

AUTOMATED INVESTIGATION AND RESPONSE WITHIN MICROSOFT

365

Liam Cleary

ABOUT ME

LIAM CLEARY | CEO @ SHAREPLICITY

MICROSOFT MVP (16 YEARS)

MICROSOFT CERTIFIED TRAINER

FOCUS ON MICROSOFT 365 AND AZURE
ARCHITECTURE, SECURITY AND COMPLIANCE,
AND DEVELOPMENT

CREATE ONLINE TRAINING COURSES AT
PLURALSIGHT, AND LINKEDIN LEARNING, AS
WELL AS TEACHING ONLINE CERTIFICATION
COURSES

I LIKE TO RUN, MOUNTAIN BIKE, AND I COACH
BOYS U12 SOCCER



www.helloitsliam.com



www.linkedin.com/in/liamcleary



twitter.com/helloitsliam

AGENDA

1

INTRODUCTION TO AUTOMATED INVESTIGATION AND RESPONSE (AIR)

2

AUTOMATED INVESTIGATION AND RESPONSE (AIR)
WITHIN MICROSOFT 365

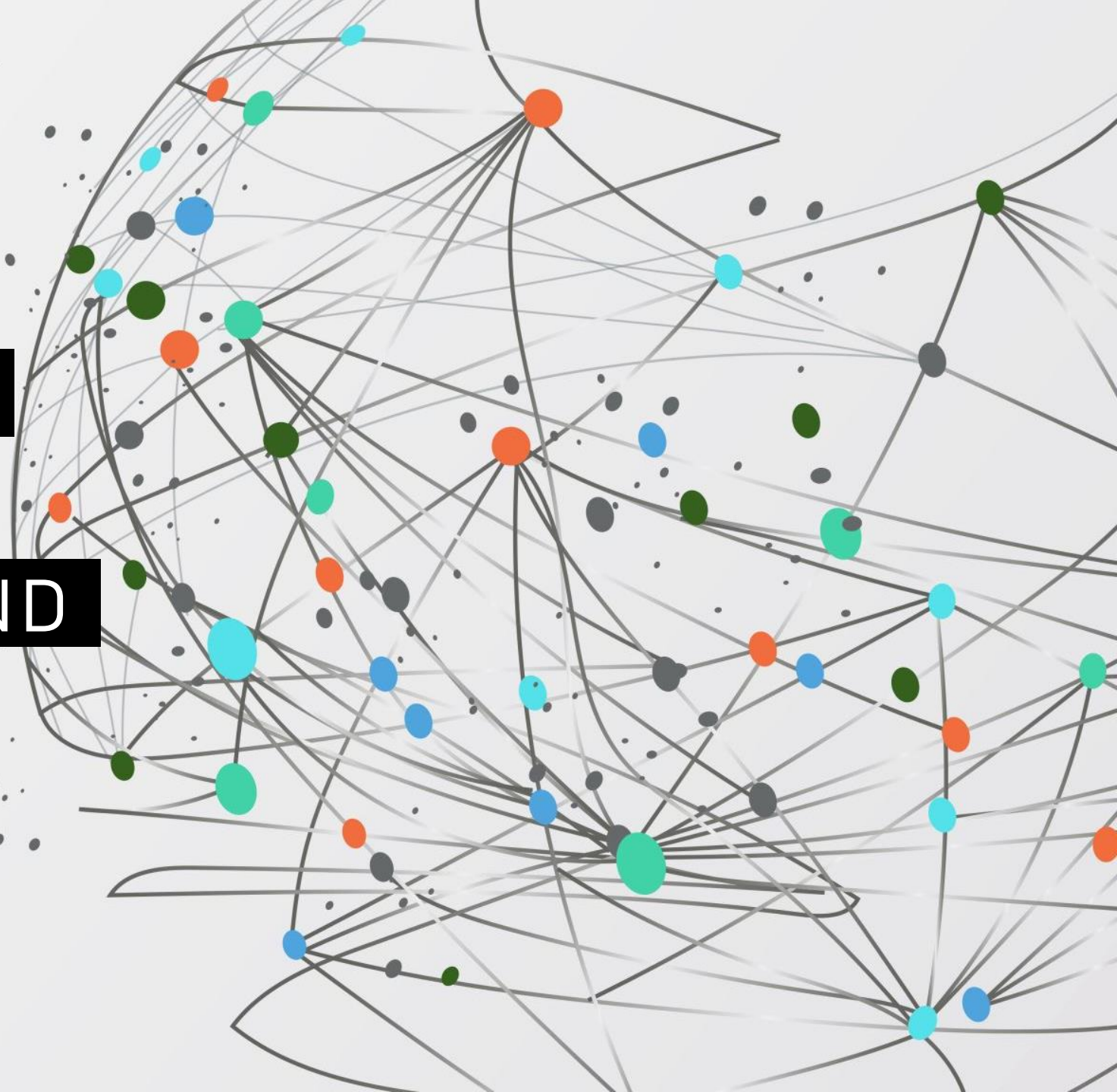
3

BENEFITS AND FEATURES

4

DEPLOYMENT AND SETUP

INTRODUCTION TO AUTOMATED INVESTIGATION AND RESPONSE (AIR)



INTRODUCTION TO AUTOMATED INVESTIGATION AND RESPONSE (AIR)

1

MICROSOFT 365'S SOLUTION FOR RAPID, EFFICIENT RESPONSE TO SECURITY THREATS

2

WORKS SEAMLESSLY WITH MICROSOFT DEFENDER FOR OFFICE 365

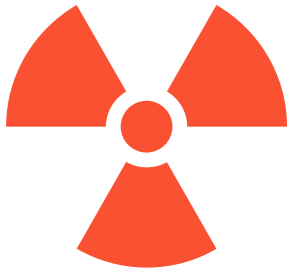
3

PERFORMS AUTOMATED INVESTIGATIONS IN RESPONSE TO SPECIFIC ALERTS

4

REDUCES MANUAL WORKLOAD, FREES UP SECURITY TEAMS FOR STRATEGIC TASKS

IMPORTANCE OF AUTOMATED INVESTIGATION AND RESPONSE (AIR)



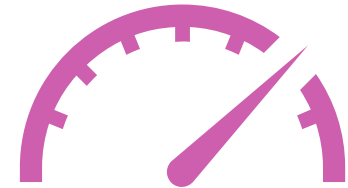
RISKS



VOLUME AND
COMPLEXITY

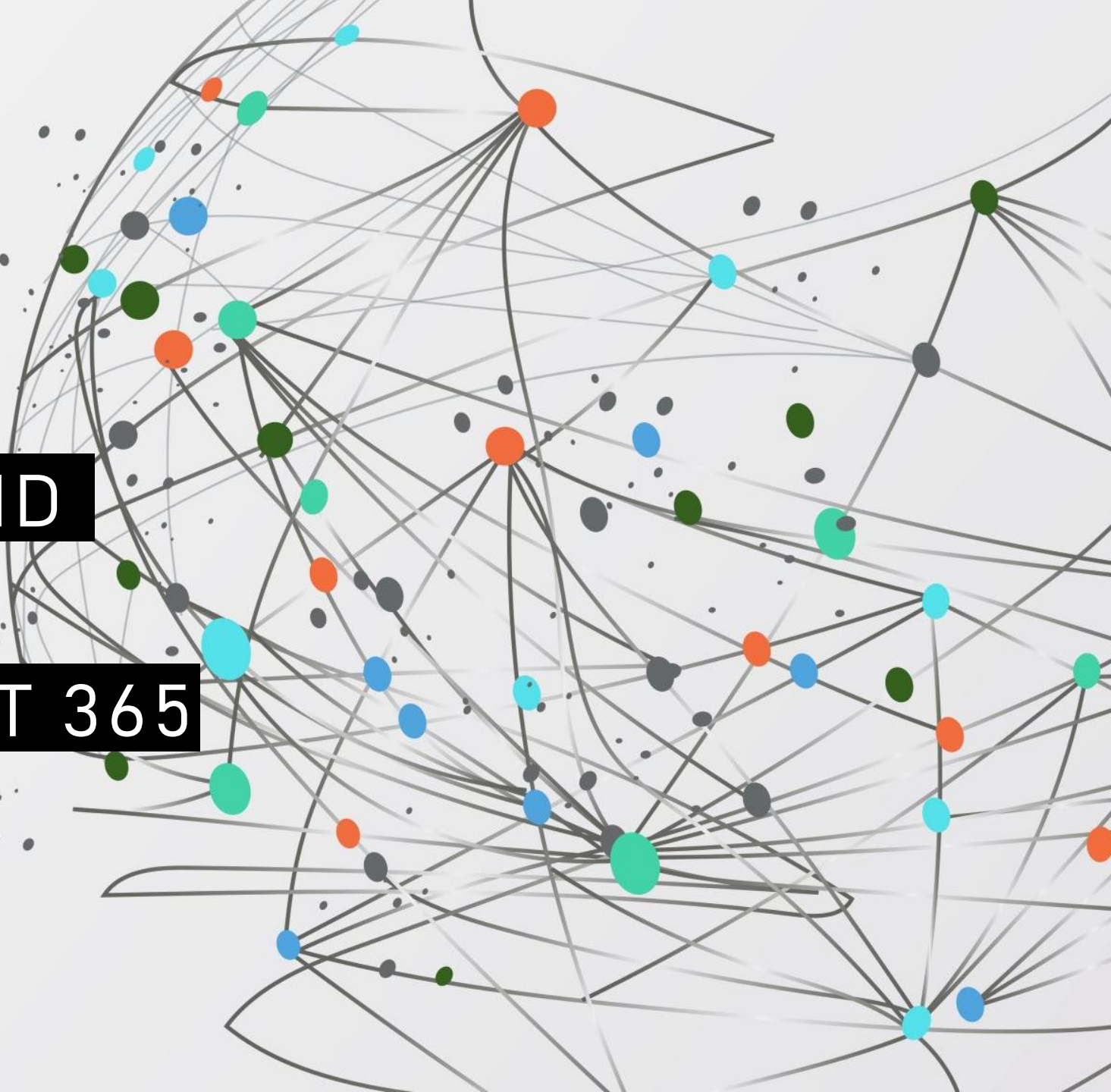


REDUCE TIME



SECURITY
POSTURE

**AUTOMATED
INVESTIGATION AND
RESPONSE (AIR)
WITHIN MICROSOFT 365**



AUTOMATED INVESTIGATION AND RESPONSE
CAPABILITIES ARE INCLUDED WITHIN MICROSOFT
DEFENDER FOR OFFICE 365

PROVIDED POLICIES AND ALERTS ARE CONFIGURED

MICROSOFT 365



KEY COMPONENT OF MICROSOFT 365'S SECURITY FRAMEWORK



INTEGRATES WITH MICROSOFT DEFENDER FOR OFFICE 365



AUTOMATED RESPONSE TO SPECIFIED SECURITY ALERTS



PROVIDES EFFICIENT MANAGEMENT OF POTENTIAL SECURITY THREATS

HOW IT WORKS WITHIN MICROSOFT 365



DETECTION



USER AND
SYSTEM
ACTIVITIES



INVESTIGATION
FINDINGS



AUTOMATED OR
MANUAL
APPROVAL

HOW IT WORKS WITHIN MICROSOFT 365



MALICIOUS FILE
DELIVERED

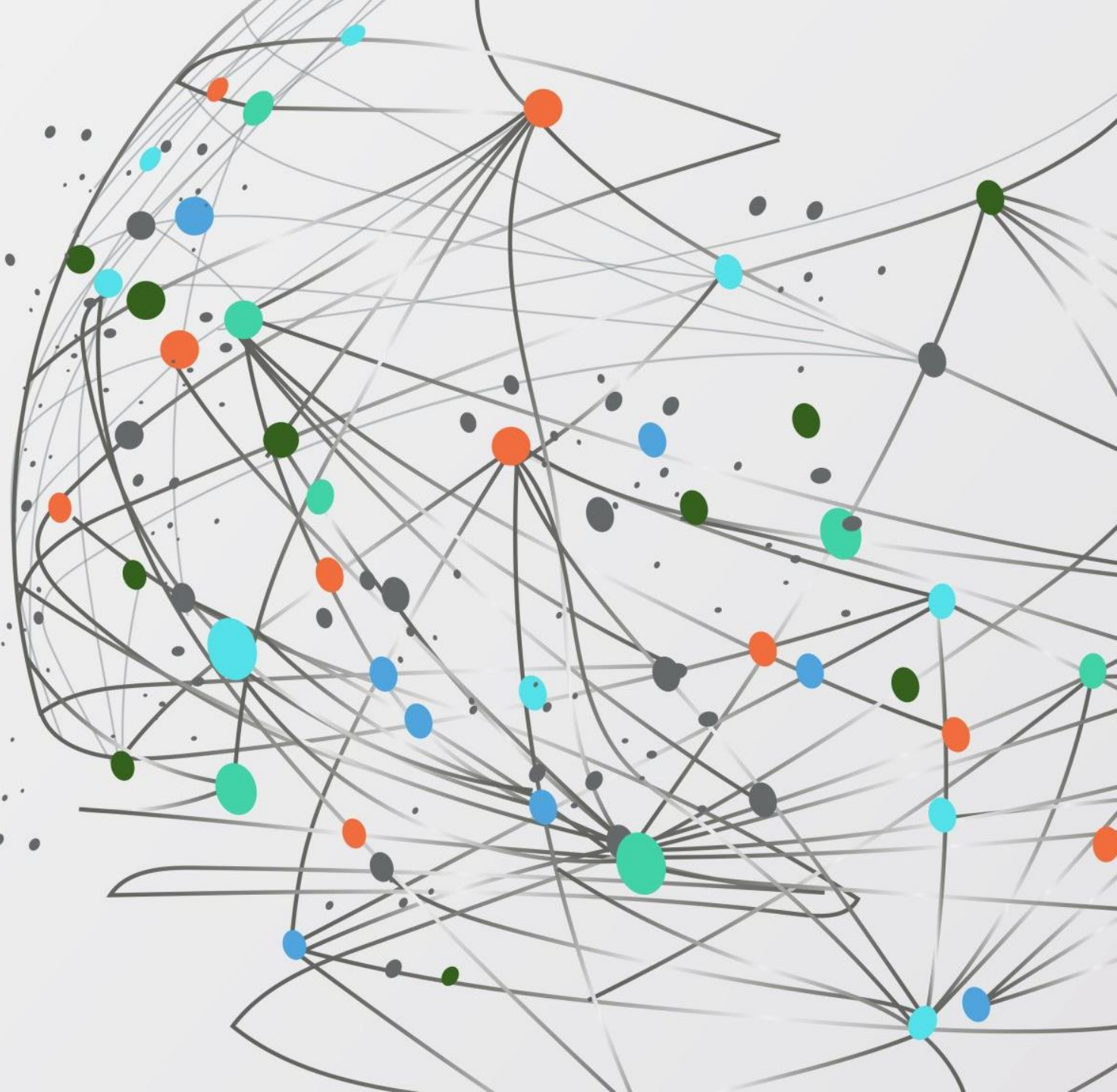


MALICIOUS URL
DELIVERED



PHISHING EMAIL
REPORTED

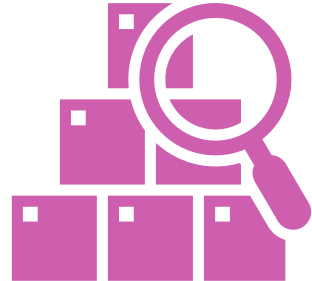
BENEFITS AND FEATURES



KEY FEATURES



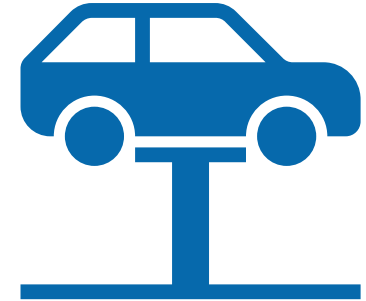
ALERT TRIGGERS



DETAILED
INVESTIGATIONS



ACTIONABLE
REPORTS



FLEXIBLE
REMEDiation

BENEFITS



ENHANCED EFFICIENCY



CONTROL AND OVERSIGHT



RAPID RESPONSE



STRENGTHENED SECURITY

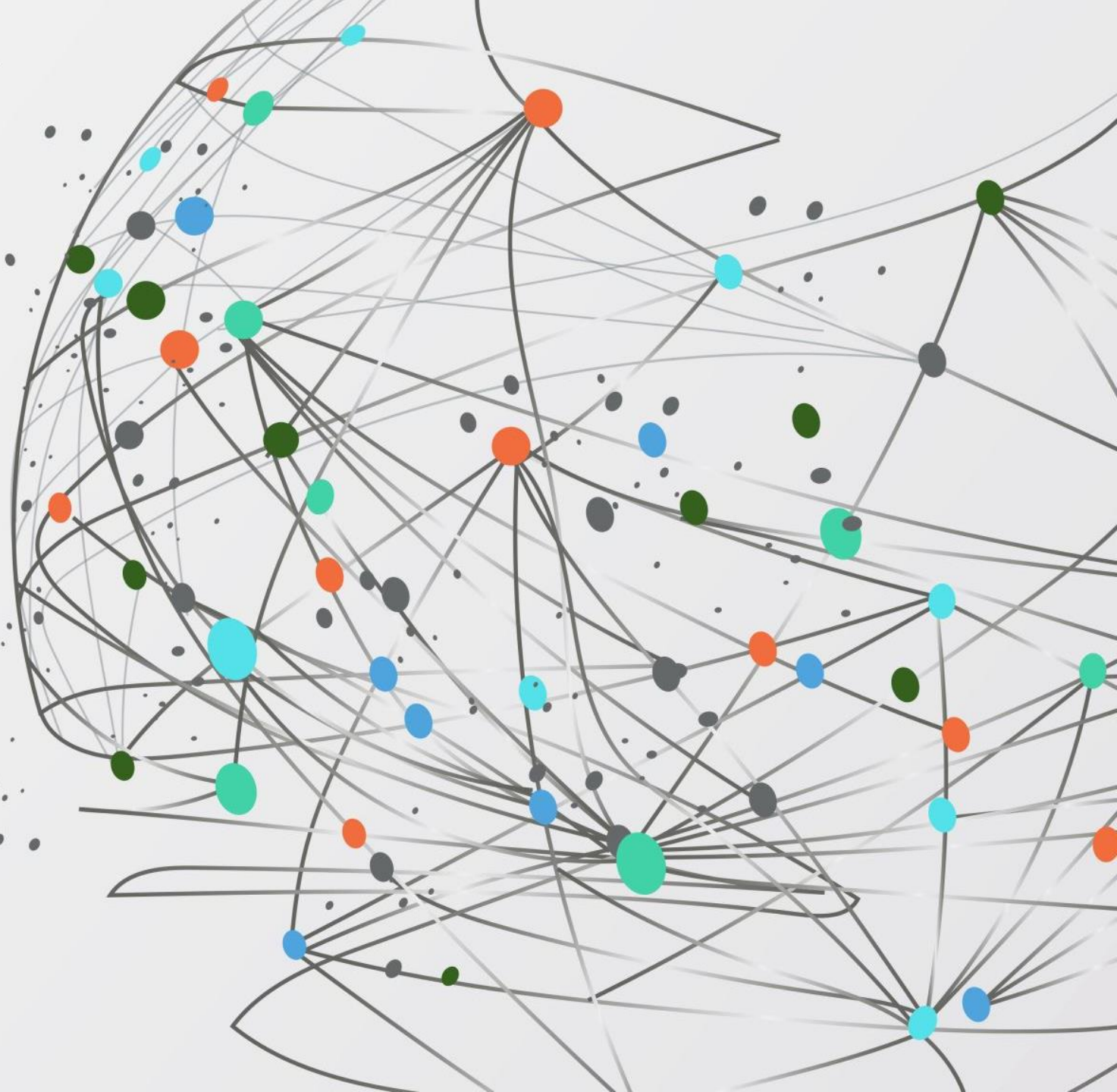


COMPREHENSIVE INSIGHTS



SCALABILITY

PREREQUISITES



SUBSCRIPTION REQUIREMENTS



MICROSOFT 365 E5/A5

MICROSOFT 365 E3 WITH THE MICROSOFT 365
E5 SECURITY ADD-ON

MICROSOFT 365 A3 WITH THE MICROSOFT 365
A5 SECURITY ADD-ON

OFFICE 365 E5 PLUS ENTERPRISE MOBILITY +
SECURITY E5 PLUS WINDOWS E5

NETWORK REQUIREMENTS



MICROSOFT DEFENDER FOR CLOUD APPS CONFIGURED



MICROSOFT DEFENDER FOR IDENTITY ENABLED



MICROSOFT DEFENDER FOR IDENTITY INTEGRATED

WINDOWS DEVICE REQUIREMENTS



WINDOWS 11 OR WINDOWS 10 (VERSION 1709 OR LATER)

MICROSOFT DEFENDER FOR ENDPOINT

MICROSOFT DEFENDER ANTIVIRUS

PERMISSIONS



GLOBAL ADMINISTRATOR

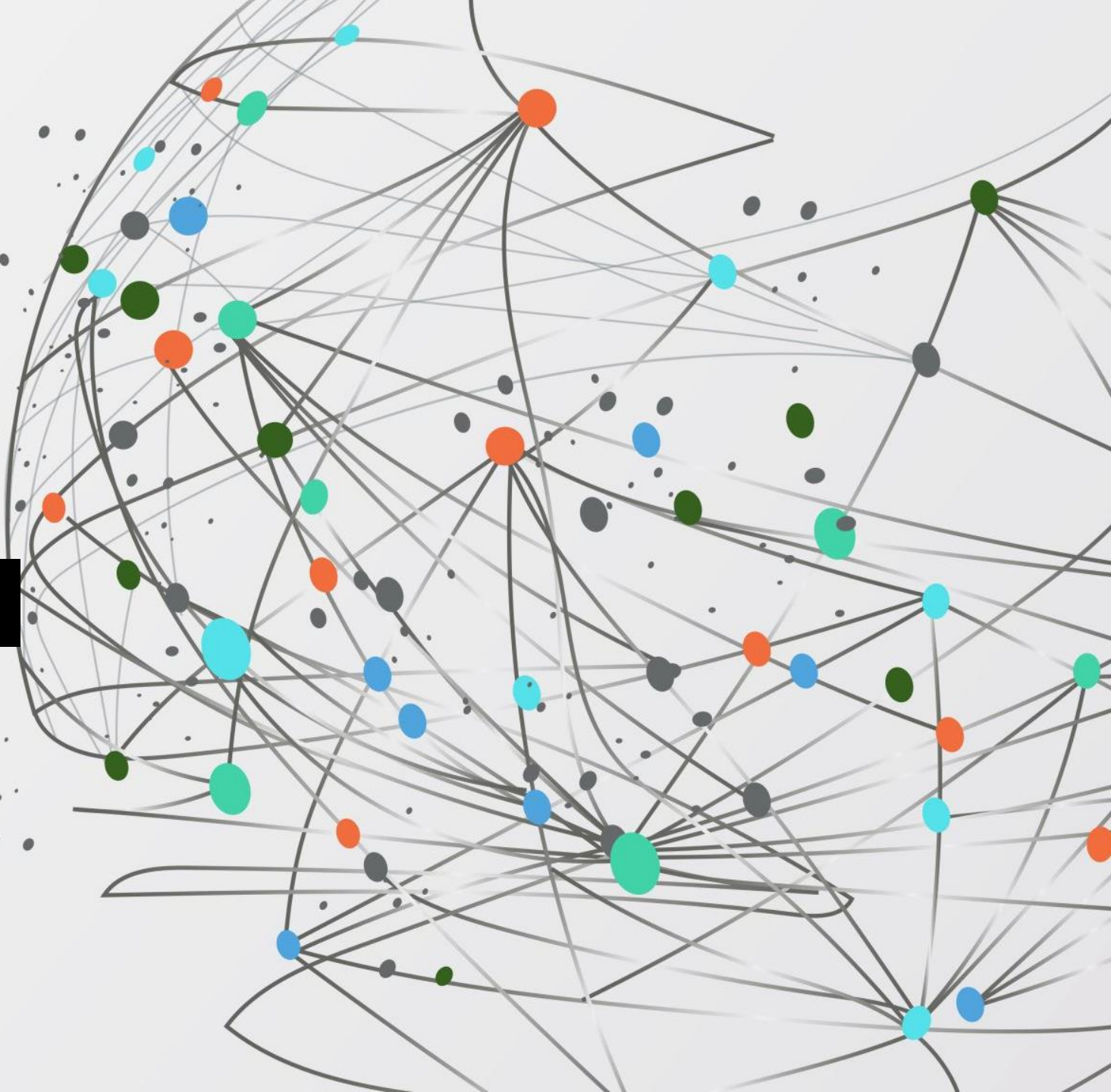
SECURITY ADMINISTRATOR

SECURITY OPERATOR

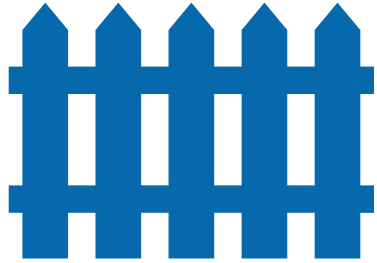
SECURITY READER

SEARCH AND PURGE

DEPLOYMENT AND SETUP



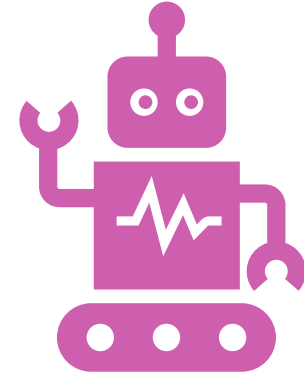
DEVICE GROUPS



MICROSOFT 365
DEFENDER



DEVICE GROUPS










AUTOMATION LEVEL

DEMO



ENDPOINTS

	Name	Description
	Security center	General settings for the Microsoft 365 security center
	Microsoft 365 Defender	General settings for Microsoft 365 Defender
	Endpoints	General settings for endpoints
	Email & collaboration	General settings for email & collaboration
	Identities	General settings for identities
	Device discovery	Select your device discovery mode and customize standard discovery settings
	Cloud Apps	General settings for cloud apps

General

Advanced features

Licenses

Email notifications

Auto remediation

Permissions

Roles

Device groups

APIs

SIEM

Rules

Alert suppression

Indicators

Process Memory Indicators

Web content filtering

Automation uploads

Automation folder exclusions

DEVICE GROUP

Add device group

☒ General

☐ Devices

☐ Preview devices

☐ User access

General

Provide a name and a description for this notification rule to make it easier to identify and manage.

Device group name *

All Devices

Remediation level *

Select remediation level

No automated response

Semi - require approval for all folders

Semi - require approval for non-temp folders

Semi - require approval for core folders

Full - remediate threats automatically

DEVICE GROUP

Add device group

- ☒ General
- ☒ **Devices**
- ☐ Preview devices
- ☐ User access

Devices

Specify the matching rule that determines which devices belong to this group.

4 items

And/Or	Condition	Operator	Value	
	Name	Starts with	WIN	+
And	Domain	Starts with	TRAINING	+
And	Tag	Starts with		+
And	OS	In	Windows 10	

DEVICE GROUP

ⓘ Device group configuration has changed. Apply changes to check matches and recalculate groupings.

Apply changes

Discard changes

Organize devices into groups, set automated remediation levels, and assign administrators.

+ Add device group

<input type="checkbox"/>	Rank ↑	Device group	Devices	Remediation level
<input type="checkbox"/>	1	All Devices	0	Full - remediate threats automatically

Organize devices into groups, set automated remediation levels, and assign administrators.

+ Add device group

<input type="checkbox"/>	Rank ↑	Device group	Devices	Remediation level
<input type="checkbox"/>	1	All Devices	0	Full - remediate threats automatically
<input type="checkbox"/>	Last	Ungrouped devices (default)	0	Full - remediate threats automatically

ALERT POLICIES

1 ANTI-MALWARE

2 ANTI-PHISHING

3 ANTI-SPAM

4 SAFE ATTACHMENTS

5 SAFE LINKS

6 ZERO-HOUR AUTO PURGE

DEMO



INCIDENTS LIST

<input type="checkbox"/> ☰	Incident name	Incident Id	Tags	Severity
<input type="checkbox"/> >	Activity from infrequent country	26		■ ■ ■ Medium
<input type="checkbox"/> >	Multi-stage incident involving multiple users	22		■ ■ ■ Medium
<input type="checkbox"/> >	Impossible travel activity involving one user	19		■ ■ ■ Medium
<input type="checkbox"/> ✓	Multi-stage incident involving Initial access & Defense evasion involving multiple users reported by multiple sources	4		■ ■ ■ Medium
<input type="checkbox"/>	Activity from infrequent country			■ ■ ■ Medium
<input type="checkbox"/>	Activity from infrequent country			■ ■ ■ Medium
<input type="checkbox"/>	Anomalous Token			■ ■ ■ Medium
<input type="checkbox"/>	Impossible travel activity			■ ■ ■ Medium
<input type="checkbox"/>	Activity from infrequent country			■ ■ ■ Medium
<input type="checkbox"/>	Activity from infrequent country			■ ■ ■ Medium
<input type="checkbox"/>	Impossible travel activity			■ ■ ■ Medium
<input type="checkbox"/>	Anonymous IP address			■ ■ ■ Medium
<input type="checkbox"/>	Anonymous IP address			■ ■ ■ Medium

INCIDENT BASIC DETAILS

Incidents

Most recent incidents and alerts

↓ Export

Filters: Status: New +1 ✕ Severity: High +2 ✕

<input type="checkbox"/>	Incident name	Incident Id	Tags
<input type="checkbox"/>	> Activity from infrequent country	26	
<input type="checkbox"/>	> Multi-stage incident involving multiple users	22	
<input type="checkbox"/>	> Impossible travel activity involving one user	19	
<input type="checkbox"/>	✓ Multi-stage incident involving Initial access & Defense evasion involving multiple users reported by multiple sources	4	
<input type="checkbox"/>	Activity from infrequent country		
<input type="checkbox"/>	Activity from infrequent country		
<input type="checkbox"/>	Anomalous Token		
<input type="checkbox"/>	Impossible travel activity		
<input type="checkbox"/>	Activity from infrequent country		
<input type="checkbox"/>	Activity from infrequent country		
<input type="checkbox"/>	Impossible travel activity		
<input type="checkbox"/>	Anonymous IP address		



Multi-stage incident involving Initial access & Defense evasion involving multiple users reported by multiple sources

■ Medium ● Active

→ Open incident page ✎ Manage incident

Incident details

Assigned to	Incident ID
Unassigned	4
Classification	Categories
Not set	Initial access, Defense evasion
First activity	Last activity
May 2, 2023 6:12:57 AM	May 2, 2023 8:06:17 AM

Impacted assets

Users (2)

👤 Nestor Wilke

👤 MOD Administrator

Apps (1)	Application ID	Risk
☁ Microsoft 365 ☒	11161	■ ■ ■ None

INCIDENT



Multi-stage incident involving Initial access & Defe...

[Manage incident](#) [Ask Defender Experts](#) [Comments and history](#)

Attack story Alerts (16) Assets (3) Investigations (0) Evidence and Response (16) Summary

Alerts

16/16 Active alerts

Unpin all

Show all

May 2, 2023 6:12 AM

New

Impossible travel activity

MOD Administrator

May 2, 2023 6:12 AM

New

Impossible travel activity

MOD Administrator

May 2, 2023 6:16 AM

New

Activity from infrequent country

MOD Administrator

May 2, 2023 6:16 AM

New

Activity from infrequent country

MOD Administrator

May 2, 2023 6:16 AM

New

Activity from infrequent country

MOD Administrator

May 2, 2023 6:16 AM

New

Anonymous IP address

MOD Administrator

Incident graph

Layout

Group similar nodes

nestorw

admin

Microsoft 365

5.8.16.167

7 IPs

Communication

Association

Multi-stage incident involving Initial access & Defense evasion involving multiple users reported by multiple sources

Medium

Active

Manage incident

Incident details

Assigned to

Unassigned

Incident ID

4

Classification

Not set

Categories

Initial access, Defense evasion

First activity

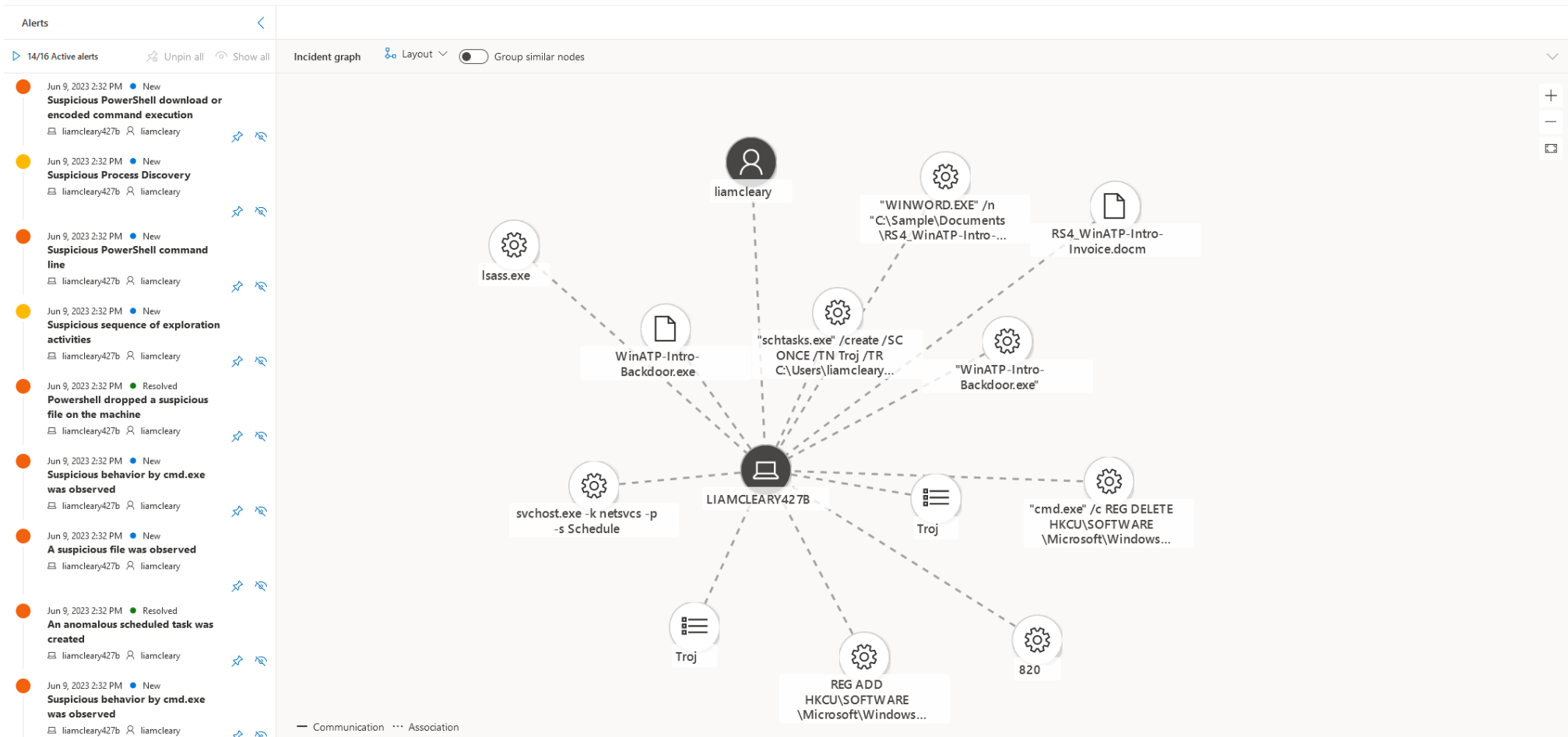
May 2, 2023 6:12:57 AM

Last activity

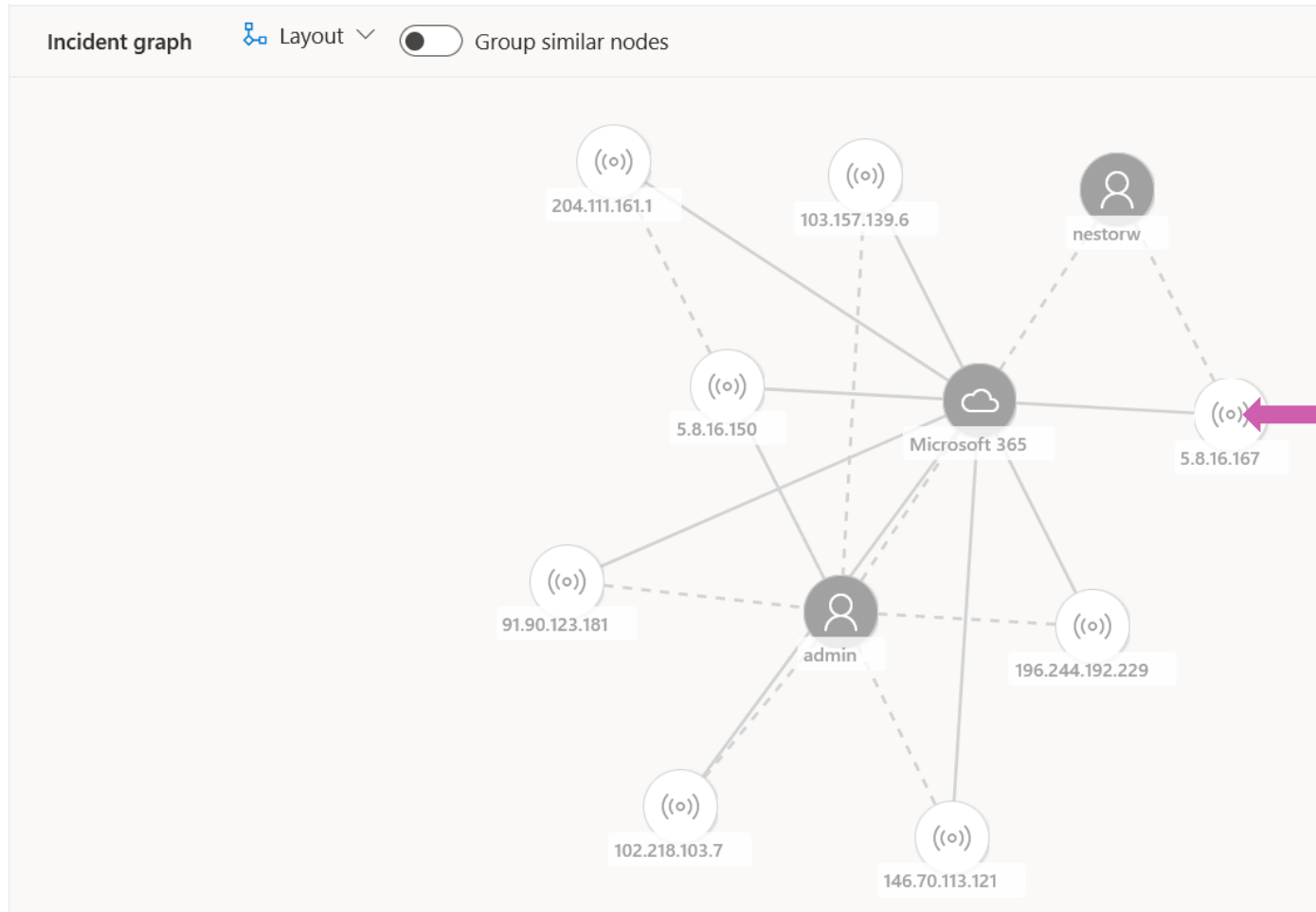
May 2, 2023 8:06:17 AM

Impacted assets

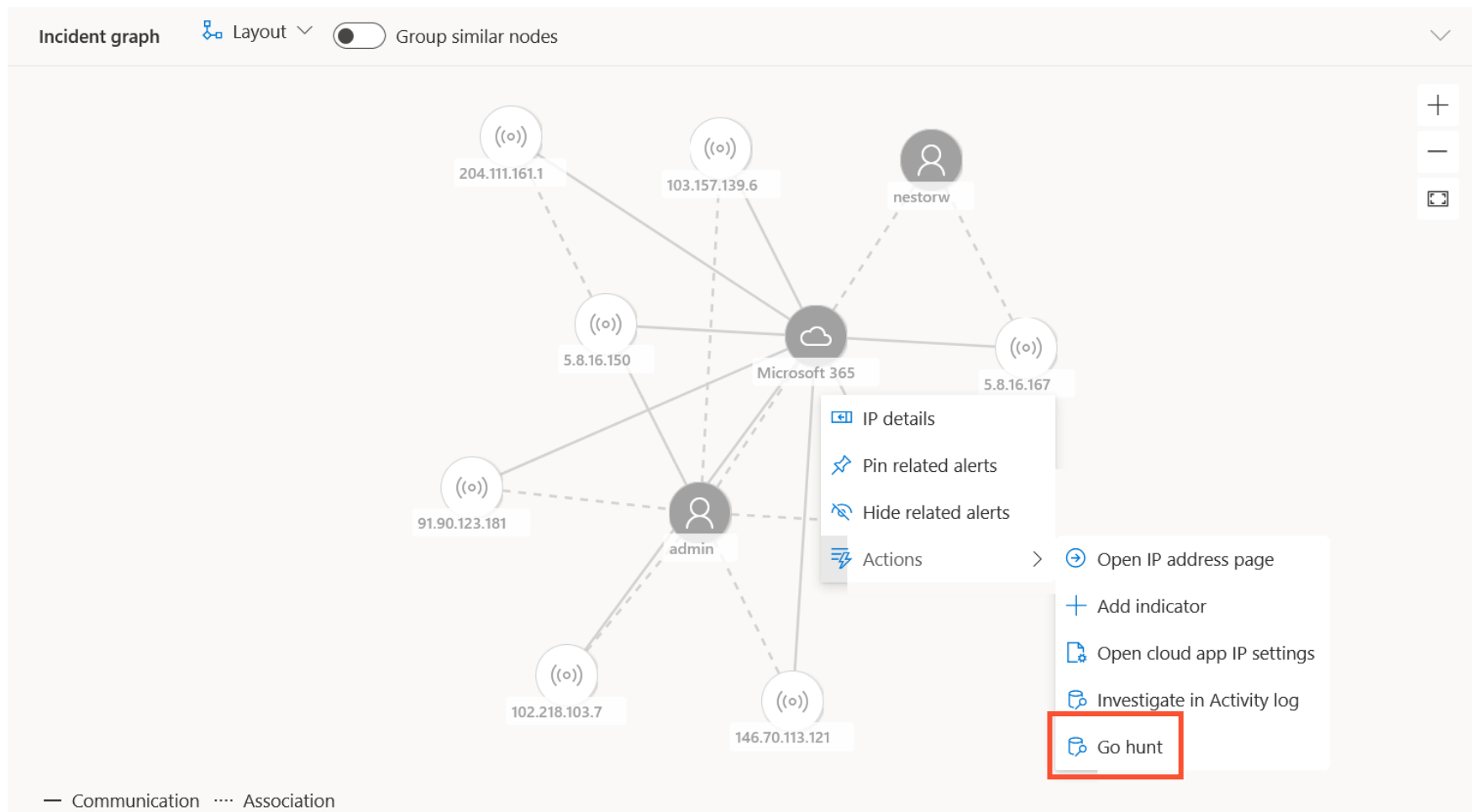
INCIDENT GRAPH



INCIDENT GRAPH



INCIDENT GRAPH ACTIONS



INCIDENT HUNTING

▶ Run query

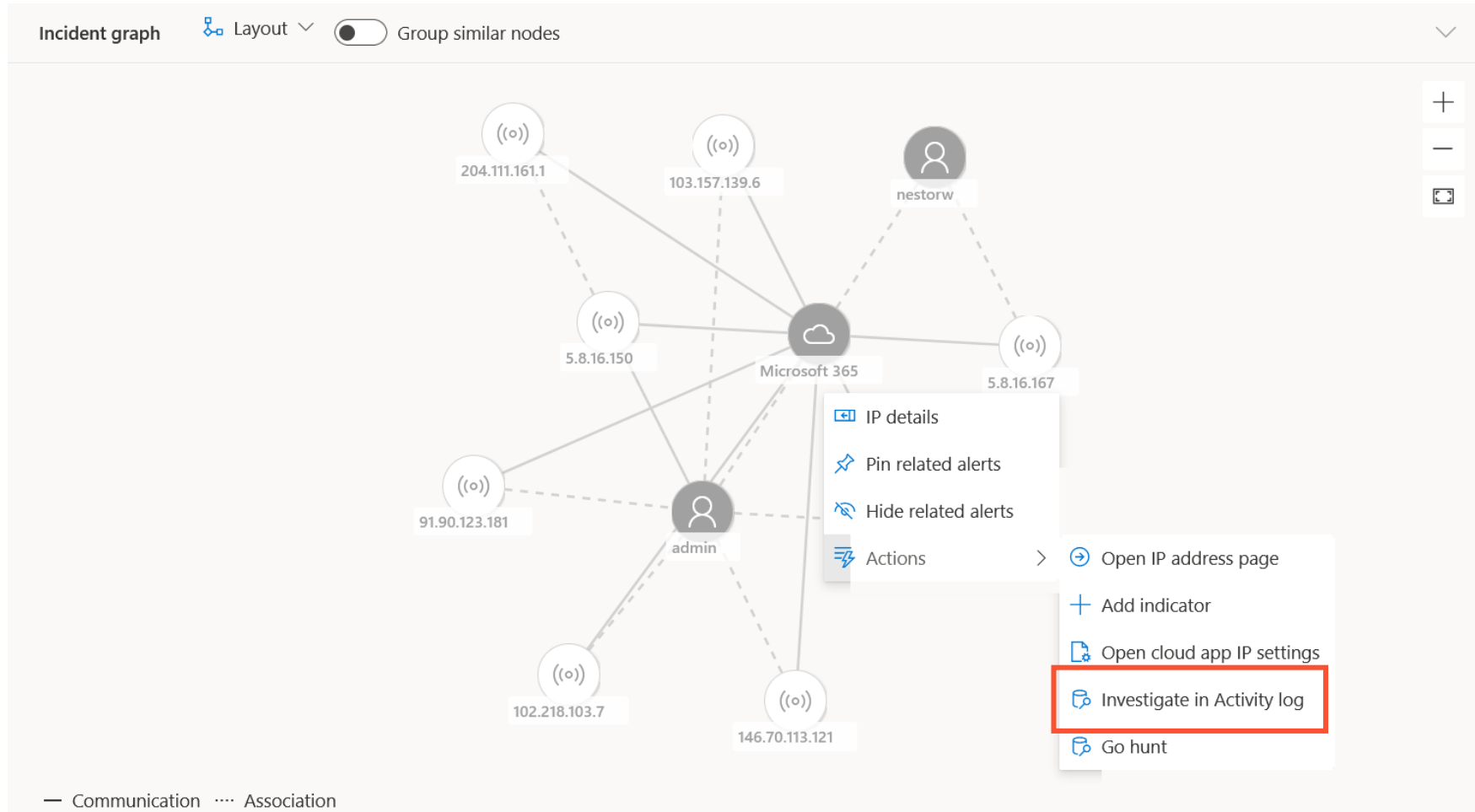
📁 Save ▾ 🔗 Share link

📅 Set in query ▾ ⚙️ Create detection rule

Query

```
1 |let ip = "5.8.16.150";
2 |search in (IdentityLogonEvents,IdentityQueryEvents,IdentityDirectoryEvents,DeviceNetworkEvents,DeviceFileEvents,DeviceLogonEvents,DeviceLogonEvents,DeviceLogonEvents)
3 |Timestamp between (ago(1d) .. now())
4 |and (// Events initiated by this IP
5 |LocalIP == ip
6 |or FileOriginIP == ip
7 |or RequestSourceIP == ip
8 |or IPAddress == ip
9 |// Events affecting this IP
10 |or RemoteIP == ip
11 |or DestinationIPAddress == ip
12 |)
13 |take 100
```

INCIDENT GRAPH ACTIONS














INVESTIGATE IN ACTIVITY LOG

✕ Raw IP address ▾ equals 5.8.16.150 +

+ Add a filter

+ New policy from search ▾ Export

1 - 5 of 5 activities ⓘ ↔ Show details ▾ Hide filters ⚙ Table settings ▾

	Activity ▾	User ▾	App ▾	IP address ▾	Location ▾	Device	Date ↓ ▾	
⇒	Log on	MOD Administrator	 Microsoft 365	5.8.16.150	Russia		May 2, 2023 6:36 ...	⋮
⇒	Log on	MOD Administrator	 Microsoft 365	5.8.16.150	Russia		May 2, 2023 6:35 ...	⋮
⇒	Log on	 MOD Administrator	 Microsoft 365	5.8.16.150	Russia		May 2, 2023 6:35 ...	⋮
⇒	Log on	MOD Administrator	 Microsoft 365	5.8.16.150	Russia		May 2, 2023 6:35 ...	⋮
⇒	Log on	MOD Administrator	 Microsoft 365	5.8.16.150	Russia		May 2, 2023 6:35 ...	⋮












INVESTIGATE IN ACTIVITY LOG

✕ Raw IP address ▾ equals 5.8.16.150 +

+ Add a filter

+ New policy from search ▾ Export

1 - 5 of 5 activities ⓘ ↔ Show details ▾ Hide filters ⚙ Table settings ▾

	Activity ▾	User ▾	App ▾	IP address ▾	Location ▾	Device	Date ↓ ▾
➞	Log on	MOD Administrator	 Microsoft 365	5.8.16.150	Russia		May 2, 2023 6:36 ... ⋮
➞	Log on	MOD Administrator	 Microsoft 365	5.8.16.150	Russia		
➞	Log on	 MOD Administrator	 Microsoft 365	5.8.16.150	Russia		
➞	Log on	MOD Administrator	 Microsoft 365	5.8.16.150	Russia		
➞	Log on	MOD Administrator	 Microsoft 365	5.8.16.150	Russia		May 2, 2023 6:35 ... ⋮

- View activity of the same type
- View all user activity
- View activity from the same IP address
- View activity from the same country/region

INCIDENT ALERTS

Filters: Status: New +1 ✕ Severity: High +2 ✕

<input type="checkbox"/>		Incident name	Incident Id	Tags	Severity	Investigation state	Categories	Impacted assets
<input type="checkbox"/>	▼	Multi-stage incident involving Execution & Coll...	27	Ransomware	■■■ High	6 investigation states	Execution, Persistence, ...	liamcleary427b 2 Accounts
<input type="checkbox"/>		Suspicious behavior by cmd.exe was observed			■■■ Medium	Running	Execution	liamcleary427b liamcleary
<input type="checkbox"/>		Suspicious behavior by cmd.exe was observed			■■■ Medium	Running	Execution	liamcleary427b liamcleary
<input type="checkbox"/>		Sensitive credential memory read			■■■ High		Credential access	liamcleary427b liamcleary
<input type="checkbox"/>		Suspicious PowerShell command line			■■■ Medium	Running	Execution	liamcleary427b liamcleary
<input type="checkbox"/>		Suspicious sequence of exploration activities			■ ■ ■ Low		Discovery	LIAMCLEARY427B liamcleary
<input type="checkbox"/>		Anomalous account lookups			■ ■ ■ Low		Discovery	liamcleary427b liamcleary
<input type="checkbox"/>		Suspicious access to LSASS service			■■■ High	Running	Credential access	liamcleary427b liamcleary
<input type="checkbox"/>		An active 'LsassDump' malware was blocked			■ ■ ■ Low	Running	Malware	liamcleary427b
<input type="checkbox"/>		Suspicious 'LsassDump' behavior was blocked			■ ■ ■ Low		Suspicious activity	liamcleary427b liamcleary
<input type="checkbox"/>		Mimikatz credential theft tool			■■■ High		Credential access	LIAMCLEARY427B liamcleary
<input type="checkbox"/>		Possible attempt to steal credentials			■■■ High	Running	Credential access	liamcleary427b liamcleary
<input type="checkbox"/>		Suspicious behavior by cmd.exe was observed			■■■ Medium	Running	Execution	liamcleary427b liamcleary
<input type="checkbox"/>		Possible Antimalware Scan Interface (AMSI) t...			■■■ High		Defense evasion	liamcleary427b liamcleary
<input type="checkbox"/>		An active 'CalelzSh' malware in a PowerShell ...			■ ■ ■ Low	Running	Malware	liamcleary427b liamcleary

INCIDENT DETAILS

liamcleary427b
⋮


LIAMCLEARY427B\liamcleary
⋮

Windows11

Alert story
↗ Maximize

⌵ Expand all

Time	Process	Command / Action	Severity	Status
6/9/2023 1:56:13 PM	[4716] explorer.exe			⋮ ⌵
2:32:13 PM	[2260] WINWORD.EXE	/n "C:\Sample\Documents\RS4_WinATP-Intro-Invoice.docm" /o ""		⋮ ⌵
2:32:24 PM	[820] powershell.exe	-W Hidden -Exec Bypass -Command cd /;fileBase64Prefix = "";fileBase64Prefix= \$fileBase64Prefix + 'TVq';fileBase64Prefix= \$fileBase64Prefix		⋮ ⌵
2:32:26 PM	powershell.exe executed a script			⌵
	⚡ Suspicious sequence of exploration activities		Low Detected New	⋮
	⚡ Suspicious Process Discovery		Low Detected New	⋮
2:32:27 PM	[5676] schtasks.exe	/create /SC ONCE /TN Troj /TR C:\Users\liamcleary\Desktop\WinATP-Intro-Backdoor.exe /ST 17:30 /F		⋮ ⌵
	⚡ Suspicious Task Scheduler activity		Medium Detected New	⋮
2:32:27 PM	powershell.exe created the scheduled task Troj by invoking schtasks.exe			⌵
	⚡ Suspicious Task Scheduler activity		Medium Detected New	⋮
2:32:28 PM	[3412] schtasks.exe	/run /TN Troj		⋮ ⌵
	⚡ Suspicious Task Scheduler activity		Medium Detected New	⋮
2:32:28 PM	powershell.exe launched the scheduled task Troj by invoking schtasks.exe			⌵
	⚡ Suspicious Task Scheduler activity		Medium Detected New	⋮
2:32:26 PM	WINWORD.EXE performed process discovery by invoking powershell.exe			⌵
	⚡ Suspicious sequence of exploration activities		Low Detected New	⋮
	⚡ Suspicious Process Discovery		Low Detected New	⋮
7:02:03 PM	[9488] WindowsTerminal.exe			⋮ ⌵



Suspicious PowerShell command line

■ ■ ■ Medium
● Detected
● New

[Manage alert](#)
[See in timeline](#)
[Tune alert](#)
⋮

Details

Recommendations

INSIGHT

Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.






Classify alert

Alert state

Classification	Assigned to
Not Set	Unassigned
Set Classification	

Alert details

Evidence

Entity Name	Remediation Status	Verdict
 rundll32.exe (11472)		
 WinCreds.exe		
 powershell.exe (12208)		
 powershell.exe (4016)		
 powershell.exe (11104)		

[View All](#)

Alert description

INCIDENT ALERTS



Multi-stage incident involving Initial access & Defe...

[Manage incident](#)

Attack story **Alerts (16)** Assets (3) Investigations (0) Evidence and Response (16)



↓ Export 6 Months ▾

<input type="checkbox"/>	Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Impacted assets
<input type="checkbox"/>	Activity from infrequent country		■ ■ ■ Medium		● New	Defense evasion	Microsoft Defender for...	👤 nestorw
<input type="checkbox"/>	Activity from infrequent country		■ ■ ■ Medium		● New	Defense evasion	Microsoft Defender for...	👤 admin
<input type="checkbox"/>	Anomalous Token		■ ■ ■ Medium		● New	Initial access	AAD Identity Protection	👤 admin
<input type="checkbox"/>	Activity from infrequent country		■ ■ ■ Medium		● New	Defense evasion	Microsoft Defender for...	👤 admin
<input type="checkbox"/>	Impossible travel activity		■ ■ ■ Medium		● New	Initial access	Microsoft Defender for...	👤 admin
<input type="checkbox"/>	Impossible travel activity		■ ■ ■ Medium		● New	Initial access	Microsoft Defender for...	👤 admin
<input type="checkbox"/>	Activity from infrequent country		■ ■ ■ Medium		● New	Defense evasion	Microsoft Defender for...	👤 admin
<input type="checkbox"/>	Anonymous IP address		■ ■ ■ Medium		● New	Initial access	AAD Identity Protection	👤 admin
<input type="checkbox"/>	Anonymous IP address		■ ■ ■ Medium		● New	Initial access	AAD Identity Protection	👤 admin
<input type="checkbox"/>	Activity from infrequent country		■ ■ ■ Medium		● New	Defense evasion	Microsoft Defender for...	👤 admin
<input type="checkbox"/>	Activity from infrequent country		■ ■ ■ Medium		● New	Defense evasion	Microsoft Defender for...	👤 admin
<input type="checkbox"/>	Anomalous Token		■ ■ ■ Medium		● New	Initial access	AAD Identity Protection	👤 admin
<input type="checkbox"/>	Anonymous IP address		■ ■ ■ Medium		● New	Initial access	AAD Identity Protection	👤 admin

INCIDENT EVIDENCE AND RESPONSE



Multi-stage incident involving Initial access & Defe...

[Manage incident](#) [Ask Defender Experts](#) [Comments and history](#)

[Attack story](#) [Alerts \(16\)](#) [Assets \(3\)](#) [Investigations \(0\)](#) [Evidence and Response \(16\)](#) [Summary](#)

All evidence (9)

[IP Addresses \(8\)](#)

[Cloud Logon Sessions \(1\)](#)

1-9 of 9 [Choose columns](#) [30 items per page](#) [Filters](#)

✓	First seen ↑	Entity	Verdict	Impacted assets	Detection origin	
	May 2, 2023 6:17 AM	196.244.192.229	Suspicious		Activity from infrequent country ...	+2 alerts
	May 2, 2023 6:18 AM	91.90.123.181	Suspicious		Activity from infrequent country ...	+5 alerts
	May 2, 2023 6:18 AM	146.70.113.121	Suspicious		Activity from infrequent country ...	+2 alerts
	May 2, 2023 6:20 AM	103.157.139.6	Suspicious		Activity from infrequent country ...	+1 alerts
	May 2, 2023 6:23 AM	204.111.161.1	Suspicious		Impossible travel activity <div><div></div><div></div><div></div></div> Medium	+1 alerts
	May 2, 2023 6:23 AM	102.218.103.7	Suspicious		Activity from infrequent country ...	+1 alerts
	May 2, 2023 6:35 AM	MOD Administrator		admin@msdx878906...	Anomalous Token <div><div></div><div></div><div></div></div> Medium	+6 alerts
	May 2, 2023 6:35 AM	5.8.16.150	Suspicious		Activity from infrequent country ...	+1 alerts
	May 2, 2023 8:06 AM	5.8.16.167	Suspicious		Activity from infrequent country <div><div></div><div></div><div></div></div> Medium	

INCIDENT EVIDENCE AND RESPONSE

Attack story Alerts (16) Assets (2) Investigations (1) Evidence and Response (20) Summary

All evidence (20)

Processes (16)

Files (2)

Registry Values (2)

1-20 of 20 Choose columns 100 items per page Filters				
✓	First seen ↑	Entity	Verdict	Detection origin
	Jun 9, 2023 2:32 PM	schtasks.exe (5676)	Suspicious	A suspicious file was observed Medium +6 alerts
	Jun 9, 2023 2:32 PM	schtasks.exe (3412)	Suspicious	Suspicious Task Scheduler activity Medium
	Jun 9, 2023 2:32 PM	lsass.exe (852)	Suspicious	Suspicious Scheduled Task Process Launched Medium
	Jun 9, 2023 2:32 PM	WinATP-Intro-Backdoor.exe (3112)	Suspicious	A suspicious file was observed Medium +2 alerts
	Jun 9, 2023 2:32 PM	svchost.exe (1384)	Suspicious	Suspicious Scheduled Task Process Launched Medium +1 alerts
	Jun 9, 2023 2:32 PM	powershell.exe (820)	Suspicious	A suspicious file was observed Medium +11 alerts
	Jun 9, 2023 2:32 PM	WINWORD.EXE (2260)	Suspicious	Suspicious PowerShell command line Medium +3 alerts
	Jun 9, 2023 2:32 PM	reg.exe (8340)	Suspicious	A suspicious file was observed Medium
	Jun 9, 2023 2:32 PM	RS4_WinATP-Intro-Invoice.docm	Suspicious	A suspicious file was observed Medium +7 alerts
	Jun 9, 2023 2:32 PM	cmd.exe (5980)	Suspicious	A suspicious file was observed Medium +1 alerts
	Jun 9, 2023 2:32 PM	WinATP-Intro-Backdoor.exe	Suspicious	A suspicious file was observed Medium +4 alerts
	Jun 9, 2023 2:32 PM	cmd.exe (1344)	Suspicious	Suspicious behavior by cmd.exe was observed Medium
	Jun 9, 2023 2:32 PM	Troj	Suspicious	Anomaly detected in ASEP registry Medium

INVESTIGATIONS



An anomalous scheduled task was created

Investigation #1 is complete - No threats found

Investigation Summary

Investigation Status Timeline

Started

Jun 9, 2023, 2:35:29 PM

Ended

Jun 9, 2023, 2:54:01 PM

00:18:31

Complete

Investigation details

Status

No threats found

No malicious entities found during the investigation.

Alert severity

Medium

Category

Persistence

Detection source

EDR

Investigation graph

Alerts (2)

Devices (1)

Evidence (3)

Entities (2.77k)

Log (40)

Device (1)

LIAMCLEAR1427B

Entities analyzed (2774)

1662 Files

118 Processes

288 Services

420 Drivers

7 IP Addresses

279 Persistence Methods



Alert received

An anomalous scheduled task was created

+ 1 correlated alert



Evidence

3 entities found



Result

No threats found

Entities

Start date

Duration

Endpoint

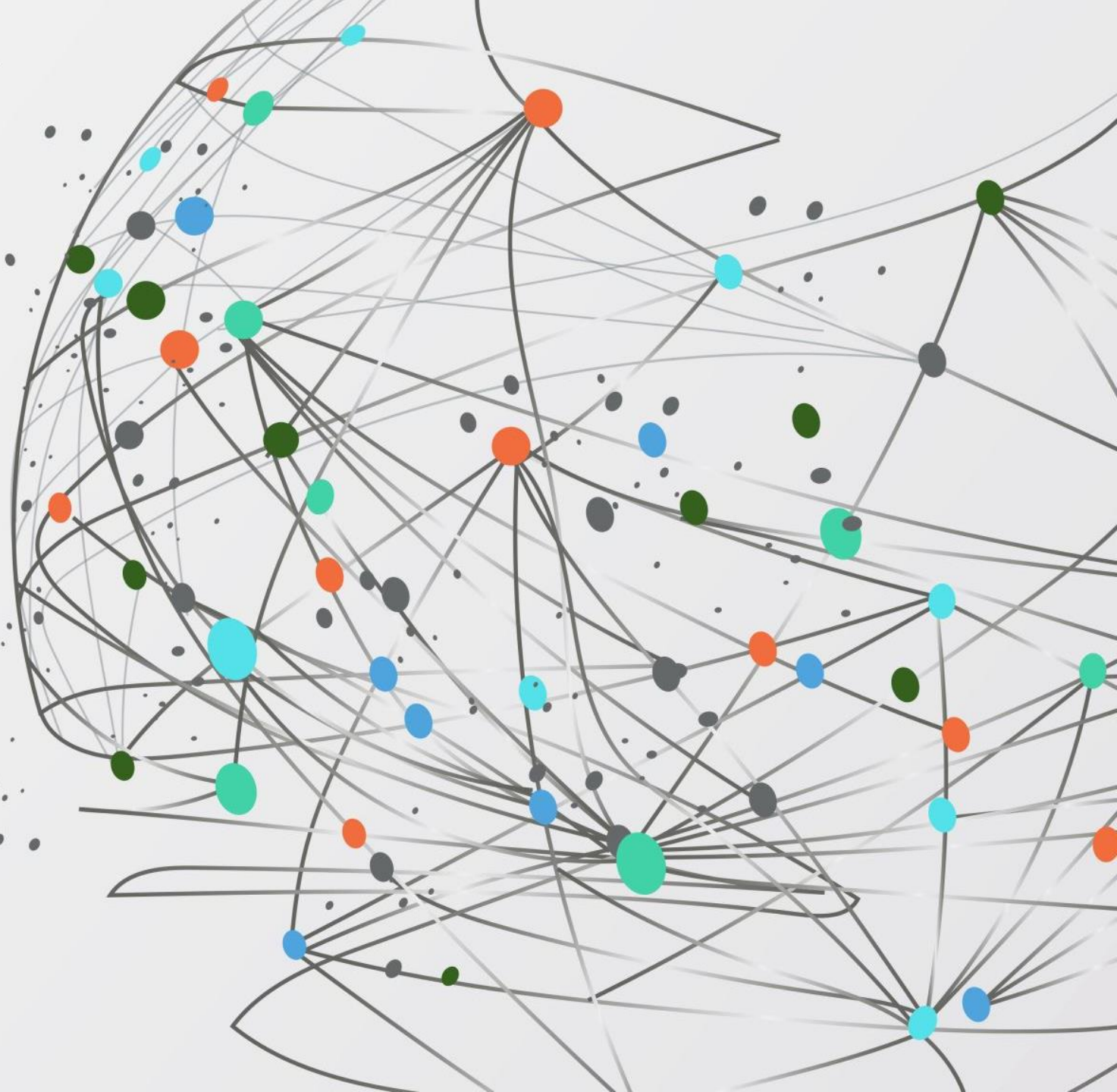


liamclear1427b

Jun 9, 2023 2:35 PM

18:31m

CONCLUSION



EVALUATION LAB

MICROSOFT 365 DEFENDER PORTAL > ENDPOINTS > EVALUATION LAB

Select your lab configuration

The following lab configuration options allows you to choose to run fewer devices for a longer period or more devices for a shorter period. When the allotted time is met, devices are automatically deleted.

- ☒ 3 devices For 72 hours each
- ☐ 4 devices For 48 hours each
- ☐ 8 devices For 24 hours each
- ☐ 16 devices For 12 hours each

When you've used up these devices and need more, you can submit a request for more devices. Once you've selected the configuration for the added devices, it cannot be modified. A deleted device can't be restored in any way and does not refresh the available test device count.

RESOURCES



AUTOMATED INVESTIGATION AND RESPONSE (AIR) IN MICROSOFT DEFENDER DOCUMENTATION

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/air-about?view=o365-worldwide>



OVERVIEW OF AUTOMATED INVESTIGATIONS

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/automated-investigations?view=o365-worldwide>



MICROSOFT 365 DEFENDER VIRTUAL NINJA TRAINING

<https://adoption.microsoft.com/en-us/ninja-show>

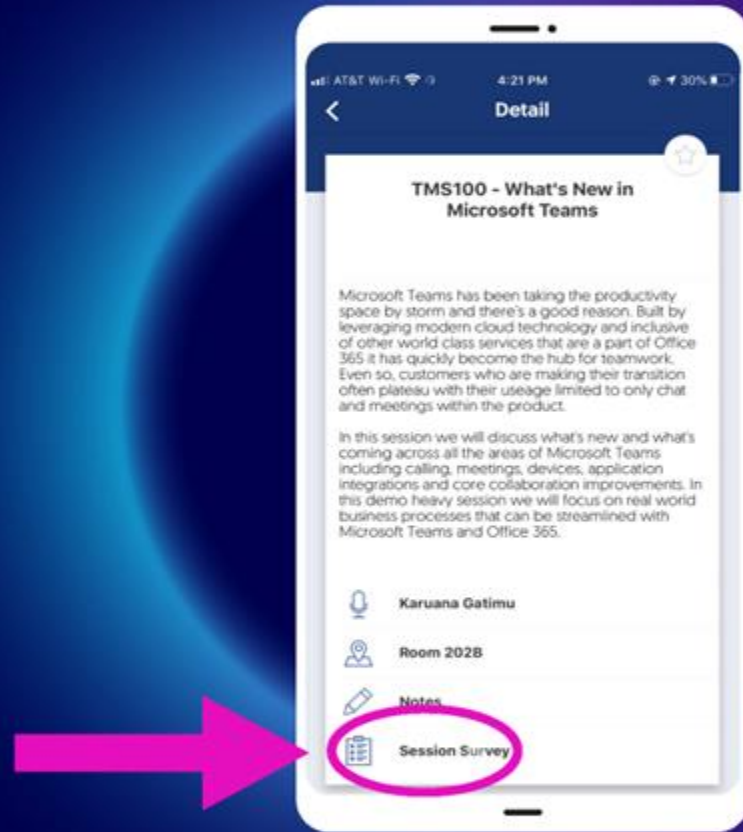
CONCLUSION

- 1 EXPLORE AUTOMATED INVESTIGATION AND RESPONSE (AIR)
- 2 EVALUATE YOUR REQUIREMENTS
- 3 PLAN YOUR DEPLOYMENT
- 4 ENABLE AUTOMATED INVESTIGATION AND RESPONSE (AIR)
- 5 MONITOR AND ADJUST AS REQUIRED

How was the session?

Search for **365 EduCon** in the App Store or Google Play

Fill out the Session Surveys in the **365 EduCon App** and be eligible to win **PRIZES!**





THANK YOU

LIAM CLEARY



www.helloitsliam.com



www.linkedin.com/in/liamcleary



twitter.com/helloitsliam