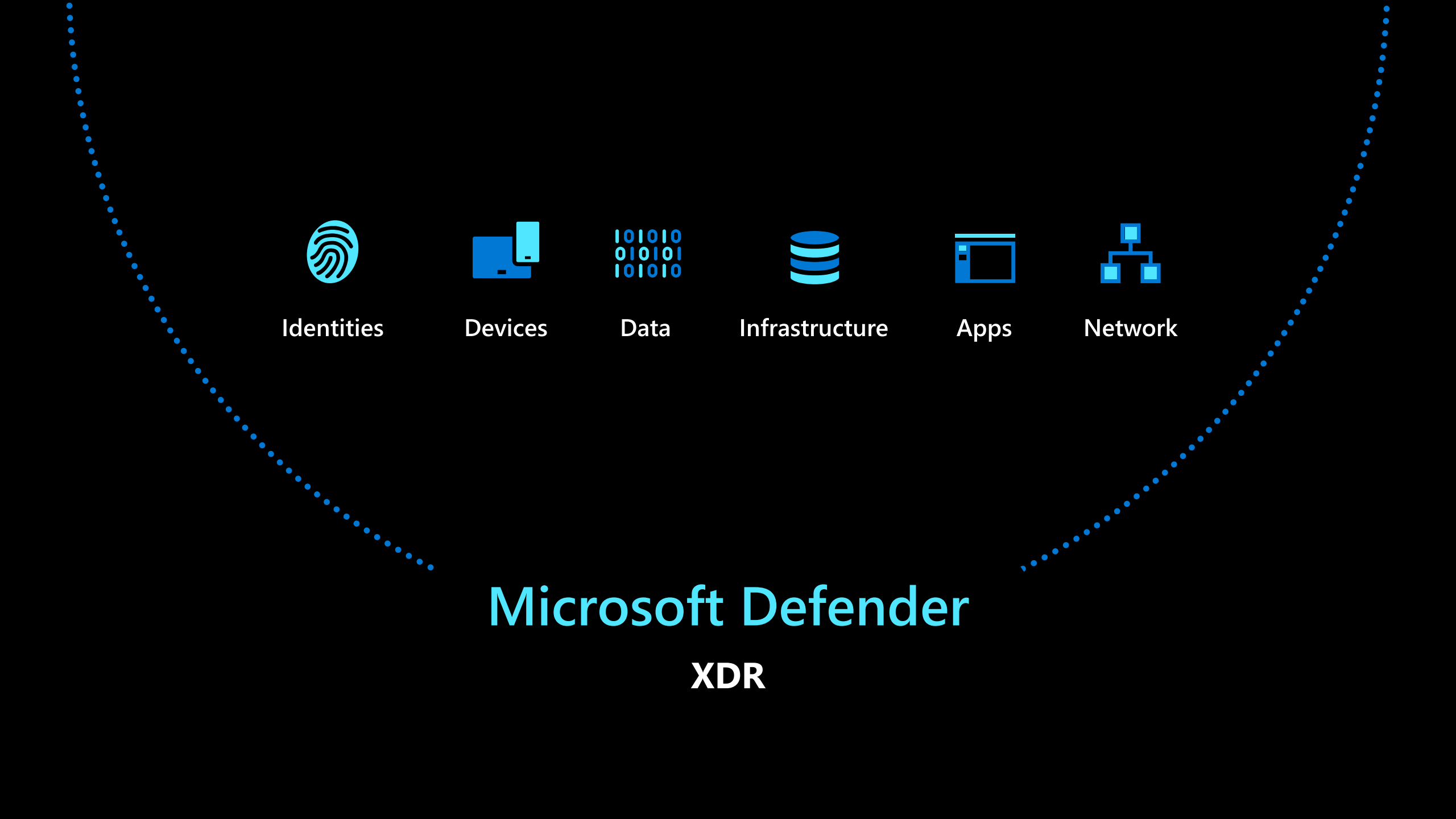
Azure Sentinel

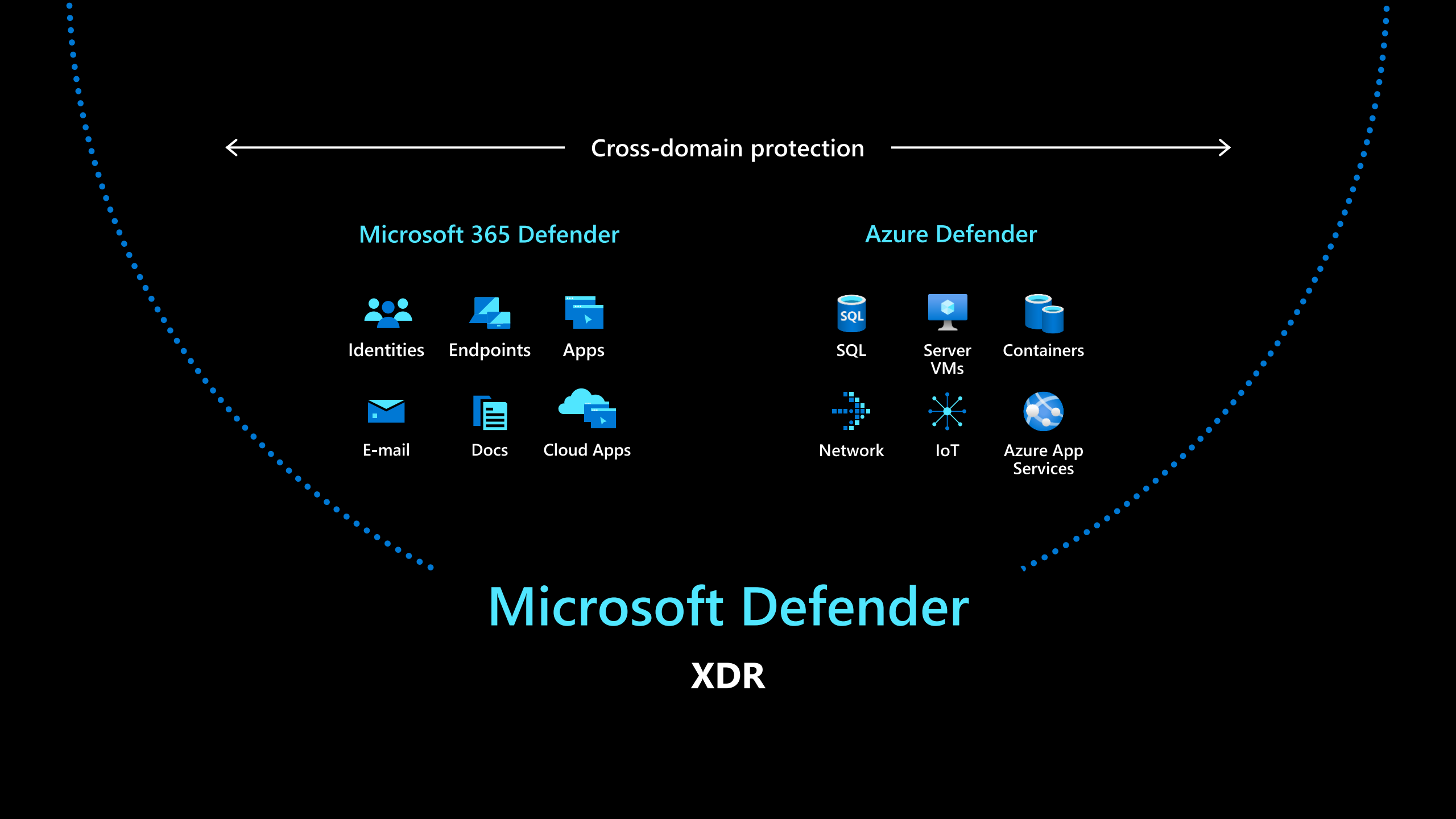
Multi-cloud

Partnerships

Microsoft Defender

XDR


Identities
Devices
Data
Infrastructure
Apps
Network
Microsoft Defender
XDR


Cross-domain protection
Microsoft 365 Defender
Identities
Endpoints
Apps
E-mail
Docs
Cloud Apps
Azure Defender
SQL
Server VMs
Containers
Network
IoT
Azure App Services
Microsoft Defender
XDR

Detect and respond across end-user environments

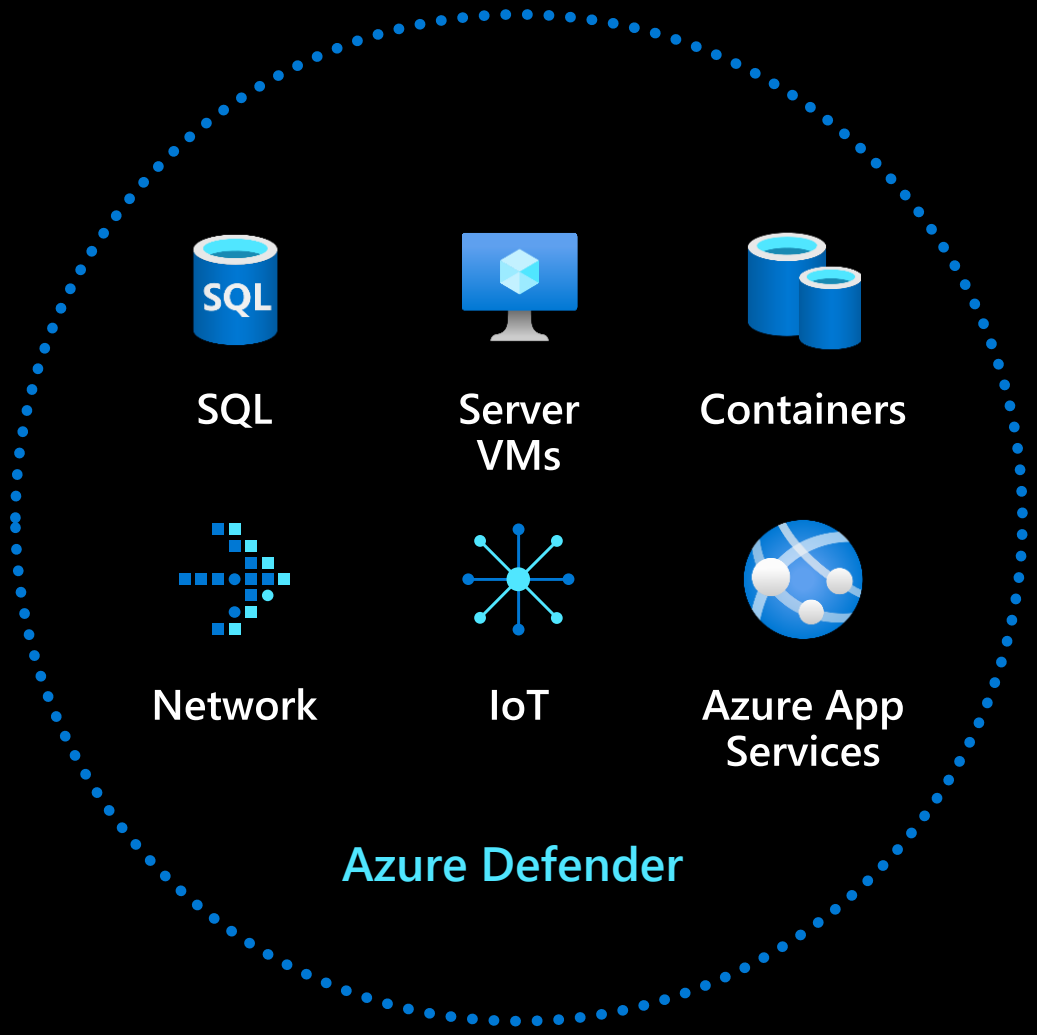
Prevent and detect threats, hunt for attacks, and coordinate response across domains

- Stop attacks before they occur by reducing your attack surface
- Detect and automate across domains, integrating threat data for rapid response
- Hunt across domains and create custom tools using your unique expertise
- View alerts and remediate across your Microsoft 365 environment in a single dashboard

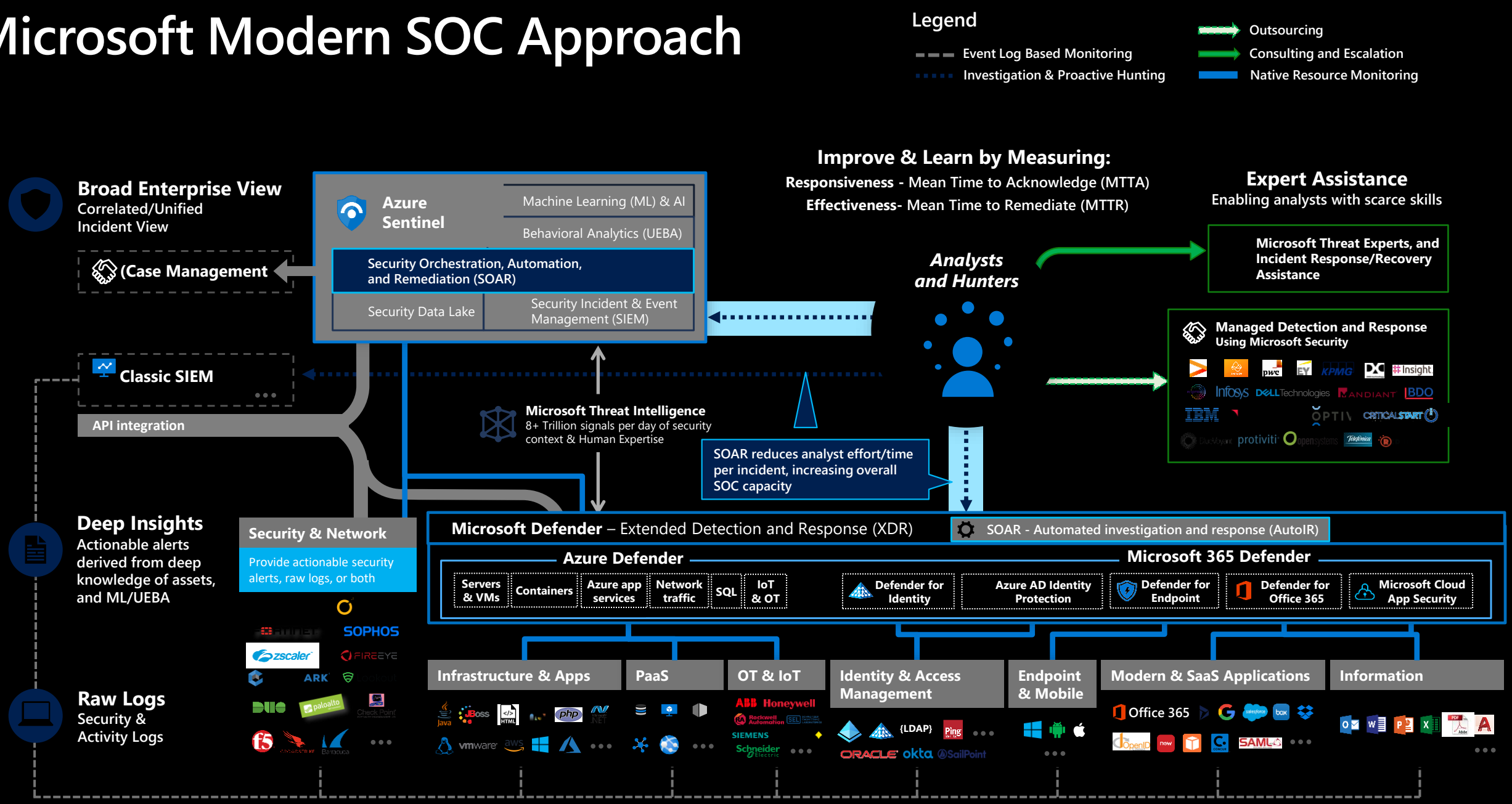
Intelligent detection and response for Azure and hybrid workloads

Use industry-leading threat intelligence to gain deep insights into your cloud workloads

- Protect data services, cloud native services, servers, and IoT from threats
- Extend protection to on-premises and multi-cloud for virtual machines and SQL databases using Azure Arc
- With prioritized alerts, focus on what matters the most



Microsoft Modern SOC Approach



SOC Model → automation role

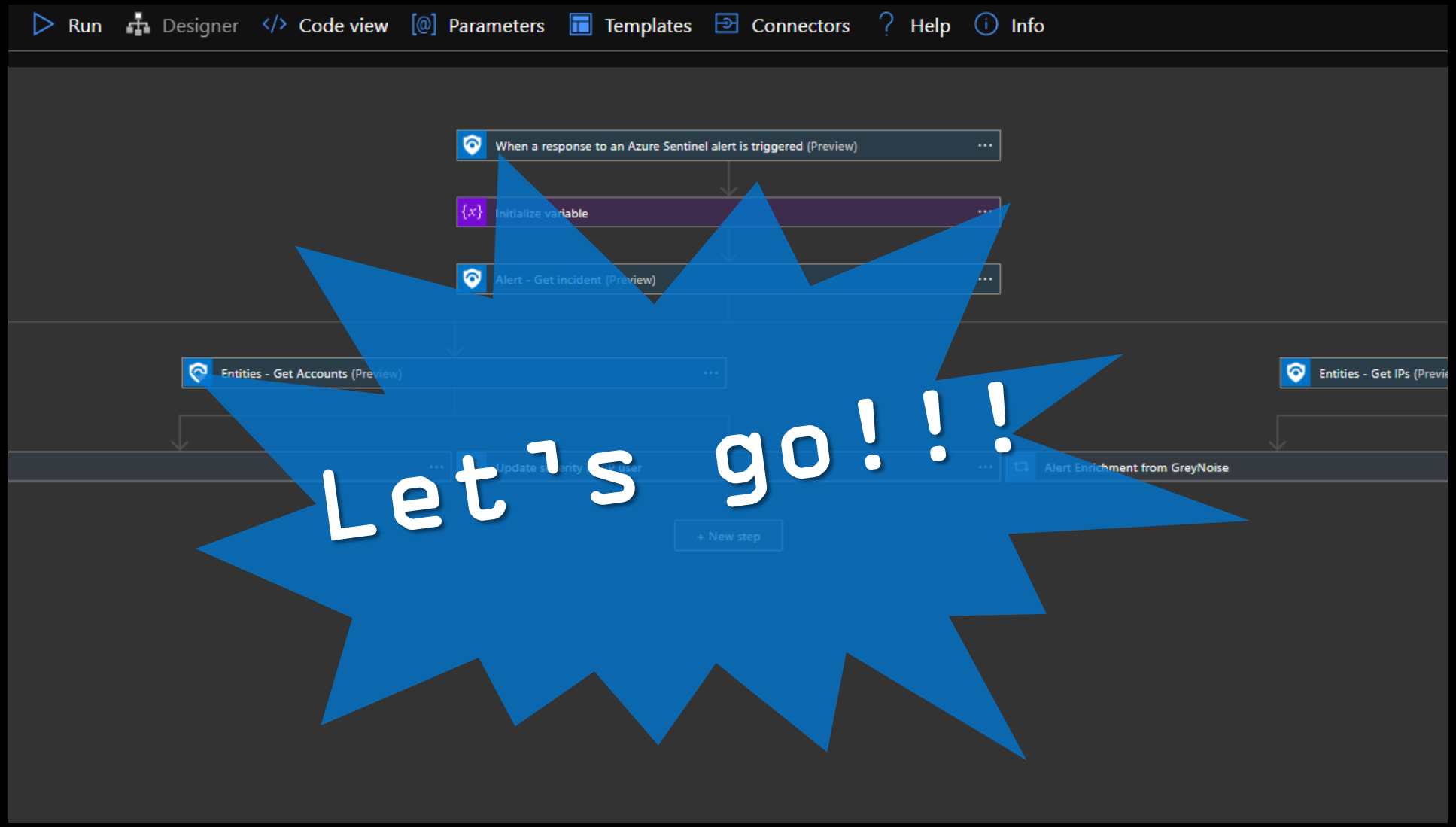
Empower humans with automation

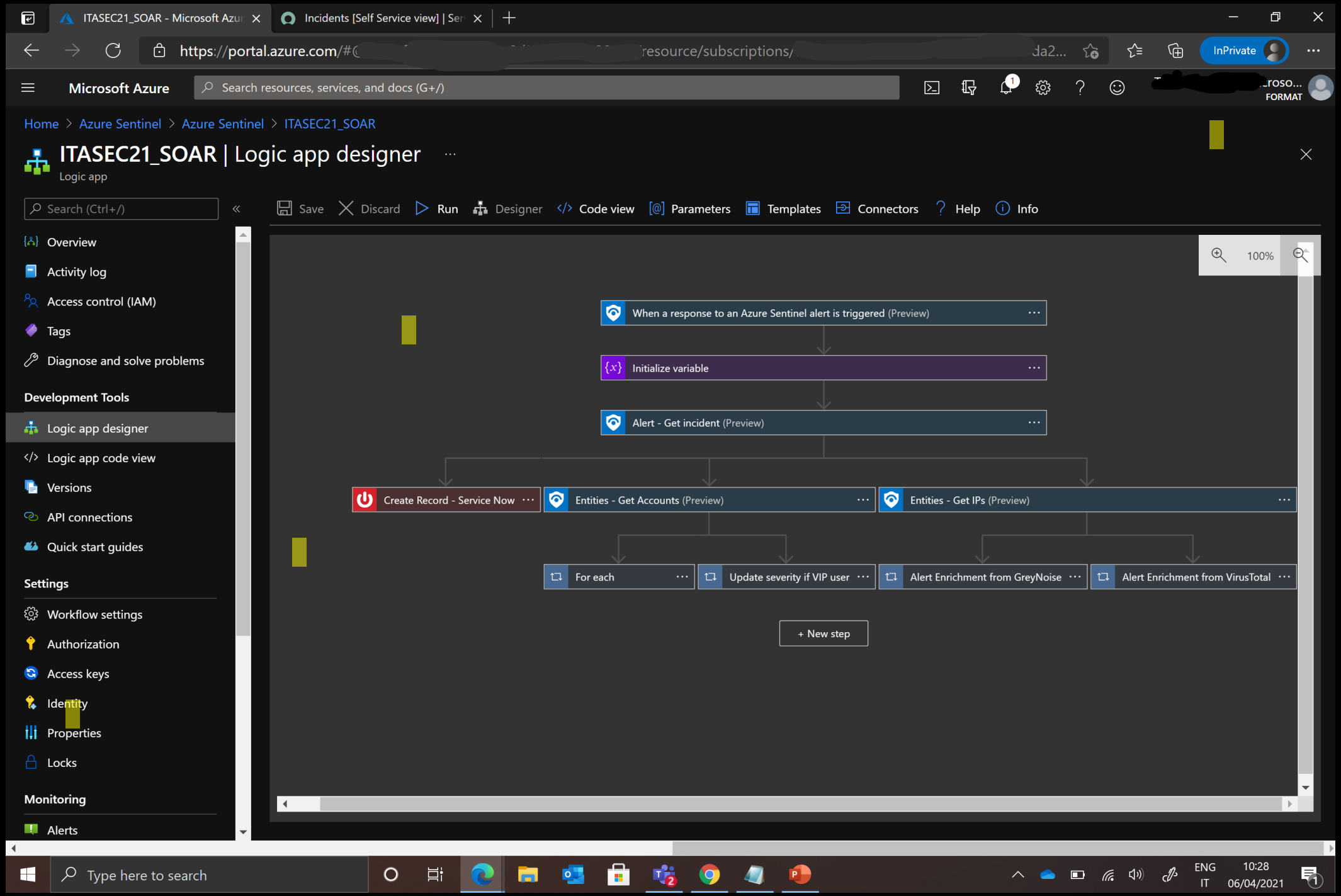
Automation is not about using efficiency to remove humans from the process—it is about empowering humans. We continuously think about how we can automate repetitive tasks from the analyst's job, so they can focus on the complex problems that people are uniquely able to solve.

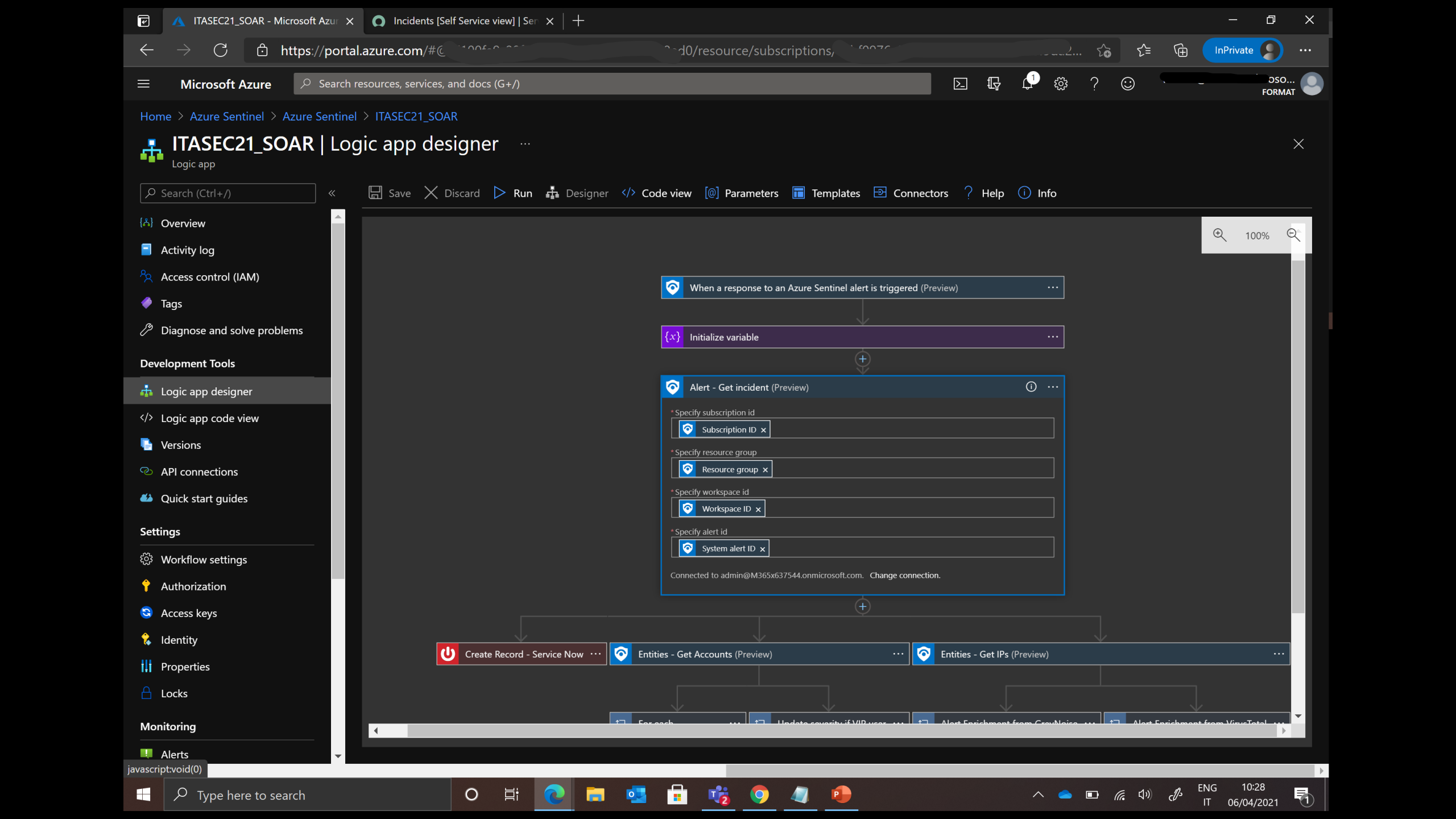
SOC Metrics

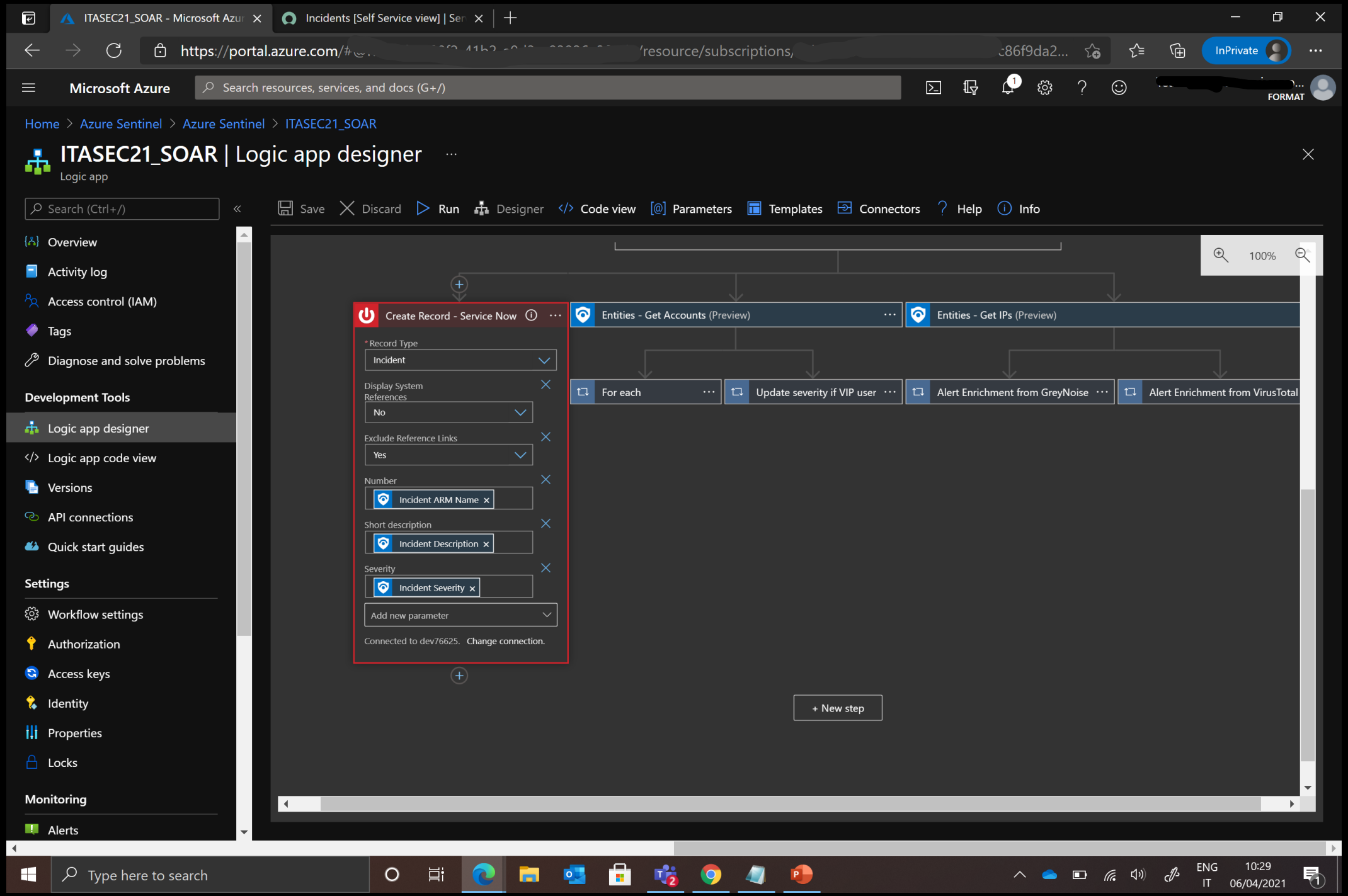
- Time to acknowledge (TtA)
- Time to remediate (TtR)
- Incidents remediated (manually/with automation)
- Escalations between each tier

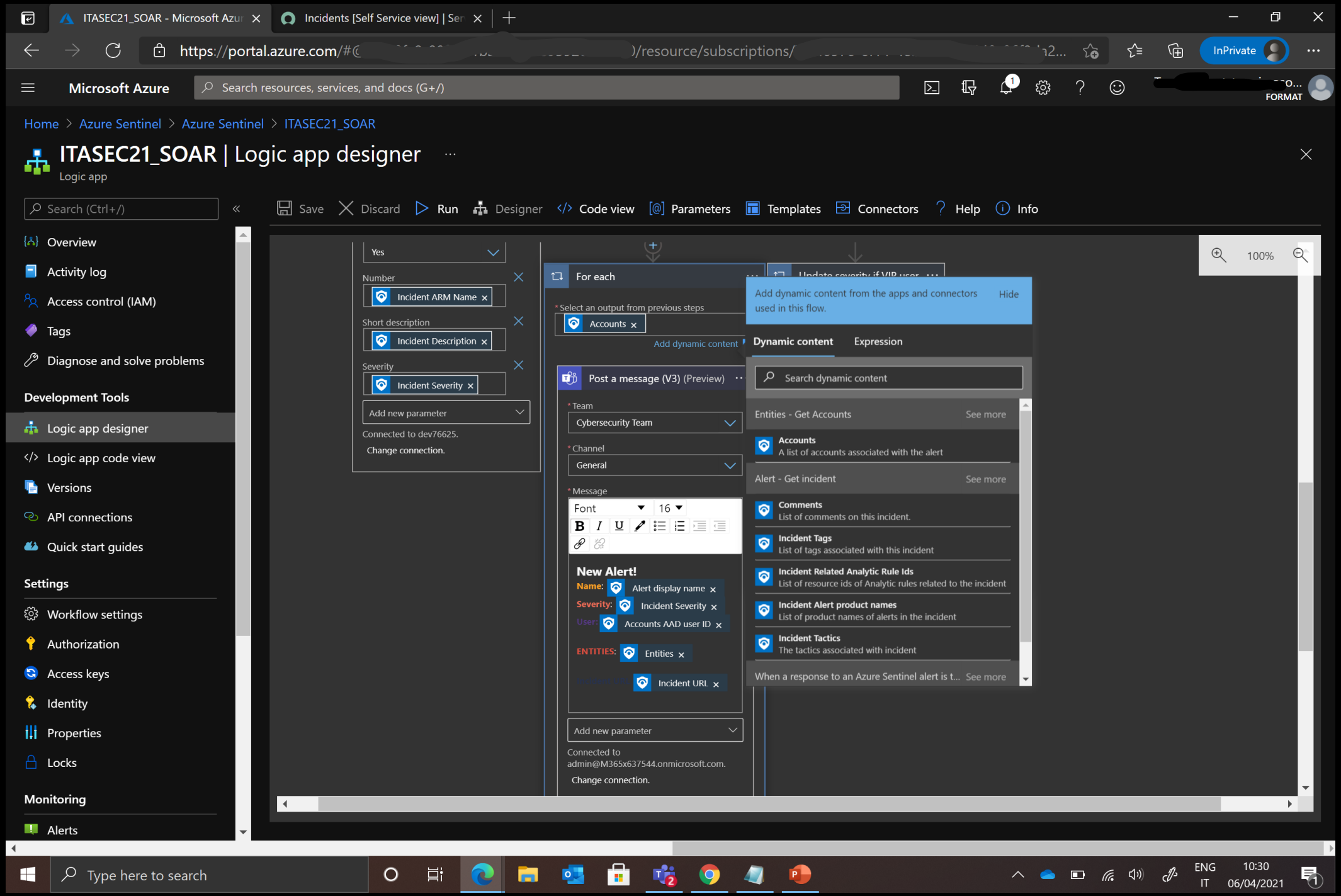
SOAR DEMO – custom playbook ITASEC21

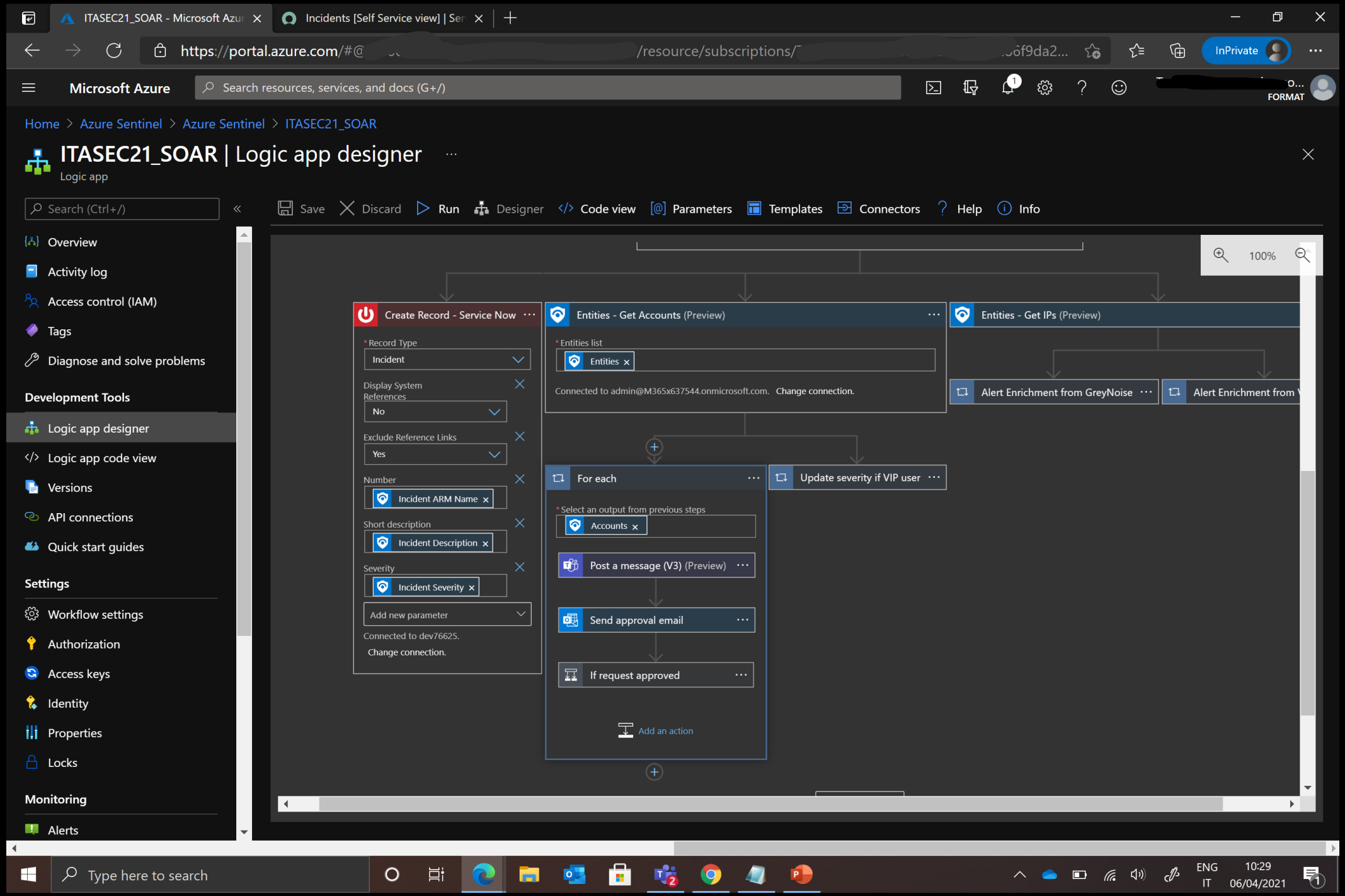


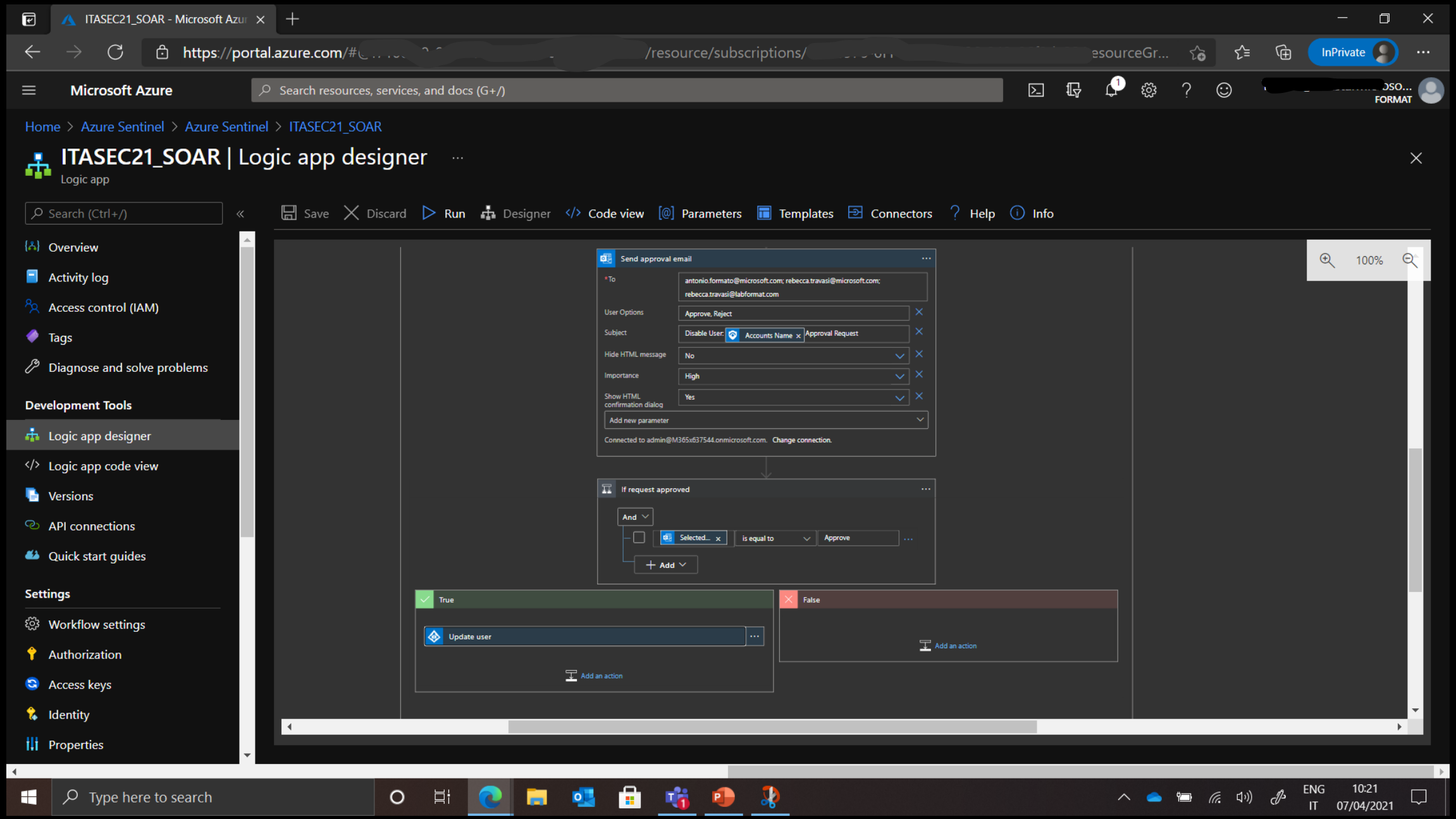

ITASEC21_SOAR - Microsoft Azu
Incidents [Self Service view] | Ser
https://portal.azure.com/#
resource/subscriptions/
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure Sentinel > Azure Sentinel > ITASEC21_SOAR
ITASEC21_SOAR | Logic app designer
Logic app
Search (Ctrl+/)
Save
Discard
Run
Designer
Code view
Parameters
Templates
Connectors
Help
Info
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Locks
Monitoring
Alerts
100%
When a response to an Azure Sentinel alert is triggered (Preview)
Initialize variable
Alert - Get incident (Preview)
Create Record - Service Now
Entities - Get Accounts (Preview)
Entities - Get IPs (Preview)
For each
Update severity if VIP user
Alert Enrichment from GreyNoise
Alert Enrichment from VirusTotal
+ New step
Type here to search
ENG
IT
10:28
06/04/2021

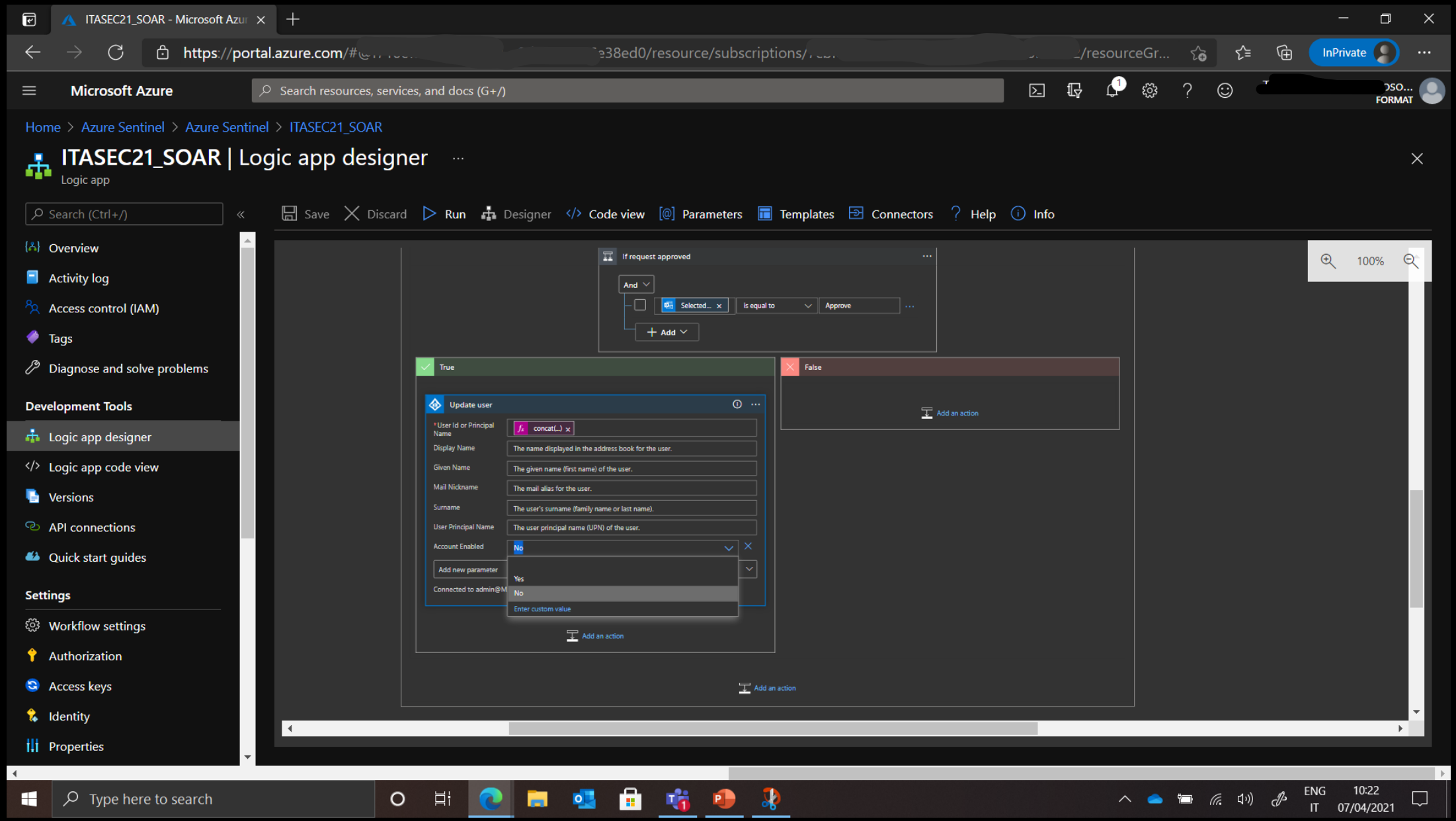

ITASEC21_SOAR - Microsoft Azur
Incidents [Self Service view] | Ser
https://portal.azure.com/#
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
FORMAT
Home > Azure Sentinel > Azure Sentinel > ITASEC21_SOAR
ITASEC21_SOAR | Logic app designer
Logic app
Search (Ctrl+/)
Save
Discard
Run
Designer
Code view
Parameters
Templates
Connectors
Help
Info
100%
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Locks
Monitoring
Alerts
When a response to an Azure Sentinel alert is triggered (Preview)
Initialize variable
Alert - Get incident (Preview)
* Specify subscription id
Subscription ID
* Specify resource group
Resource group
* Specify workspace id
Workspace ID
* Specify alert id
System alert ID
Connected to admin@M365x637544.onmicrosoft.com. Change connection.
Create Record - Service Now
Entities - Get Accounts (Preview)
Entities - Get IPs (Preview)
javascript:void(0)
Type here to search
ENG
IT
10:28
06/04/2021

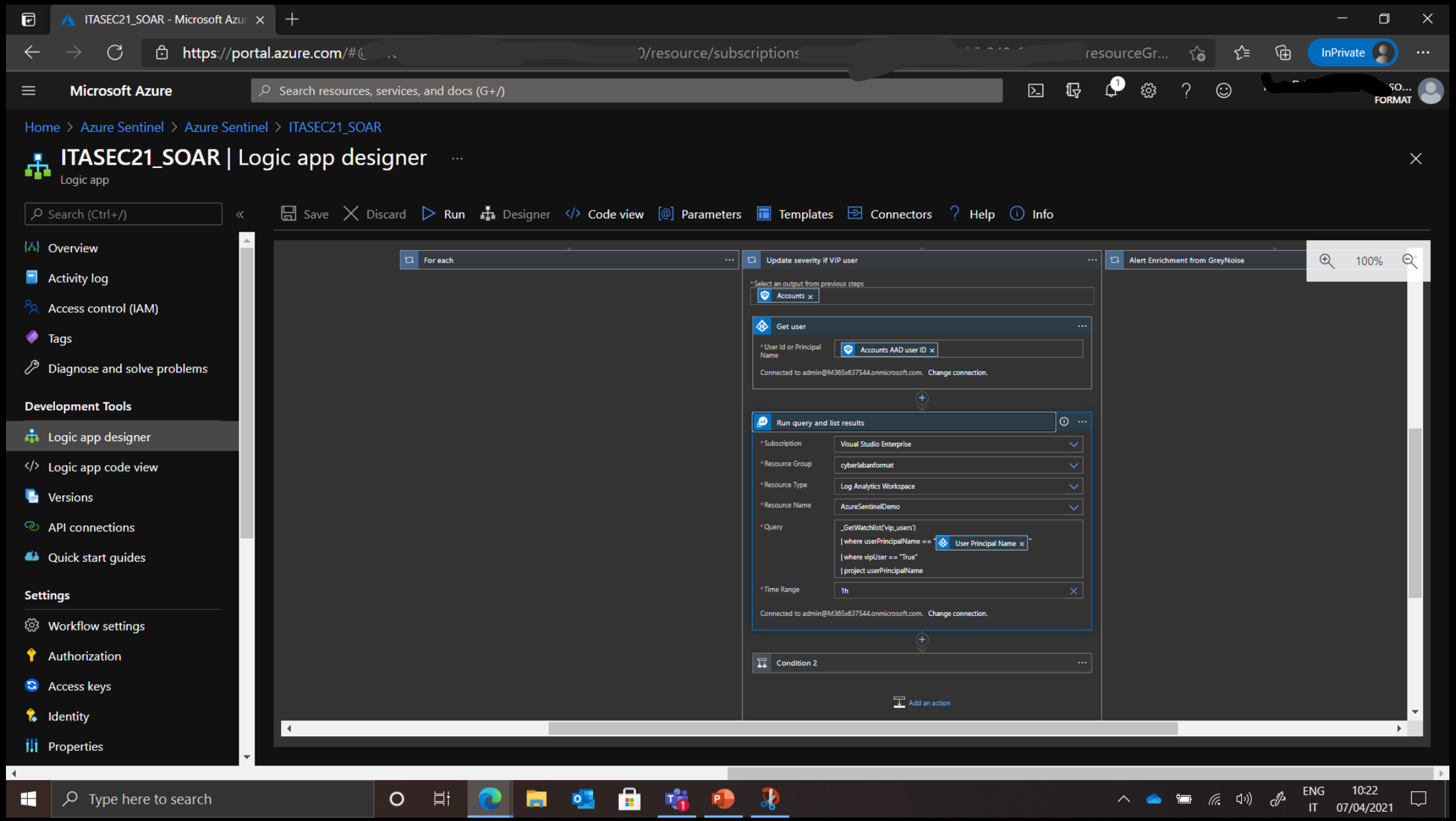

ITASEC21_SOAR - Microsoft Azur
Incidents [Self Service view] | Ser
https://portal.azure.com/#
/resource/subscriptions/
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
FORMAT
Home > Azure Sentinel > Azure Sentinel > ITASEC21_SOAR
ITASEC21_SOAR | Logic app designer
Logic app
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Locks
Monitoring
Alerts
Save
Discard
Run
Designer
Code view
Parameters
Templates
Connectors
Help
Info
100%
Create Record - Service Now
Record Type
Incident
Display System References
No
Exclude Reference Links
Yes
Number
Incident ARM Name
Short description
Incident Description
Severity
Incident Severity
Add new parameter
Connected to dev76625. Change connection.
Entities - Get Accounts (Preview)
Entities - Get IPs (Preview)
For each
Update severity if VIP user
Alert Enrichment from GreyNoise
Alert Enrichment from VirusTotal
+ New step
Type here to search
ENG
IT
10:29
06/04/2021

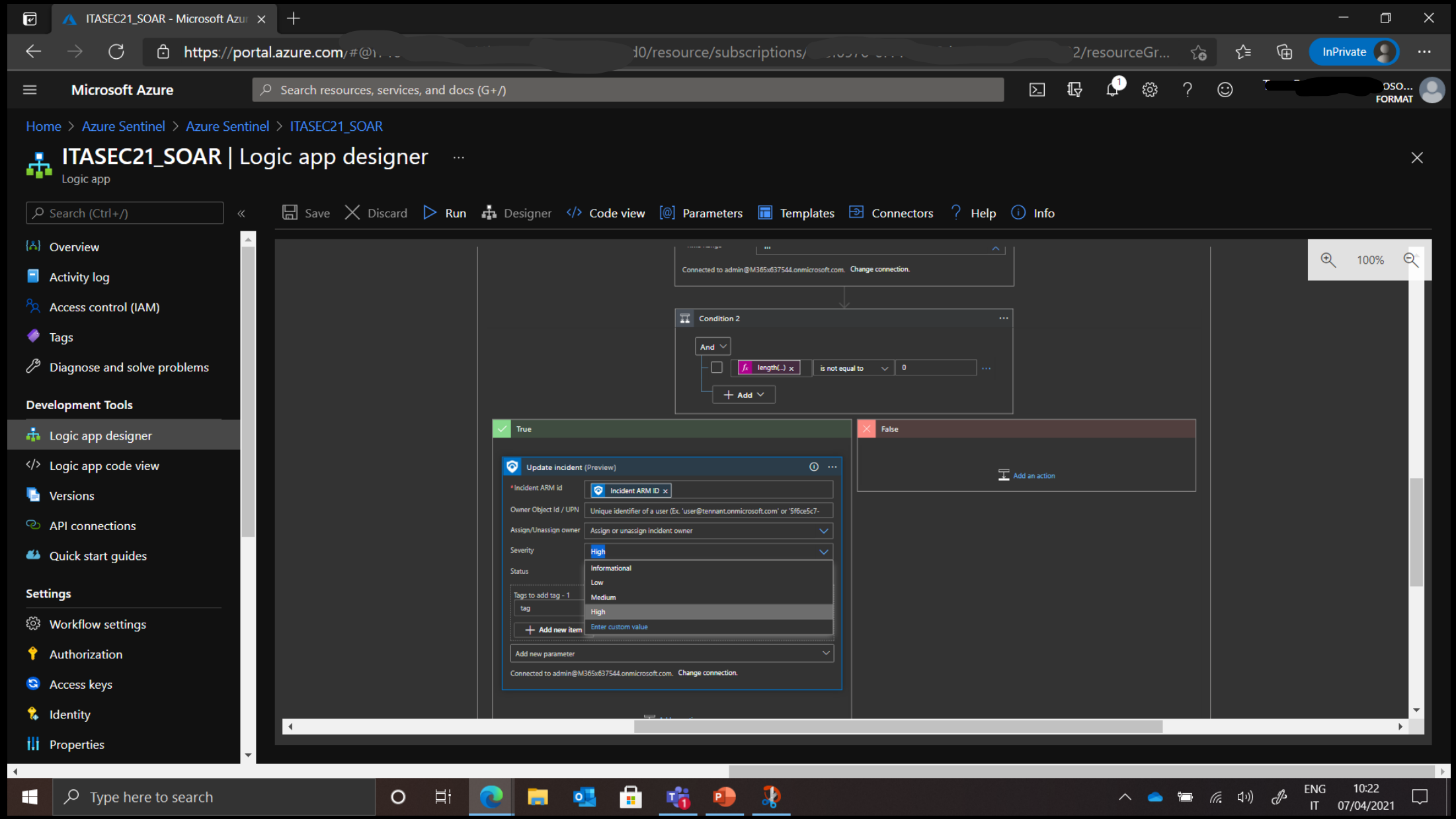

ITASEC21_SOAR - Microsoft Azu
Incidents [Self Service view] | Ser
https://portal.azure.com/#
/resource/subscriptions/
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
FORMAT
Home > Azure Sentinel > Azure Sentinel > ITASEC21_SOAR
ITASEC21_SOAR | Logic app designer
Logic app
Search (Ctrl+/)
Save
Discard
Run
Designer
Code view
Parameters
Templates
Connectors
Help
Info
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Locks
Monitoring
Alerts
Yes
Number
Incident ARM Name
Short description
Incident Description
Severity
Incident Severity
Add new parameter
Connected to dev76625.
Change connection.
For each
Select an output from previous steps
Accounts
Add dynamic content
Post a message (V3) (Preview)
Team
Cybersecurity Team
Channel
General
Message
Font
16
New Alert!
Name:
Alert display name
Severity:
Incident Severity
User:
Accounts AAD user ID
ENTITIES:
Entities
Incident URL
Add new parameter
Connected to admin@M365x637544.onmicrosoft.com.
Change connection.
Add dynamic content from the apps and connectors used in this flow.
Hide
Dynamic content
Expression
Search dynamic content
Entities - Get Accounts
See more
Accounts
A list of accounts associated with the alert
Alert - Get incident
See more
Comments
List of comments on this incident.
Incident Tags
List of tags associated with this incident
Incident Related Analytic Rule Ids
List of resource ids of Analytic rules related to the incident
Incident Alert product names
List of product names of alerts in the incident
Incident Tactics
The tactics associated with incident
When a response to an Azure Sentinel alert is t...
See more
100%
Type here to search
ENG
IT
10:30
06/04/2021

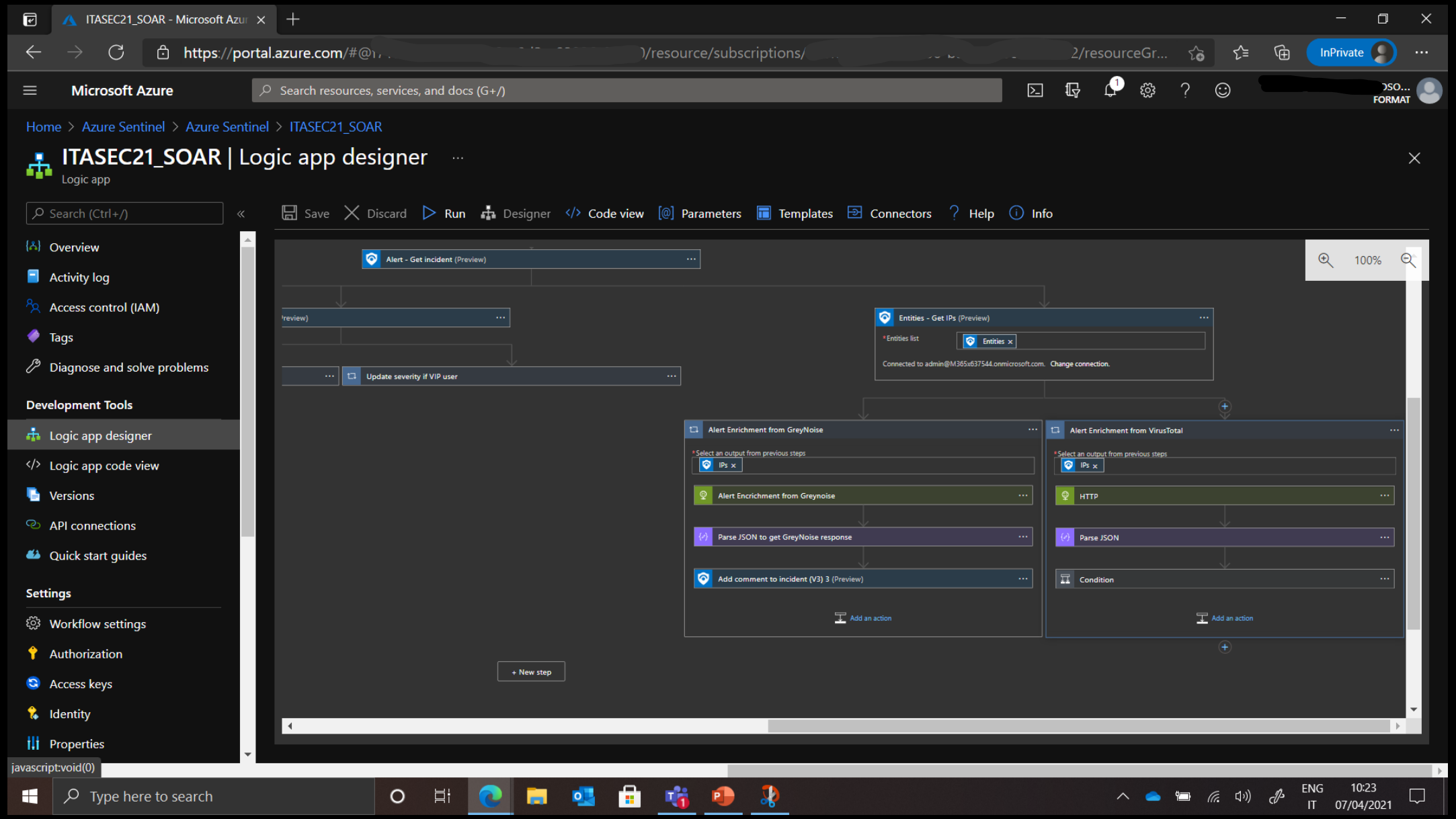

ITASEC21_SOAR - Microsoft Azur
Incidents [Self Service view] | Ser
https://portal.azure.com/#@
/resource/subscriptions/
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
FORMAT
Home > Azure Sentinel > Azure Sentinel > ITASEC21_SOAR
ITASEC21_SOAR | Logic app designer
Logic app
Search (Ctrl+/)
Save
Discard
Run
Designer
Code view
Parameters
Templates
Connectors
Help
Info
100%
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Locks
Monitoring
Alerts
Create Record - Service Now
* Record Type
Incident
Display System References
No
Exclude Reference Links
Yes
Number
Incident ARM Name
Short description
Incident Description
Severity
Incident Severity
Add new parameter
Connected to dev76625.
Change connection.
Entities - Get Accounts (Preview)
* Entities list
Entities
Connected to admin@M365x637544.onmicrosoft.com. Change connection.
Entities - Get IPs (Preview)
Alert Enrichment from GreyNoise
Alert Enrichment from
For each
* Select an output from previous steps
Accounts
Post a message (V3) (Preview)
Send approval email
If request approved
Add an action
Update severity if VIP user
Type here to search
ENG
IT
10:29
06/04/2021

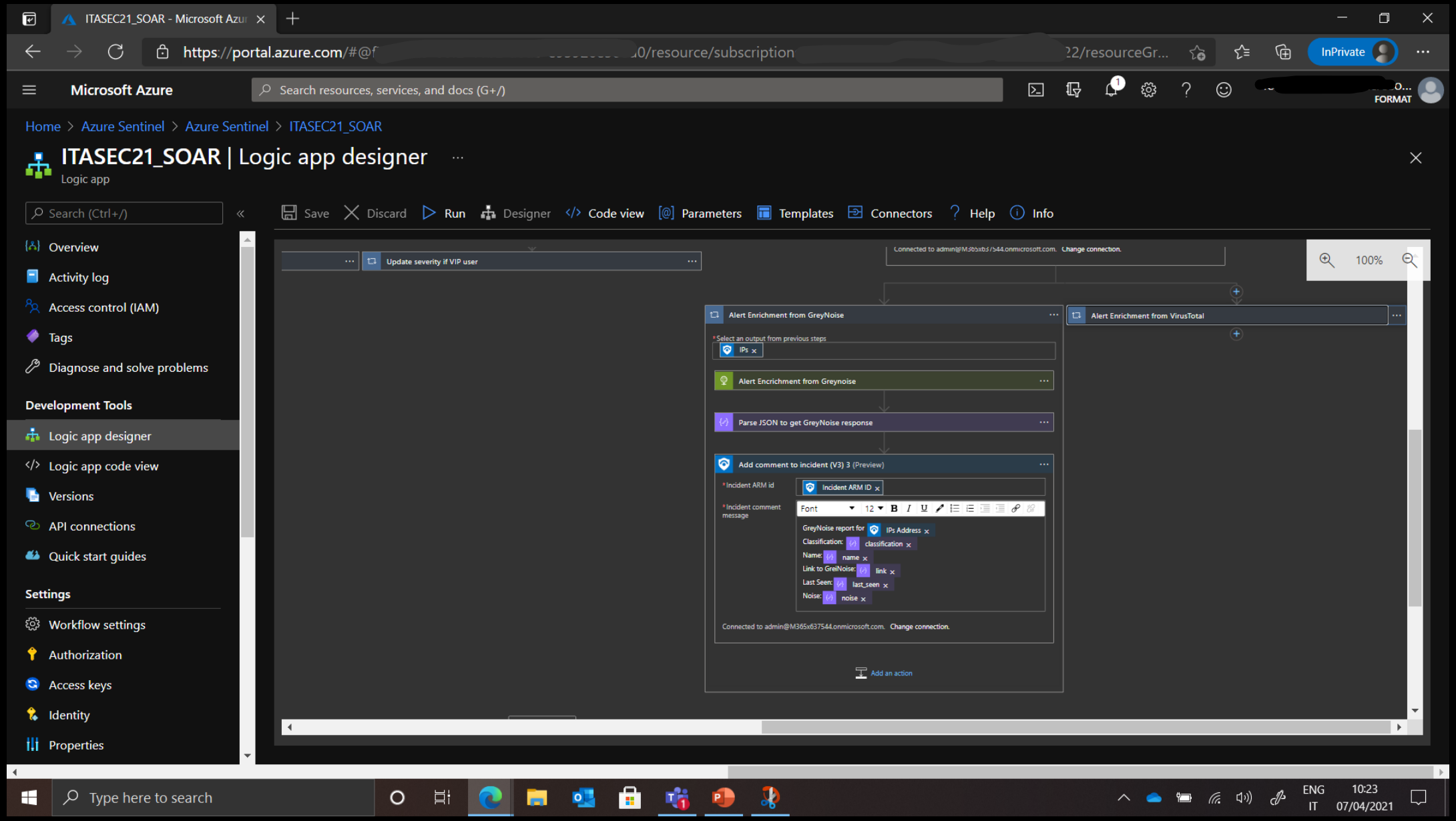

ITASEC21_SOAR - Microsoft Azur
https://portal.azure.com/#
/resource/subscriptions/
esourceGr...
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
FORMAT
Home > Azure Sentinel > Azure Sentinel > ITASEC21_SOAR
ITASEC21_SOAR | Logic app designer
Logic app
Search (Ctrl+/)
Save
Discard
Run
Designer
Code view
Parameters
Templates
Connectors
Help
Info
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Send approval email
*To
antonio.formato@microsoft.com; rebecca.travasi@microsoft.com; rebecca.travasi@labformat.com
User Options
Approve, Reject
Subject
Disable User: Accounts Name Approval Request
Hide HTML message
No
Importance
High
Show HTML confirmation dialog
Yes
Add new parameter
Connected to admin@M365x637544.onmicrosoft.com. Change connection.
If request approved
And
Selected...
is equal to
Approve
Add
True
Update user
Add an action
False
Add an action
100%
Type here to search
ENG
IT
10:21
07/04/2021

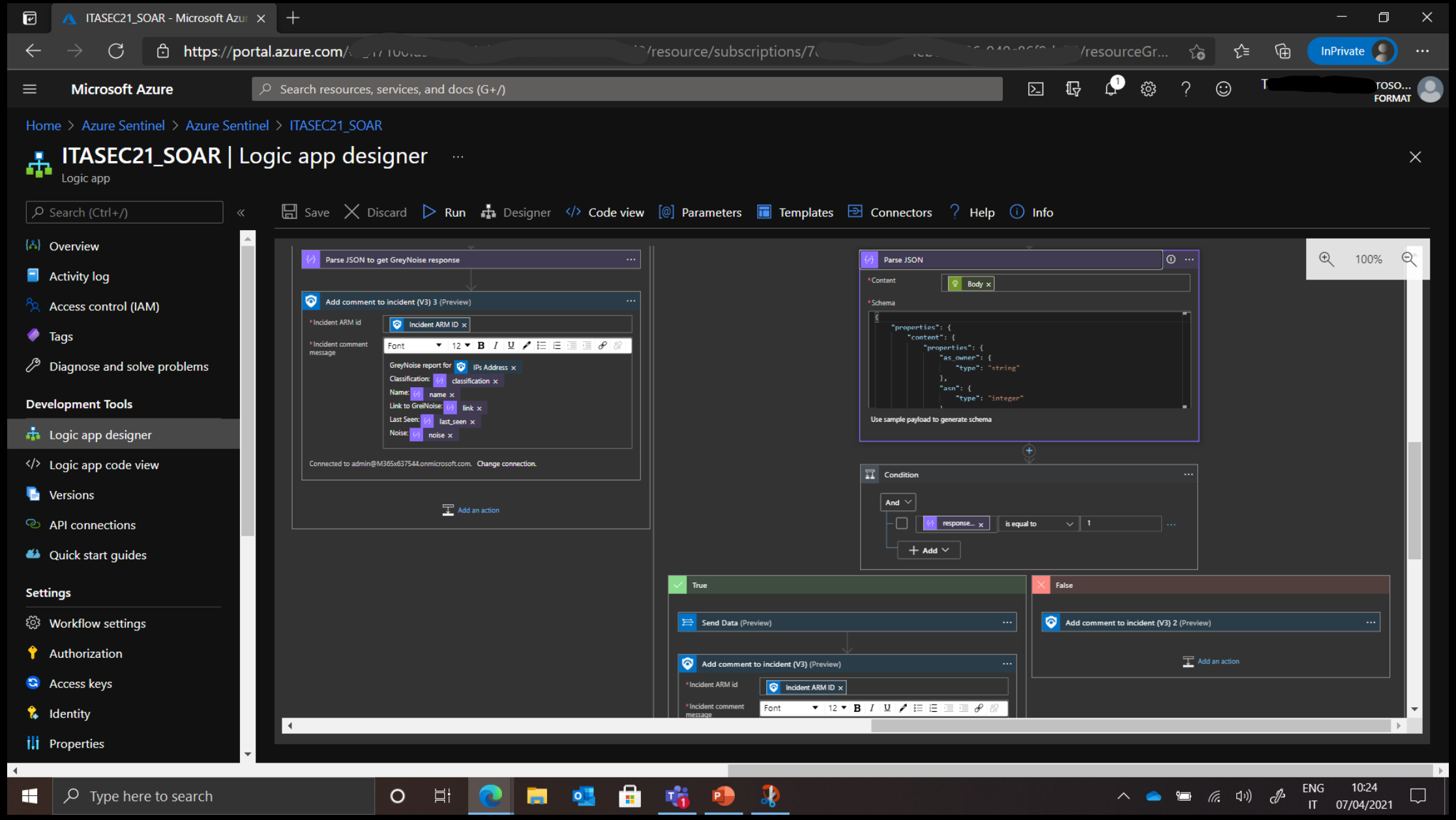

ITASEC21_SOAR - Microsoft Azur
https://portal.azure.com/#
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure Sentinel > Azure Sentinel > ITASEC21_SOAR
ITASEC21_SOAR | Logic app designer
Logic app
Search (Ctrl+/)
Save
Discard
Run
Designer
Code view
Parameters
Templates
Connectors
Help
Info
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
If request approved
And
Selected...
is equal to
Approve
Add
True
False
Update user
User Id or Principal Name
concat(...)
Display Name
The name displayed in the address book for the user.
Given Name
The given name (first name) of the user.
Mail Nickname
The mail alias for the user.
Surname
The user's surname (family name or last name).
User Principal Name
The user principal name (UPN) of the user.
Account Enabled
No
Yes
No
Enter custom value
Add new parameter
Add an action
100%
Type here to search
ENG
IT
10:22
07/04/2021


ITASEC21_SOAR - Microsoft Azur
https://portal.azure.com/#
/resource/subscriptions
resourceGr...
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
FORMAT
Home > Azure Sentinel > Azure Sentinel > ITASEC21_SOAR
ITASEC21_SOAR | Logic app designer
Logic app
Search (Ctrl+/)
Save
Discard
Run
Designer
Code view
Parameters
Templates
Connectors
Help
Info
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
For each
Update severity if VIP user
Alert Enrichment from GreyNoise
100%
Select an output from previous steps
Accounts
Get user
User Id or Principal Name
Accounts AAD user ID
Connected to admin@M365x637544.onmicrosoft.com. Change connection.
Run query and list results
Subscription
Visual Studio Enterprise
Resource Group
cyberlabanformat
Resource Type
Log Analytics Workspace
Resource Name
AzureSentinelDemo
Query
_GetWatchlist('vip_users')
| where userPrincipalName ==
User Principal Name
| where vipUser == "True"
| project userPrincipalName
Time Range
1h
Connected to admin@M365x637544.onmicrosoft.com. Change connection.
Condition 2
Add an action
Type here to search
ENG
IT
10:22
07/04/2021


ITASEC21_SOAR - Microsoft Azu
https://portal.azure.com/#@
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure Sentinel > Azure Sentinel > ITASEC21_SOAR
ITASEC21_SOAR | Logic app designer
Logic app
Search (Ctrl+/)
Save
Discard
Run
Designer
Code view
Parameters
Templates
Connectors
Help
Info
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Connected to admin@M365x637544.onmicrosoft.com. Change connection.
Condition 2
And
length(...)
is not equal to
0
Add
True
False
Update incident (Preview)
Incident ARM id
Incident ARM ID
Owner Object Id / UPN
Unique identifier of a user (Ex: 'user@tennant.onmicrosoft.com' or '5f6ce5c7-
Assign/Unassign owner
Assign or unassign incident owner
Severity
High
Informational
Low
Medium
High
Enter custom value
Status
Tags to add tag - 1
tag
Add new item
Add new parameter
Connected to admin@M365x637544.onmicrosoft.com. Change connection.
Add an action
100%
Type here to search
ENG
IT
10:22
07/04/2021


ITASEC21_SOAR - Microsoft Azur
https://portal.azure.com/#@
)/resource/subscriptions/
2/resourceGr...
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
FORMAT
Home > Azure Sentinel > Azure Sentinel > ITASEC21_SOAR
ITASEC21_SOAR | Logic app designer
Logic app
Search (Ctrl+/)
Save
Discard
Run
Designer
Code view
Parameters
Templates
Connectors
Help
Info
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Alert - Get incident (Preview)
Update severity if VIP user
Entities - Get IPs (Preview)
*Entities list
Entities
Connected to admin@M365x637544.onmicrosoft.com. Change connection.
Alert Enrichment from GreyNoise
*Select an output from previous steps
IPs
Alert Encrichment from Greynoise
Parse JSON to get GreyNoise response
Add comment to incident (V3) 3 (Preview)
Add an action
Alert Enrichment from VirusTotal
*Select an output from previous steps
IPs
HTTP
Parse JSON
Condition
Add an action
+ New step
100%
javascript:void(0)
Type here to search
ENG
IT
10:23
07/04/2021


ITASEC21_SOAR - Microsoft Azur
https://portal.azure.com/#@f 0/resource/subscription 22/resourceGr...
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
FORMAT
Home > Azure Sentinel > Azure Sentinel > ITASEC21_SOAR
ITASEC21_SOAR | Logic app designer
Logic app
Search (Ctrl+/)
Save
Discard
Run
Designer
Code view
Parameters
Templates
Connectors
Help
Info
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Update severity if VIP user
Connected to admin@M365x637544.onmicrosoft.com. Change connection.
100%
Alert Enrichment from GreyNoise
Alert Enrichment from VirusTotal
Select an output from previous steps
IPs
Alert Encrichment from Greynoise
Parse JSON to get GreyNoise response
Add comment to incident (V3) 3 (Preview)
Incident ARM id
Incident ARM ID
Incident comment message
Font
GreyNoise report for IPs Address
Classification: classification
Name: name
Link to GreiNoise: link
Last Seen: last_seen
Noise: noise
Connected to admin@M365x637544.onmicrosoft.com. Change connection.
Add an action
Type here to search
ENG
IT
10:23
07/04/2021


ITASEC21_SOAR - Microsoft Azu
https://portal.azure.com/
/resource/subscriptions/7
/resourceGr...
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure Sentinel > Azure Sentinel > ITASEC21_SOAR
ITASEC21_SOAR | Logic app designer
Logic app
Search (Ctrl+/)
Save
Discard
Run
Designer
Code view
Parameters
Templates
Connectors
Help
Info
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Parse JSON to get GreyNoise response
Add comment to incident (V3) 3 (Preview)
Incident ARM id
Incident ARM ID
Incident comment message
GreyNoise report for
IPs Address
Classification:
classification
Name:
name
Link to GreiNoise:
link
Last Seen:
last_seen
Noise:
noise
Connected to admin@M365x637544.onmicrosoft.com. Change connection.
Add an action
Parse JSON
Content
Body
Schema
"properties": {
"content": {
"properties": {
"as_owner": {
"type": "string"
},
"asn": {
"type": "integer"
Use sample payload to generate schema
100%
Condition
And
response...
is equal to
1
Add
True
False
Send Data (Preview)
Add comment to incident (V3) (Preview)
Add comment to incident (V3) 2 (Preview)
Add an action
Type here to search
ENG
IT
10:24
07/04/2021

SCAN ME!

QR Code to Playbook Template on GitHub

Domande?
Unmute o scrivici su Slack
#stakeholder-space

Rebecca Travasi
rebecca.travasi@microsoft.com
https://www.linkedin.com/in/rebeccatravasi/

Antonio Formato
antonio.formato@microsoft.com
https://www.linkedin.com/in/antonioformato/

Thank you