#CIAOPS

Microsoft 365 Incident Response

October 2023

@directorcia

http://about.me/ciaops

Before 70%

During 20%

After 10%

Before

Assess Risk

- What actually has value and requires protection?
- You can't eliminate risk
- Which has the higher ROI ? 98% of $1000 vs 0.1% of 1,000,000
- What are the high value assets (HVA)?

Risk Assessment

- Do a risk assessment
  - External users
  - External entities (i.e. web sites and DNS)
  - Remote workers
  - Third party apps
- Where are the major risk going to come from?
  - Typically, outside the organisation
  - But insider threats are growing
- Deal with the highest and most likely risks first
  - Email is the most likely
  - Browser is next
- How are externals managed?
- How are suppliers managing their own environments?

Communications

- Agree on the medium
- Keep it simple
- Chain of command?
- Who needs to access it?
- Who needs to be included?
  - Insurance companies
- Who needs to be excluded?
- How often will updates occur
- Where can progress be viewed?
- Get help when needed

Regulation

- Is growing
- Is changing
- Government
  - Privacy act
  - Data Breach
  - Will we see something like GDPR?
- Industry
- Are you aware of the regulations your business needs to comply

OAIC puts MSPs on notice over data breach reporting

By Chris Player
Jan 29 2021
12:47PM

0 Comments

The Office of the Australian Information Commissioner (OAIC) has sounded a warning to managed service providers (MSPs) to ensure they are reporting breaches, even if their customers do not.

In the latest *Notifiable Data Breaches Report* [pdf] which covered the second half of 2020, the Commissioner warned MSPs that it was the responsibility of both the holder and the customer to determine which party would report a data breach to the Government.

The OAIC said it had received a number of notifications involving an MSP hosting or holding data on behalf of one or more customers.

The OAIC has stated that it considers a data breach at a customer to be a data breach at the MSP and vice versa.

While both entities are not required to report, at least one is and the OAIC warned that MSPs needed to establish this clearly with the customer.

RELATED ARTICLES

Ex-Microsoft exec Colin Gniel joins Canberra MSP The Factor

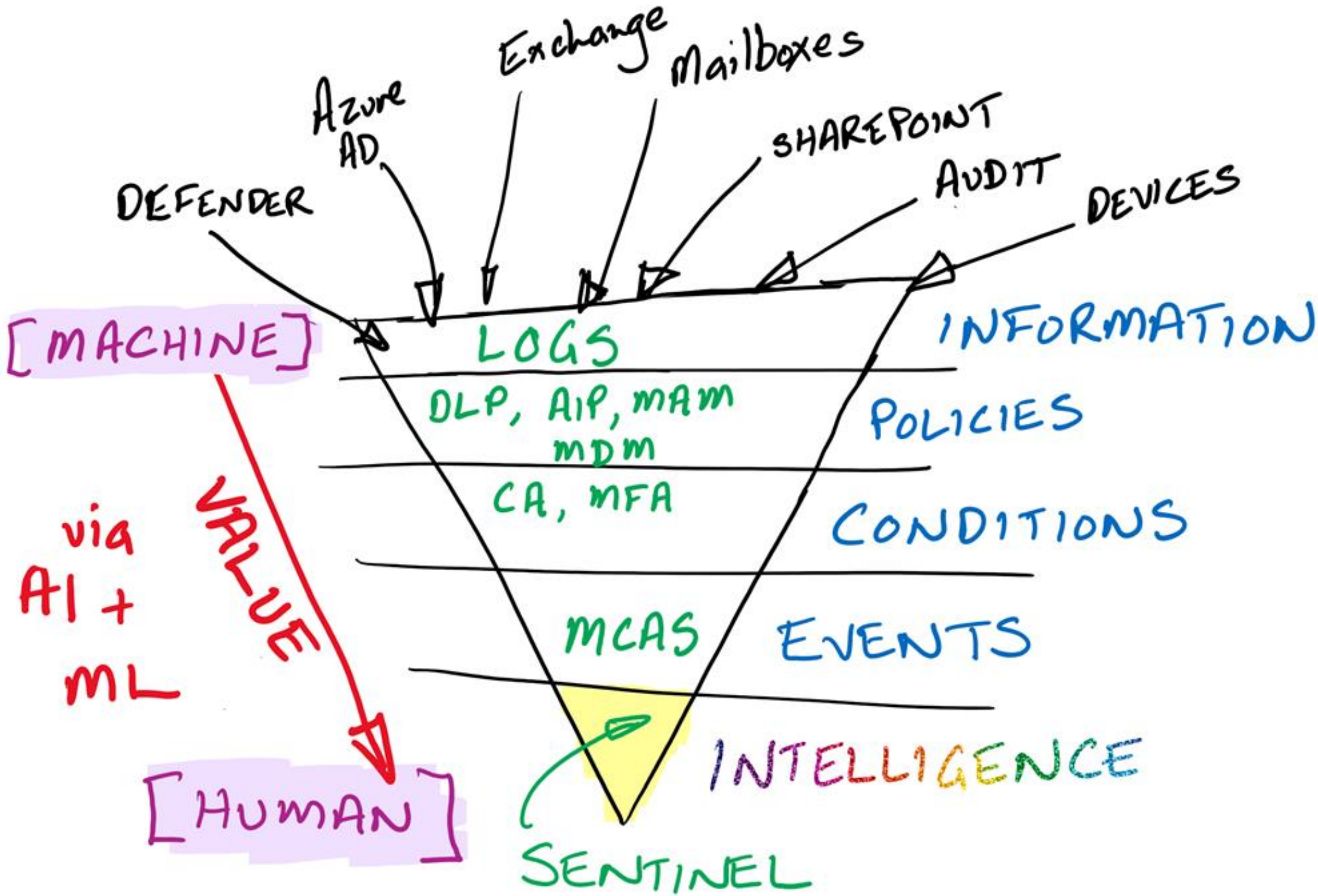
Melbourne's LiveTiles cuts staff, chief exec resigns

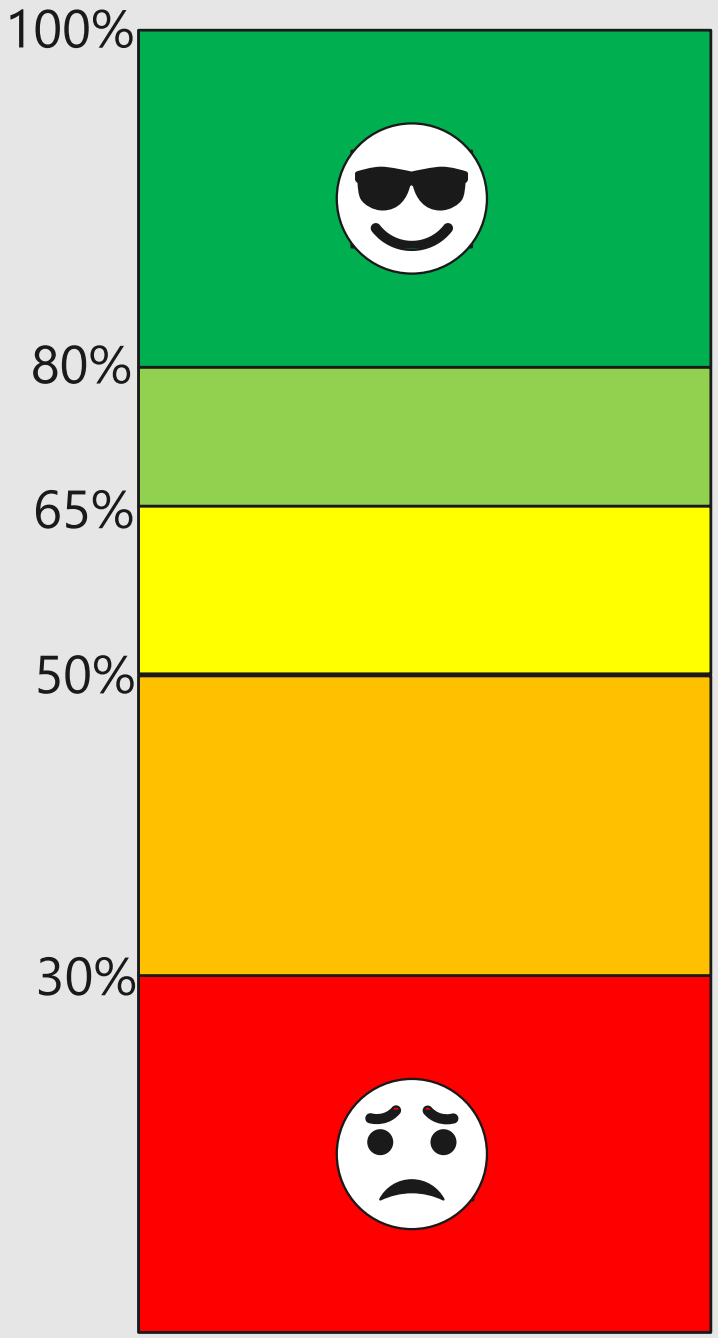

TIME
IS
MONEY

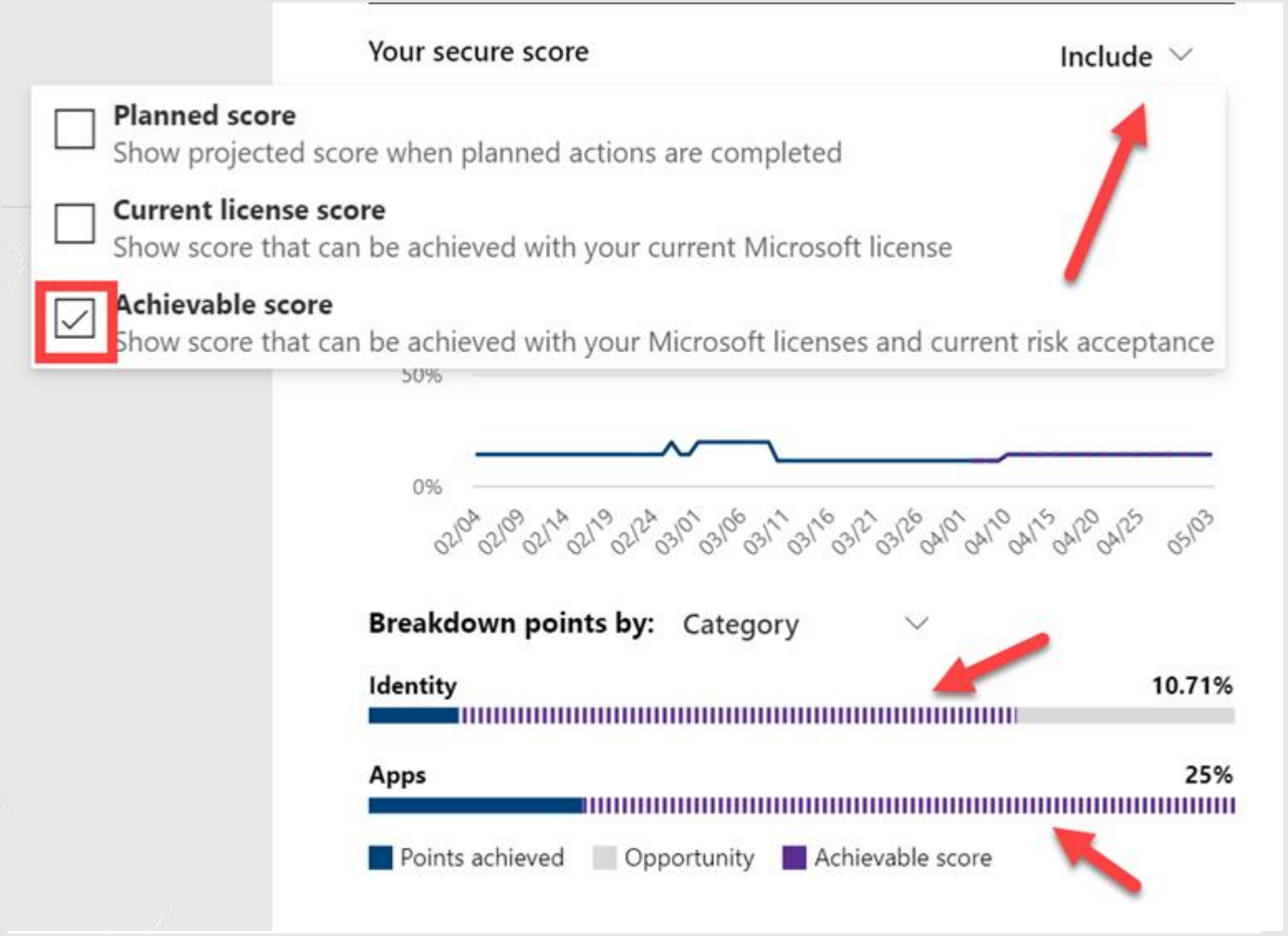
Do you deploy commercial grade antivirus and firewalls across your network? ☐ Yes ☐ No

Do you password protect all portable media including smartphones, tablet and memory sticks? ☐ Yes ☐ No

Please confirm whether multi-factor authentication is required for *all remote access to your network*: ☐ Yes ☐ No


Exchange
Mailboxes
Azure AD
SHAREPOINT
AUDIT
DEVICES
DEFENDER
[MACHINE]
LOGS
INFORMATION
DLP, AIP, MAM
MDM
POLICIES
CA, MFA
CONDITIONS
via AI + ML
VALUE
MCAS
EVENTS
[HUMAN]
INTELLIGENCE
SENTINEL


100%
80%
65%
50%
30%


Your secure score
Include
Planned score
Show projected score when planned actions are completed
Current license score
Show score that can be achieved with your current Microsoft license
Achievable score
Show score that can be achieved with your Microsoft licenses and current risk acceptance
50%
0%
02/04
02/09
02/14
02/19
02/24
03/01
03/06
03/11
03/16
03/21
03/26
04/01
04/10
04/15
04/20
04/25
05/03
Breakdown points by: Category
Identity
10.71%
Apps
25%
Points achieved
Opportunity
Achievable score

ance Manager

assification

nnectors

scopes

t search

unication compliance

ss prevention

very

ecycle management

tion protection

Audit

Learn about audit

New Search | Classic Search | Audit retention policies (Preview)

Searches completed | Active searches | Active unfiltered searches

Date and time range (UTC) *

Start: Oct 17 00:00

End: Oct 18 00:00

Activities - friendly names

Choose which activities to search for

Activities - operation names

Enter operation values, separated by commas

Users

Add the users whose audit logs you want to sea...

File, folder, or site

Enter all or a part of the name of a file, website,...

Keyword Search

Enter the keyword to search for

Record types

Select the record types to search for

Workloads

Enter the workloads to search for

Admin Units

Choose which Admin Units to search for

Search name

Give the search a name

Search | Clear all

Copy this search | Delete | Refresh

0 items

Search name	Job status	Progress ...	Search ti...	Total results	Creation time (...	Search performed by

New default retention period for activity logs

Starting in October 2023, we began rolling out changes to extend **default retention to 180 days** from 90 for audit logs generated by Audit (Standard) customers. Audit (Premium) license holders will continue with a default of one year, and the option to extend up to 10 years. Our public roadmaps detail when retention changes will reach your organization, starting with worldwide enterprise customers and quickly followed by our government customers in accordance with our standard service rollout process. This update helps all organizations minimize risk by increasing access to historical audit log activity data that is critical when investigating the impact from a security breach incident or accommodating a litigation event.

ciaopslabs | Sign-ins

Azure Active Directory

- Overview
- Preview features
- Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations

Download | Export Data Settings | Troubleshoot | Refresh | Columns | Got feedback?

Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : **Last 24 hours** | Show dates as : **Local** | Add filters

User sign-ins (interactive) | User sign-ins (non-interactive) | Service principal sign-ins | Managed identity sign-ins

Date	Request ID	User	Application	Status	IP address	Location
8/2/2021, 1:42:19 PM	89d68567-99e9-4fb...	09dabc45-a14b-47a...	Azure Portal	Interrupted	203.129.21.57	
8/2/2021, 1:39:58 PM	37a89011-e1c3-477...	Robert Crane	Microsoft App Acces...	Success	203.129.21.57	Coogee, New South
8/2/2021, 1:39:50 PM	ca294ba3-5859-49d...	Robert Crane	My Profile	Success	203.129.21.57	Morwell, Victoria, AU
8/2/2021, 1:39:39 PM	a231f36d-f776-4c7e...	Robert Crane	Azure Portal	Success	203.129.21.57	Morwell, Victoria, AU
8/2/2021, 1:39:37 PM	bfc6db96-ab38-47bf...	Robert Crane	Azure Portal	Interrupted	203.129.21.57	Coogee, New South

How long does Azure AD store the data?

Activity reports

Report	Azure AD Free	Azure AD Premium P1	Azure AD Premium P2
Audit logs	7 days	30 days	30 days
Sign-ins	7 days	30 days	30 days
Azure AD MFA usage	30 days	30 days	30 days

Security signals

Report	Microsoft Entra ID Free	Microsoft Entra ID P1	Microsoft Entra ID P2
Risky users	No limit	No limit	No limit
Risky sign-ins	7 days	30 days	90 days

Mailbox actions logged by mailbox audit logging

When you enable mailbox audit logging for a mailbox, access to the mailbox and certain administrator and delegate actions are logged by default. To log actions taken by the mailbox owner, you must specify which owner actions should be audited.

Action	Description	Admin	Delegate	Owner
Copy	An item is copied to another folder.	Yes	No	No
Create	An item is created in the Calendar, Contacts, Notes, or Tasks folder in the mailbox; for example, a new meeting request is created. Note that message or folder creation isn't audited.	Yes[1]	Yes[1]	Yes
FolderBind	A mailbox folder is accessed.	Yes[1]	Yes[2]	No
HardDelete	An item is deleted permanently from the Recoverable Items folder.	Yes[1]	Yes[1]	Yes
MailboxLogin	The user signed in to their mailbox.	No	No	Yes[3]
MessageBind	An item is accessed in the reading pane or opened.	Yes	No	No
Move	An item is moved to another folder.	Yes[1]	Yes	Yes
MoveToDeletedItems	An item is moved to the Deleted Items folder.	Yes[1]	Yes	Yes
SendAs	A message is sent using Send As permissions.	Yes[1]	Yes[1]	No
SendOnBehalf	A message is sent using Send on Behalf permissions.	Yes[1]	Yes	No
SoftDelete	An item is deleted from the Deleted Items folder.	Yes[1]	Yes[1]	Yes
Update	An item's properties are updated.	Yes[1]	Yes[1]	Yes

```
C:\Windows\System32>auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               Success and Failure
  System Integrity                        Success and Failure
  IPsec Driver                            No Auditing
  Other System Events                     Success and Failure
  Security State Change                   Success
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success
  Account Lockout                         Success and Failure
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           Success
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   Success and Failure
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             Success and Failure
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              Success and Failure
```

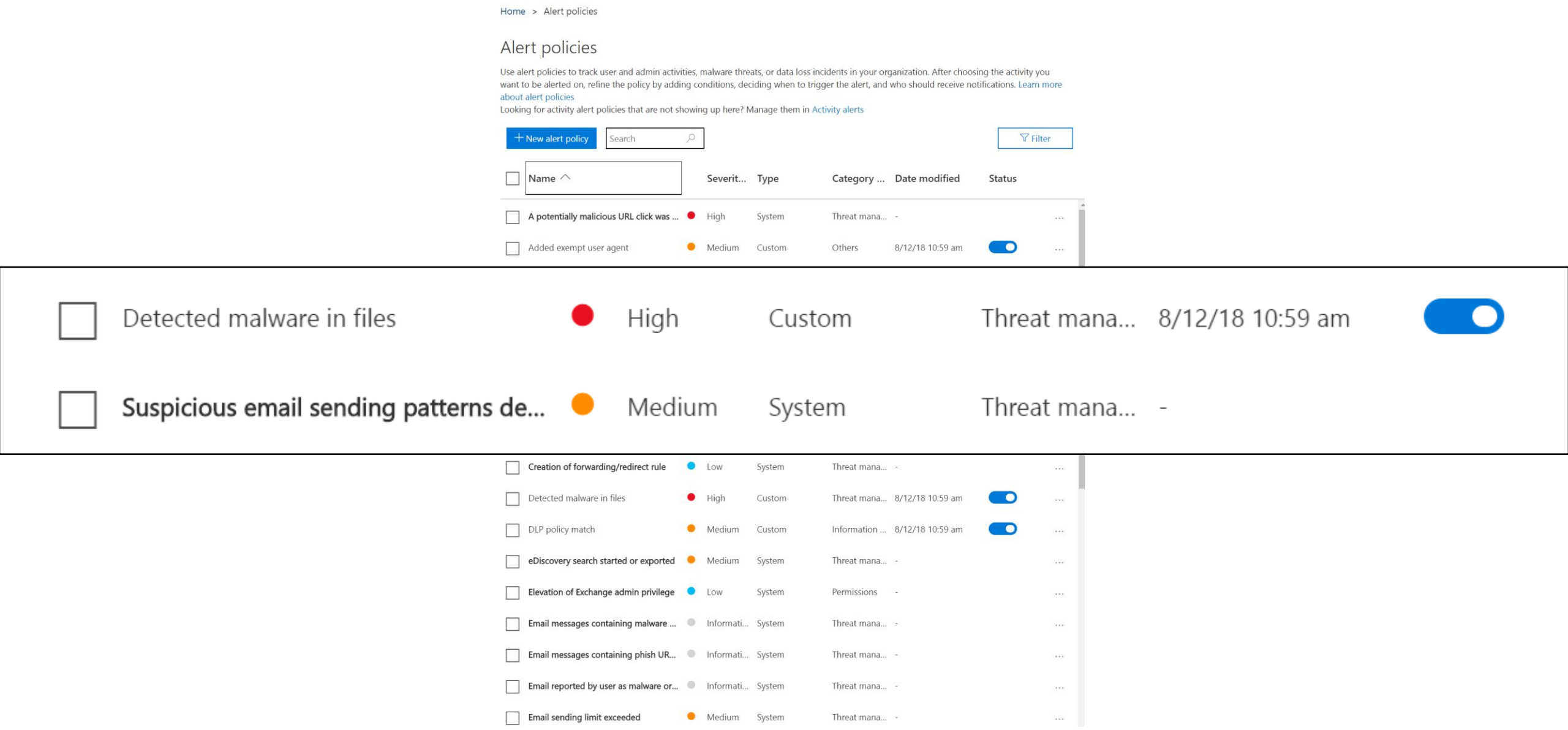
```
Attack Surface Reduction Rules

16 of 16 ASR rules found active

Block executable content from email client and webmail = Enabled
Block all Office applications from creating child processes = Enabled
Block Office applications from creating executable content = Enabled
Block Office applications from injecting code into other processes = Enabled
Block JavaScript or VBScript from launching downloaded executable content = Enabled
Block execution of potentially obfuscated scripts = Enabled
Block Win32 API calls from Office macros = Enabled
Block executable files from running unless they meet a prevalence, age, or trusted list crit
erion = Enabled
Use advanced protection against ransomware = Enabled
Block credential stealing from the Windows local security authority subsystem (lsass.exe) =
Enabled
Block process creations originating from PSExec and WMI commands = Enabled
Block untrusted and unsigned processes that run from USB = Enabled
Block Office communication application from creating child processes = Enabled
Block Adobe Reader from creating child processes = Enabled
Block persistence through WMI event subscription = Enabled
Block abuse of exploited vulnerable signed drivers = Enabled

Script completed
```

Protection Alerts



https://protection.office.com/alertpolicies

Activity Alerts

Home > Manage alerts

Activity alerts

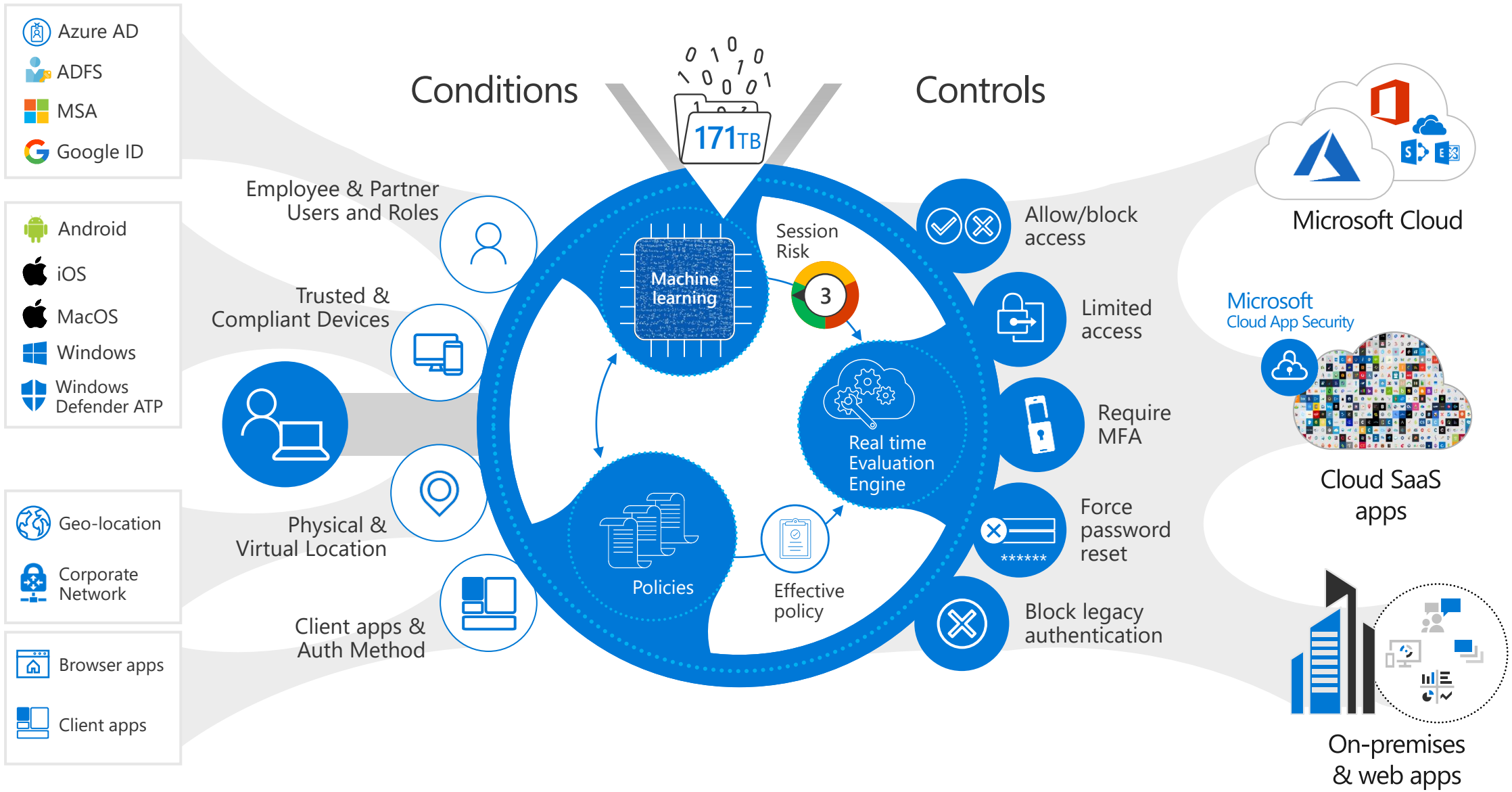
! We are working on a better experience for you to manage and view security and compliance alerts. Go to Alert policies

+ New alert policy

Name	Recipients	Status	Date modified
Role Alert	admin@ciaops365.com	On	2018-07-03 13:01:37
Administrator Password change	director@ciaops.com	On	2017-10-03 18:17:45
Company Information Alert	admin@ciaops365.com	On	2018-07-03 13:01:37
File and Page Alert	admin@ciaops365.com	On	2018-07-03 13:01:29
Site Alert	admin@ciaops365.com	On	2018-07-03 13:01:32
Domain Alert	admin@ciaops365.com	On	2018-07-03 13:01:38
Sharing Alert	admin@ciaops365.com	On	2018-07-03 13:01:30
Access Alert	admin@ciaops365.com	On	2018-07-03 13:01:32
OneDrive sharing	admin@ciaops365.com	On	2017-05-07 10:51:06
Anonymous Links Alert	admin@ciaops365.com	On	2018-07-03 13:01:30
Office Alert	admin@ciaops365.com	On	2018-07-03 13:01:33
Password Alert	admin@ciaops365.com	On	2018-07-03 13:01:36
Mailbox Alert	admin@ciaops365.com	On	2018-07-03 13:01:34

https://protection.office.com/managealerts

Conditional Access + Identity Protection



Activity log

Investigate 6 months back

Queries: Select a query | Save as

Advanced filters

App: **Select apps** | User name: **Robert Crane (admin@ciaops365.com)** | Raw IP address: Enter IP address

Activity type: **Select value** | Location: **Select countries/regions**

New policy from search | Export | 1 - 20 of 5,000+ activities | Show details | Hide filters | Table settings

Activity	User	App	IP address	Loca...	Device	Date
Log on	Robert Crane	Microsoft...	210.55.146.203	New Ze...		19 Oct 2023 8:...

SHOW SIMILAR | General | User | IP address | Send us feedback...

Robert Crane

Groups: Microsoft 365 adminis...

INTERNAL ADMINISTRATOR

Go to user page

User actions

ACTIVE INCIDENTS: 25

MATCHES: 0

ACTIVITIES: 5K

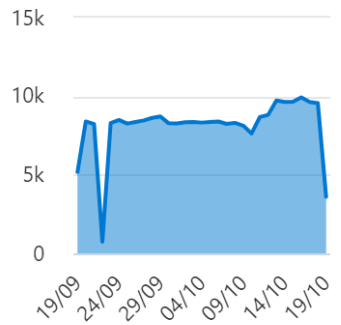
CONNECTED FROM (30 DAYS)

5 countries

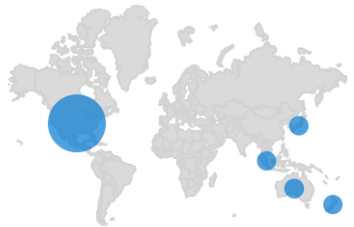
19 ISPs

148 IP addresses

USER ACTIVITIES (30 DAYS) See all



FREQUENT LOCATIONS



Activity	User	App	IP address	Loca...	Device	Date
Log on	Robert Crane	Microsoft...	210.55.146.203	New Ze...		19 Oct 2023 8:...

Azure Sentinel | Data connectors

Selected workspace: 'ciaops'

Search (Ctrl+/)

General
- Overview
- Logs
- News & guides

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

Configuration
- Data connectors
- Analytics
- Watchlist (Preview)
- Playbooks
- Community
- Settings

Guides & Feedback | Refresh

74 Connectors | 8 Connected | 0 Coming soon

Search by name or provider | Providers : All | Data Types : All | Status : All

Status	Connector name
	AI Vectra Detect (Preview) — Vectra AI
	Alcide kAudit (Preview) — Alcide
	Amazon Web Services — Amazon
	Azure Active Directory — Microsoft
	Azure Active Directory Identity Protection — Microsoft
	Azure Activity — Microsoft
	Azure DDoS Protection — Microsoft
	Azure Defender — Microsoft
	Azure Defender for IoT — Microsoft
	Azure Firewall — Microsoft

Azure Active Directory

Connected (Status) | Microsoft (Provider) | 2 hours ago (Last Log Received)

Description

Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Azure Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

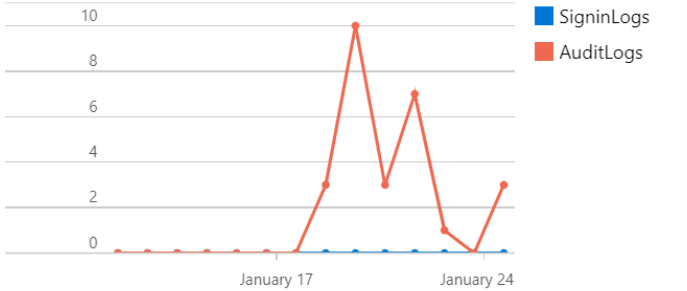
Last data received

01/25/21, 02:00 PM

Related content

6 Workbooks | 2 Queries | 36 Analytic rules templates

Data received — Go to log analytics



Total data received | Total data received

Threat management

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

Configuration

- Data connectors
- Analytics
- Watchlist (Preview)
- Playbooks
- Community
- Settings

Search | Severity : All | Rule Type : All | Status : All | Tactics : All

SEVERITY	NAME	RULE TYPE	STATUS	TACTICS
High	Known Strontium group domains	Scheduled	Enabled	Commar
High	Known IRIDIUM IP	Scheduled	Enabled	Commar
High	Known Phosphorus group domains/IP	Scheduled	Enabled	Commar
High	Create incidents based on Azure Security Center al...	Microsoft Secur...	Enabled	
High	Create incidents based on Azure Active Directory I...	Microsoft Secur...	Enabled	
High	Advanced Multistage Attack Detection	Fusion	Enabled	
High	Create incidents based on Azure Advanced Threat ...	Microsoft Secur...	Enabled	
High	Create incidents based on Microsoft Defender Adv...	Microsoft Secur...	Enabled	
High	Create incidents based on Microsoft Cloud App Se...	Microsoft Secur...	Enabled	
High	Known Manganese IP and UserAgent activity	Scheduled	Enabled	
High	Create incidents based on Office 365 Advanced Th...	Microsoft Secur...	Enabled	
High	Suspicious application consent similar to O365 Att...	Scheduled	Enabled	
High	First access credential added to Application or Ser...	Scheduled	Enabled	Credenti
Medium	Failed AzureAD logons but success logon to host	Scheduled	Enabled	
Medium	Malware in the recycle bin	Scheduled	Enabled	Defense
Medium	CIAOPS - URL detonation	Scheduled	Enabled	
Medium	Suspicious number of resource creation or deploy...	Scheduled	Enabled	Impact
Medium	SSH Potential Brute Force	Scheduled	Enabled	Credenti
Medium	Rare high NXDomain count	Scheduled	Enabled	Commar
Medium	SharePointFileOperation via devices with previousl...	Scheduled	Enabled	Exfiltratic
Medium	Process executed from binary hidden in Base64 en...	Scheduled	Enabled	
Medium	Brute force attack against Azure Portal	Scheduled	Enabled	Credenti
Medium	SSH newly internet-exposed endpoints	Scheduled	Enabled	Initial Ac
Medium	Multiple users email forwarded to same destination	Scheduled	Enabled	
Medium	User account created and deleted within 10 mins	Scheduled	Enabled	

High
Severity

Enabled
Status

Id
d0fe6fe9-d84d-4186-aab1-f05ca5c32994

Description
Matches domain name IOCs related to Phosphorus group activity with CommonSecurityLog, DnsEvents, OfficeActivity and VMConnection dataTypes. References: https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/.

Tactics
Command and Control

Rule query

```
let timeframe = 1d;
let DomainNames = dynamic(["yahoo-verification.org",
"accounts-web-mail.com","customer-certificate.com","
"yahoo-verification.net","yahoo-verify.net","outlook
"com-identifier-servicelog.name","microsoft-update.b
"confirm-session-identifier.info","session-managemen
```

Rule frequency
Run query every **1 day**

Rule period
Last **1 day** data

Rule threshold
Trigger alert if query returns **more than 0** results

Event grouping
Group all events into a single alert

Suppression
Not configured

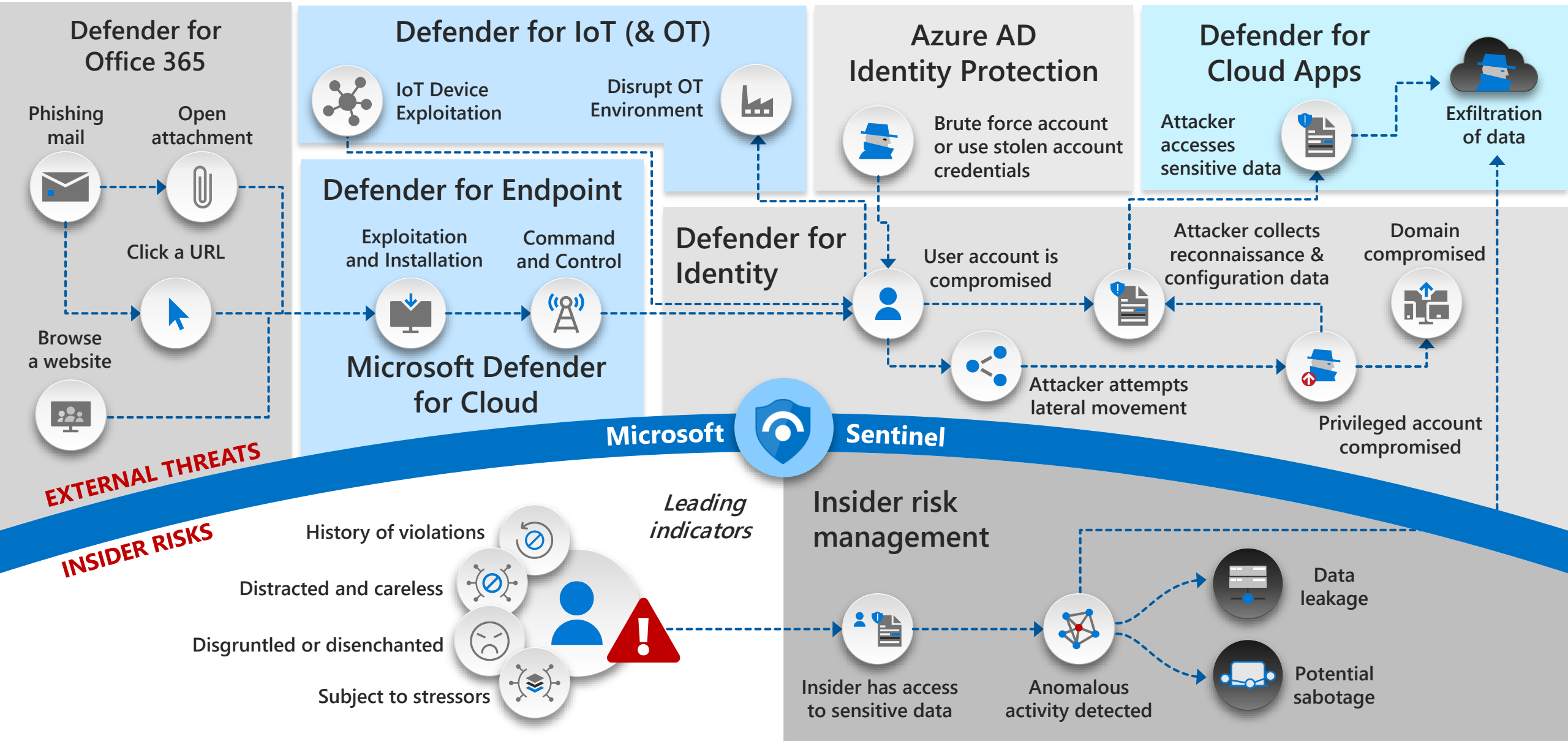
Create incidents from this rule
Enabled

Alert grouping
Disabled

Defend across attack chains

Insider and external threats

Microsoft December 2021 – https://aka.ms/MCRA



Converging Tools & Data

Engineering a single seamless system with automation

Single Portal Experience

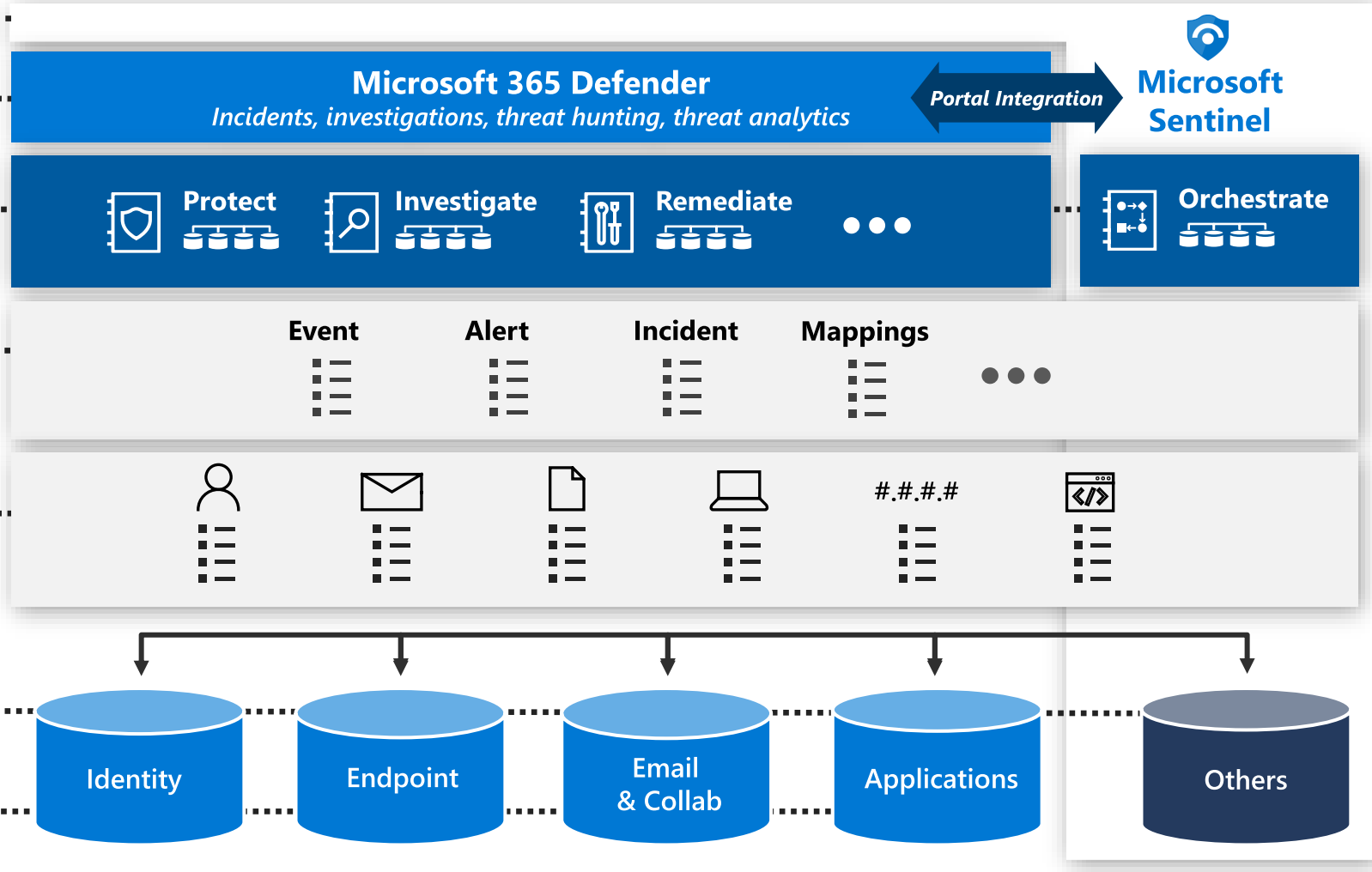
Playbook Automation
Ensure automation runs across all systems

Semantics and Meaning
Correlation, prioritization, orchestration, etc.

Unified entity definitions
Reputation for Users, machines, email, IPs, etc.

Signal sharing

Intelligent Capabilities
High Quality Detection and Data



During

Remember

1. Keep calm
2. Start documenting. Where will you keep all this?
3. Alert people who need to know
4. Contact people that you may need assistance from to let them know and confirm
5. Recon - do no harm initially
6. What is the impact?
7. Reporting cadence? Every two hours is suggested
8. Who is working on this?
9. Capture basic incident information, especially times
10. Get another opinion

Dump the logs as a snaphot

- Unified audit log
  - Export
  - Search
- Defender for Cloud Apps
  - Activity log | Export
- Azure AD logs
  - Download
- Do some basic filtering first to cut down the size
- HAWK - start-hawktenantinvestigation

Don’t forget the basics

- Licensing
- Devices
- Last logins
- Mailboxes

Sources of information

- Investigate alerts
- https://security.microsoft.com
  - Incidents
  - Alerts
  - Check automated investigations
- Sentinel
- Defender for Cloud Apps
- Email threat explorer
- Incident queue
- Unified Audit logs
- Automated responses
- What alert policies trigger automated investigations?
- Where will the alerts you want appear?

Take action

- Close out access area by area
- What needs to be disabled?
  - Disable user account in an automated way
  - Defender for Endpoint device isolation
  - Defender for Endpoint Restrict app execution
- What is the impact?
- What needs to be collected?
  - Collect investigation package from devices
- Don't disable everything

Devices > vm02

vm02

null resource | High

Device value ···

Overview | Incidents and alerts | Security recommendations | Device configuration

VM details

Domain	OS
AAD joined	Windows 11 64-bit (Release 21H2 Build 22000.2295)
SAM name	Asset group
-	-
Health state	IP addresses
Inactive	192.16

Active alerts (Last 180 days)

Risk level: High

3 active alerts, 2 active incidents

Active alerts

High (2) Low (1)

View all incidents and alerts

Security assessments

Exposure level: High

17 active security recommendations

- Manage tags
- Report device inaccuracy
- Run Antivirus Scan
- Collect Investigation Package
- Restrict App Execution
- Initiate Automated Investigation
- Initiate Live Response Session
- Isolate Device
- Action center
- Download force release from isolation script
- Exclude
- Go hunt
- Turn on troubleshooting mode
- Policy sync

SU

Super User

Administrator

Confirm user compromised ···

- Suspend user in Azure AD
- Require user to sign in again
- Azure AD account settings
- View related activity
- View related governance
- View owned files
- View files shared with this user
- View related incidents
- Microsoft 365

Overview | Alerts (4) | Observed in organization | Timeline

Entity details

User threat

Azure AD Identity risk level

Medium

Observed in organization

Last Seen	First Seen
10/27/2023	—

Lateral movement paths	Devices
0	0

Groups	Locations

Incidents and Alerts

4 alerts over 7 incidents

Open alerts by severity

Low | Informational

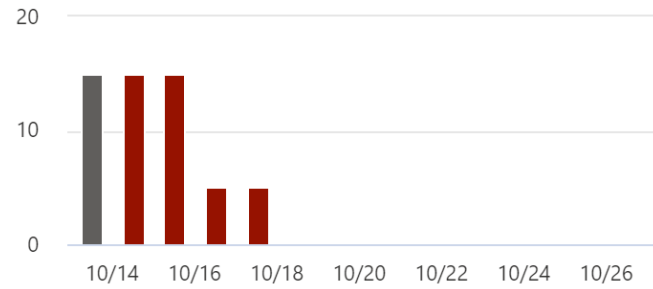
View all alerts

Investigation Priority

Score: 0

This user has no alerts or risky activ
score from the past week.

Investigation priority score over the last 2 weeks



Active Directory account controls

Data is not available

Action Center

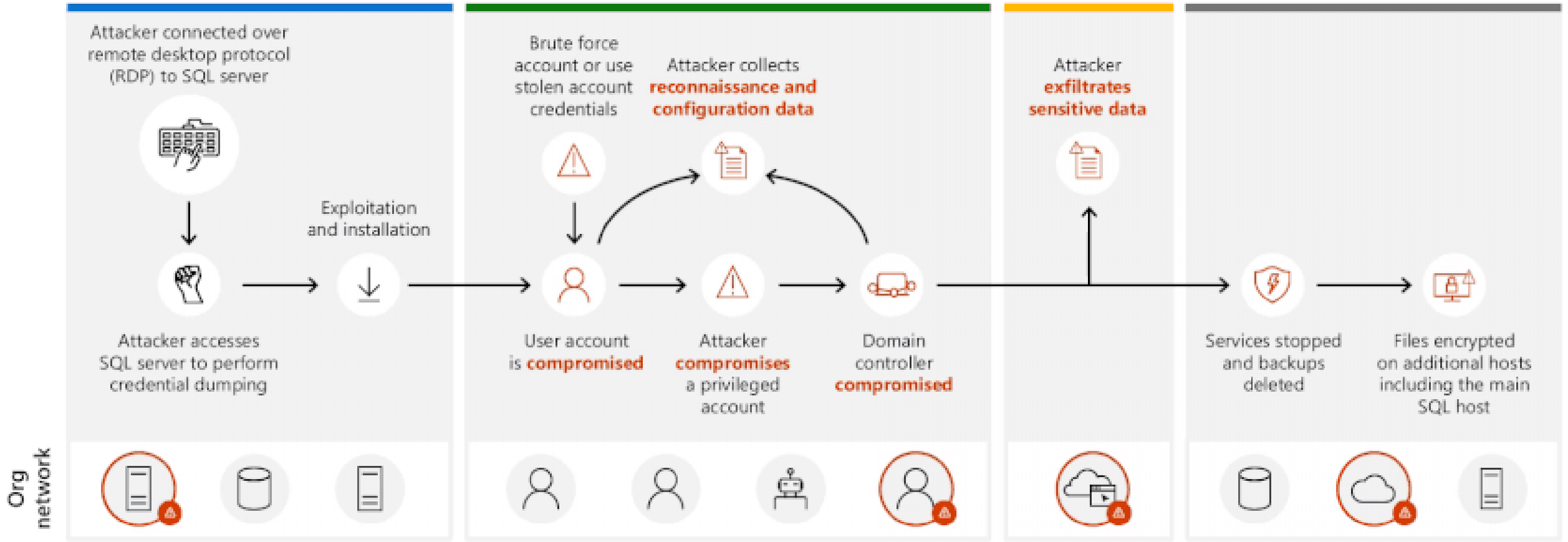
Email Notifications

Pending | History

Export | 1-8 of 8 | 6 months | Choose columns | 30 items per page | Filters

Action update time	Investigation ID	Approval ID	Action type	Details	Entity type
Sep 29, 2023 2:55 PM			Stop isolation		
Sep 29, 2023 2:47 PM			Stop isolation		
Sep 26, 2023 4:44 PM			Stop isolation		
Sep 26, 2023 4:39 PM			Isolate device		
Sep 4, 2023 10:16 PM	20		Quarantine file	c:\windows\system32\eicar.com.txt	File
Jun 8, 2023 1:59 PM			Stop isolation		
Jun 8, 2023 1:56 PM			Isolate device		
May 3, 2023 11:32 AM	69fd5f		Live Response command	connect	

Without automatic attack disruption…



Hunting

- Do you have time for this?
- Is it going to be profitable?
- Who is paying?
- What are you looking for?
- Good UAL Hunting
- Forensic artifacts in Office 365 and where to find them
- KQL is a handy skill to have

Resolve

- When is the response done?
- Verify results
- Document summary
- An important piece of the puzzle that should be reviewed later
- Create a time line for review
- Report to someone

After

Celebrate

- Celebrate it is resolved
- Especially for those who worked on the incident
- Recognition is important

Report

- Does the incident need to be reported to anyone?
- Government
  - Report a data breach
- Management
- Board
- Insurance company

Initial entry

- How did they gain access?
- Is it worth investigating
- What information needs to provided?
- When does it need to be provided?

Mitigations

- What steps can be taken to prevent that reoccurring?
- Was it a technology failure or a human failure?
- How long will mitigations take?

Improvements

- How could the investigation process be improved?
- Review the entire process
- Automations

Log retention

- Do the log records need to be maintained?
- How long for?
- In what format?
- What about your own records about the work carried out?

https://bit.ly/cia-m365irt