



BCNET
CONNECT
HIGHER ED & RESEARCH TECH SUMMIT

Into the Microsoft Cloud:

A Security Prospective

Taylor Masson
Senior Information Security Analyst
Thompson Rivers University



BCNET
CONNECT

The Beginning

Are we there yet?

- Hybrid environment decided (Local and Cloud services)
- Lead to issues with email systems, slowdown when cloud accounts talk back to campus resources
- AD/AAD connection fine, Password writeback is a want (Soon a need)

New Features

- Easier email access
- Microsoft Teams and integration
- OneDrive Cloud
- More Email storage

New Risks

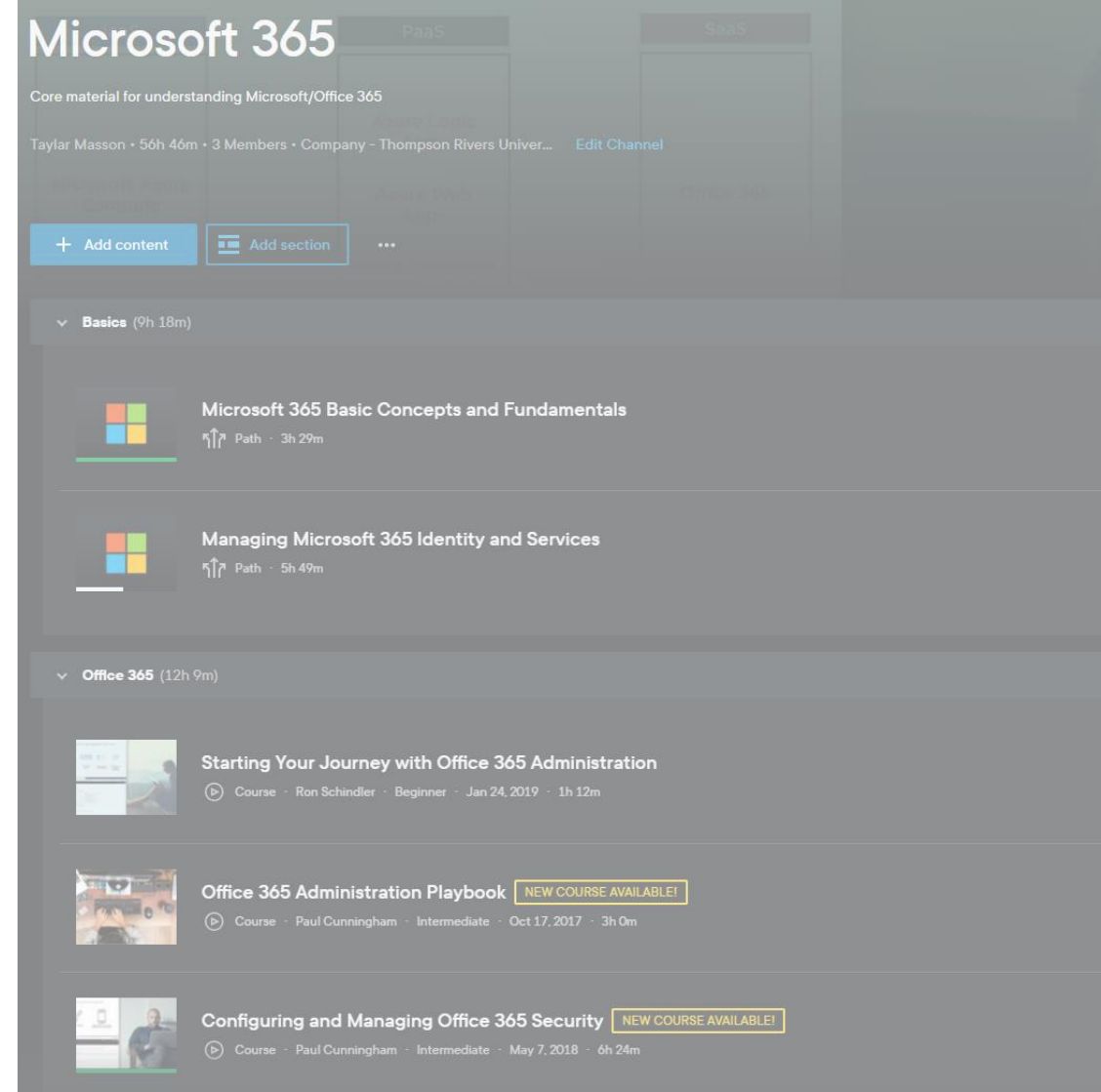
- Outlook.com is common target
- Our email addresses are public
- Constant brute force attempts we can't block
- Once into email has access to personal and shared directories, intranet, internal communications

Moving to A5

- TRU (from recommendation of Hugh Burley) changed licensing from A3 to A5 for all faculty/staff
- Adds many more security tools such as:
 - Cloud App Security (MCAS)
 - Azure P2
 - Defender for Identity
- Also increase log collection/visibility from accounts.
- Worth the price?

M365 training

- Pluralsight
- Good information
- Only problem, out of date
- Microsoft adding more tools, changing old
- Only way to keep up with changes was to dive into the product, watch for notices and get update emails from MS



Who's role is it anyway?

- MS not clear on what permissions are needed for what jobs
- Most sources stated that “Security Operator” would be enough for any daily task. Not the case.
- Eventually got Infosec team on “Security Administrator”, finding recently that even this isn't enough.
- MS has “RBAC” permissions carried over from an old product that isn't compatible with PIM.

ⓘ Note

The **Organization Management** role group exists in both Exchange Online and in the Microsoft 365 compliance center. These are separate role groups that give different permissions. Being a member of **Organization Management** in Exchange Online does not grant the required permissions to delete email messages. If you aren't assigned the **Search And Purge** role in the compliance center (either directly or through a role group such as **Organization Management**), you'll receive an error in Step 3 when you run the **New-ComplianceSearchAction** cmdlet with the message "A parameter cannot be found that matches para

ⓘ Note

To view the **Permissions** tab in the Security & Compliance Center, you need to be an admin. Specifically, you need to be assigned the **Role Management** role, and that role is assigned only to the **Organization Management** role group in the Security & Compliance Center by default. Furthermore, the **Role Management** role allows users to view, create, and modify role groups.

ⓘ Note

To view the **Permissions** tab in the Security & Compliance Center, you need to be an admin. Specifically, you need to be assigned the **Role Management** role, and that role is assigned only to the **Organization Management** role group in the Security & Compliance Center by default. Furthermore, the **Role Management** role allows users to view, create, and modify role groups.

Security Permissions Findings

- Security Operator can manage alerts, not much else
 - Security Reader grants all view permissions needed
 - Global Reader “always on” for most sites to work
 - Security Administrator doesn’t do all that it should
 - Global Admin is needed for too many tasks
-
- Don’t always play fair with PIM
 - Azure permissions aren’t always the same as S&C Center



BCNET
CONNECT

The Tools

Security Console – Alerts/Incidents

Incidents

Most recent incidents and alerts

1-30 < > 30 days Choose columns 30 items per page								
✓	Incident name	Tags	Severity	Investigation state	Categories	Impacted entities	Active alerts	Service sources
>	Activity from infrequent country involving one user		■ ■ ■ Medium	N/A	Defense evasion	🔍	1/1	Microsoft Defender for Cloud Apps
>	Suspected brute-force attack (Kerberos, NTLM) on one endpoint		■ ■ ■ Medium	N/A	Credential access	🔍	1/1	Identity
>	Impossible travel activity involving one user		■ ■ ■ Medium	N/A	Defense evasion	🔍	1/1	Microsoft Defender for Cloud Apps
>	Impossible travel activity involving one user		■ ■ ■ Medium	N/A	Defense evasion	🔍	1/1	Microsoft Defender for Cloud Apps
>	Impossible travel activity involving one user		■ ■ ■ Medium	N/A	Defense evasion	🔍	1/1	Microsoft Defender for Cloud Apps
>	Activity from infrequent country involving one user		■ ■ ■ Medium	N/A	Defense evasion	🔍	1/1	Microsoft Defender for Cloud Apps
>	Remote code execution attempt on multiple endpoints		■ ■ ■ Medium	N/A	Execution	🔍	1/1	Identity
>	Suspected brute-force attack (Kerberos, NTLM) on one endpoint		■ ■ ■ Medium	N/A	Credential access	🔍	1/1	Identity
>	Impossible travel activity involving one user		■ ■ ■ Medium	N/A	Defense evasion	🔍	1/1	Microsoft Defender for Cloud Apps
>	Mass download involving one user		■ ■ ■ Medium	N/A	Collection	🔍	1/1	Microsoft Defender for Cloud Apps
>	Suspected brute-force attack (Kerberos, NTLM) on one endpoint		■ ■ ■ Medium	N/A	Credential access	🔍	1/1	Identity
>	Impossible travel activity involving one user		■ ■ ■ Medium	N/A	Defense evasion	🔍	1/1	Microsoft Defender for Cloud Apps
>	Impossible travel activity involving one user		■ ■ ■ Medium	N/A	Defense evasion	🔍	1/1	Microsoft Defender for Cloud Apps
>	Suspected brute-force attack (Kerberos, NTLM) on one endpoint		■ ■ ■ Medium	N/A	Credential access	🔍	1/1	Identity
>	Suspected brute-force attack (LDAP) on multiple endpoints		■ ■ ■ Medium	N/A	Credential access	🔍	1/1	Identity
>	Suspected brute-force attack (Kerberos, NTLM) on one endpoint		■ ■ ■ Medium	N/A	Credential access	🔍	1/1	Identity
>	Suspicious network connection over Encrypting File System Remote Protocol on one endpoint	Vulnerability Scan	■ ■ ■ High	N/A	Lateral movement	🔍	0/1	Identity
>	Impossible travel activity involving one user		■ ■ ■ Medium	N/A	Defense evasion	🔍	1/1	Microsoft Defender for Cloud Apps
>	Impossible travel activity involving one user		■ ■ ■ Medium	N/A	Defense evasion	🔍	1/1	Microsoft Defender for Cloud Apps
>	Activity from infrequent country involving one user		■ ■ ■ Medium	N/A	Defense evasion	🔍	1/1	Microsoft Defender for Cloud Apps

Part of incident: Suspected brute-force attack (Kerberos, NTLM) on one endpoint. [View incident page](#)

707 Accounts
Related Accounts

2 Accounts
Suspect Accounts

Destination Host

4 Hosts
Related Hosts

What happened

An actor on successfully generated a suspicious number of failed login attempts on [679 accounts](#), while trying to access [2 accounts](#) eventually authenticated

Important information

Authentication failure details by date

- On 2/6/22 [120 accounts](#) each failed to authenticate from 1 times, exceeding the normal failure rate for that machine.
- On 2/5/22 [31 accounts](#) each failed to authenticate from 2 times, exceeding the normal failure rate for that machine.
- On 2/4/22 [3 accounts](#) each failed to authenticate from 77 times, exceeding the normal failure rate for that machine.
- On 2/3/22 failed to authenticate from 747 times, exceeding the normal failure rate for that machine.
- On 2/2/22 [49 accounts](#) each failed to authenticate from 2 times, exceeding the normal failure rate for that machine.
- On 2/1/22 [13 accounts](#) each failed to authenticate from 4 times, exceeding the normal failure rate for that machine.
- On 1/31/22 [41 accounts](#) each failed to authenticate from 2 times, exceeding the normal failure rate for that machine.
- Dec 8, 2021 4:06 PM - Feb 7, 2022 2:26 PM
[679 accounts](#) didn't update their password within the last 24 hours.
- None of the passwords attempted were previously used passwords.
- [679 accounts](#) weren't recently observed logging into .
- Jan 13, 2022 4:00 PM
[2 accounts](#) successfully logged in after multiple authentication failures.
- The suspicious authentication failures used [2 protocols](#).



Suspected brute-force attack (Kerberos, NTLM)

Medium Unknown New

[Manage alert](#) [Export](#) [Link alert to another incident](#) ...

Classify this alert

True alert

False alert

Alert state

Classification

Not Set

[Set Classification](#)

Assigned to

Unassigned

Alert details

Category

Credential access

MITRE ATT&CK Techniques

[T1110.001: Password ...](#) +1 More

[View all techniques](#)

Detection source

MDI

Service source

Microsoft Defender for Identity

Detection status

Unknown

Detection technology

-

Generated on

Dec 9, 2021 2:59:51 AM

First activity

Dec 8, 2021 4:06:10 PM

Last activity

Feb 7, 2022 10:46:13 AM

Security Console – Explorer

Explorer

Explorer is a powerful, near real-time tool to help Security Operations teams investigate and respond to threats in the Security & Compliance Center. [Learn more about Explorer.](#)

View All email

This view shows information about all email messages sent by external users into your organization, or internal email sent between your users. This view can help you find missed threats. You can filter the view for threat hunting, and you can export up to 200,000 records for offline analysis. [Show more](#)

Save query | Save query as | Saved query settings | Export

MDE Settings

Sender Refresh 2022-01-09 00:00 — 2022-01-14 23:59

Sender :

Delivery action

3k

Delivered Blocked Delivered to junk

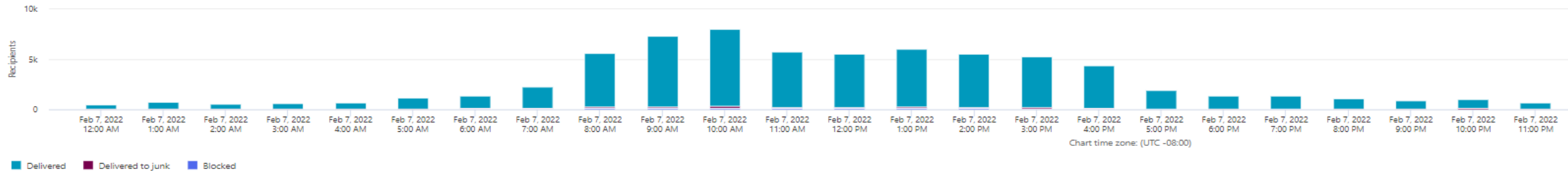


Explorer

All email Malware Phish Campaigns Content Malware

Sender Use commas (,) to separate multiple entries. Click Refresh to filter the results. Refresh

Delivery action



Email URL clicks Top URLs Top clicks Top targeted users Email origin Campaign

Security Console – Threat Hunting

[Run query](#) [Save](#) [Share link](#)

Query

```
1 EmailEvents
2 | where SenderFromDomain has "tru.ca"
3 | summarize Count = count() by SenderFromAddress
4 | top 10 by Count
```

SenderFromAddress	Count
noreply@moodle.tru.ca	7613
root@.tru.ca	5037
WhatsUpGold@tru.ca	4320
celt@tru.ca	2472
@tru.ca	1973
insidetru@tru.ca	1773
president@tru.ca	1753
@tru.ca	1694
tdxreplies@tru.ca	1671
lapply@tru.ca	1575

Advanced Hunting

Schema Functions Queries Detection Rules

Alerts

- AlertInfo
- AlertEvidence

Apps & Identities

- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents
- IdentityDirectoryEvents
- CloudAppEvents
- AADSpnSignInEventsBeta
- AADSignInEventsBeta

Email

- EmailEvents
- EmailAttachmentInfo
- EmailUrlInfo
- EmailPostDeliveryEvents

Devices

- DeviceInfo
- DeviceNetworkInfo
- DeviceProcessEvents
- DeviceNetworkEvents
- DeviceFileEvents
- DeviceRegistryEvents
- DeviceLogonEvents
- DeviceImageLoadEvents
- DeviceEvents
- DeviceFileCertificateInfo

Threat & Vulnerability Management

- DeviceTvmSoftwareVulnerabilities
- DeviceTvmSoftwareVulnerabilitiesKB
- DeviceTvmSecureConfigurationAssessment
- DeviceTvmSecureConfigurationAssessmentKB
- DeviceTvmSoftwareInventory
- DeviceTvmSoftwareEvidenceBeta

▶ Run query



Save ▾



Share link

Query

```
1 CloudAppEvents
2 | where UserAgent contains "jndi:"
3 or AccountDisplayName contains "jndi:"
4 or Application contains "jndi:"
5 or AdditionalFields contains "jndi:"
6 | project Timestamp, ReportId, ActivityType, Application, AccountDisplayName, IPAddress, UserAgent, AdditionalFields
```

Azure (P2) – Risky Sign ins

Risky sign-ins

Download Learn more Export Data Settings Configure trusted IPs Troubleshoot

Auto refresh : Off Date : Last 7 days Show dates as : Local Risk state : 2 selected
Detection type(s) : None Selected Sign-in Type : 2 selected Add filters

<input type="checkbox"/> Date ↑↓	User ↑↓	IP address
<input type="checkbox"/> 2/23/2022, 11:15:13 AM		223.233.65.
<input type="checkbox"/> 2/22/2022, 7:49:50 PM		185.171.60.
<input type="checkbox"/> 2/22/2022, 12:28:13 PM		52.254.53.
<input type="checkbox"/> 2/22/2022, 12:03:29 PM		207.228.78.
<input type="checkbox"/> 2/21/2022, 6:41:47 PM		174.4.149.
<input type="checkbox"/> 2/21/2022, 2:53:26 PM		54.164.70.
<input type="checkbox"/> 2/21/2022, 12:42:19 PM		172.225.43.
<input type="checkbox"/> 2/20/2022, 1:20:24 PM		172.225.43.
<input type="checkbox"/> 2/20/2022, 1:20:24 PM		172.225.43.
<input type="checkbox"/> 2/20/2022, 1:20:24 PM		172.225.43.
<input type="checkbox"/> 2/20/2022, 1:16:31 PM		172.225.43.

User's risk report User's sign-ins User's risky sign-ins

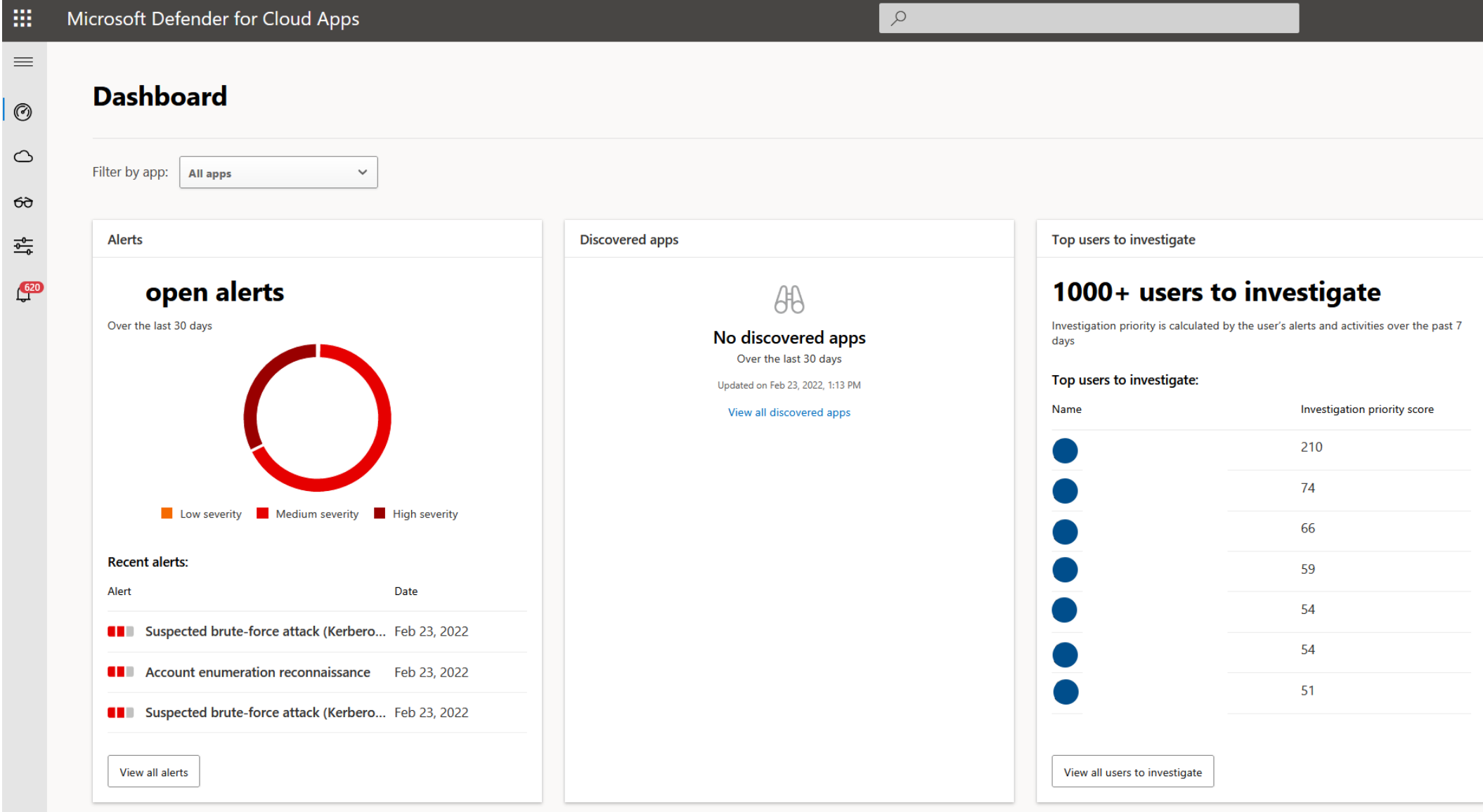
Basic info	Device info	Risk info	MFA info
Request ID	043ae376-0b33-4d77-8efb-		
Correlation ID	f783a304-3406-4ea0-a835-		
Sign-in Type	Interactive		
User			
Username			
User ID	d2940a1e-ce34-40a4-a406-		
Application	Office 365 Exchange Online		
Application ID	00000002-0000-0ff1-ce00-000000000000		
Resource	Office 365 Exchange Online		
Resource ID	00000002-0000-0ff1-ce00-000000000000		
IP address	185.171.60.		
Location	AL		
Date	2/22/2022, 7:49:50 PM		




Into The Microsoft Cloud

https://portal.azure.com/#blade/Microsoft_AAD_IAM/RiskySignInsBlade

Microsoft Cloud App Security (MCAS) (A5)





MCAS – Alerts


Alerts >  **Impossible travel activity** 2/21/22 6:43 PM

+35


MEDIUM SEVERIT

 Impossible travel

 Office 365



 2 IP addresses

 2 Countries

Close alert


Description

The user was involved in an impossible travel incident. The user connected from two countries within 1 minutes, from these IP addresses: Canada (174.4.149.) and Vietnam (113.185.44.). If any of these IP addresses are used by the organization for VPN connections and do not necessarily represent a physical location, we recommend categorizing them as VPN in the IP Address range page in Microsoft Defender for Cloud Apps portal to avoid false alerts.








Important information

- Vietnam was visited for the first time in 180 days by this user.
- ISP ip adsl static + cable tv voip was used for the first time in 180 days in your organization.
- User agent Edge was used for the first time in 180 days by this user.
- This alert falls under the following [MITRE](#) tactic: Defense Evasion

Activity log

 Investigate in Activity log

1 - 2 of 2 activities ⓘ [↔ Show details](#) [⚙ Table settings](#) ▾

Activity	User	App	IP address	Location	Device	Date ▾
 Log on		 Office 365	113.185.44.	Vietnam		Feb 21, 2022, 6:43 PM <div></div>
 Log on		 Office 365	174.4.149.	Canada		Feb 21, 2022, 6:41 PM <div></div>



Into The Microsoft Cloud



Taylor Masson
Information Tech Analyst-AUX
IT Services\Information Security

[View related activity](#) [View related governance](#) [View related alerts](#) ...

User summary

User threat

Investigation priority
19

Open alerts
0

Identity risk level
Medium

User exposure

Last seen
Feb 23, 2022

Accounts
4

Devices
24

Logon Types
2

Locations
2

Matched files
0

Contact information

Email
tmasson@tru.ca

Phone
1-250-828-5327

Manager
John Cuzzola

Address
INFORMATION TECHNOLOGY SERVICES BC CENTRE F...

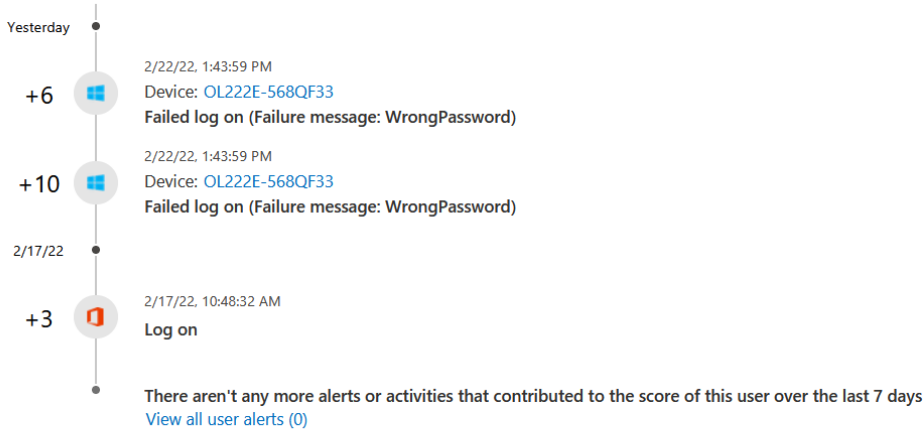


Investigation priority score

Score is based on the last 7 days [How do we score?](#) User score in the last two weeks



Alerts and activities that contributed to the score (last 7 days) [View all user alerts \(0\)](#)



Into The Microsoft Cloud



BCNET
CONNECT

Policies

Security Console – Secure Score

- Helpful guideline on what changes will make the most security impact

[Overview](#) [Improvement actions](#) [History](#) [Metrics & trends](#)

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

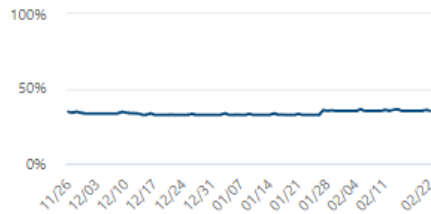
Applied filters:

Your secure score

Include ▾

Secure Score: 35.23%

66.24/188 points achieved



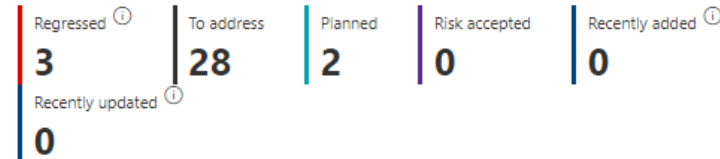
Breakdown points by: Category ▾

Identity 34.64%

Apps 36.26%

■ Points achieved ■ Opportunity

Actions to review

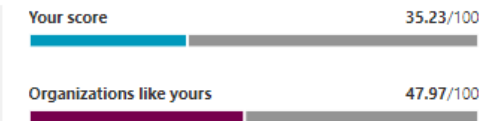


Top improvement actions

Improvement action	Score impact	Status	Category
Ensure all users can complete multi-factor authentic...	+4.79%	<input type="radio"/> To address	Identity
Create Safe Links policies for email messages	+4.79%	<input type="radio"/> To address	Apps
Do not expire passwords	+4.26%	<input checked="" type="radio"/> Planned	Identity
Turn on Safe Attachments in block mode	+4.26%	<input type="radio"/> To address	Apps
Enable policy to block legacy authentication	+4.26%	<input checked="" type="radio"/> Planned	Identity
Turn on sign-in risk policy	+3.72%	<input type="radio"/> To address	Identity
Turn on user risk policy	+3.72%	<input type="radio"/> To address	Identity

[View all](#)

Comparison



















Messages from Microsoft

Get the inside scoop from Microsoft Security.

[See recent blogs](#)

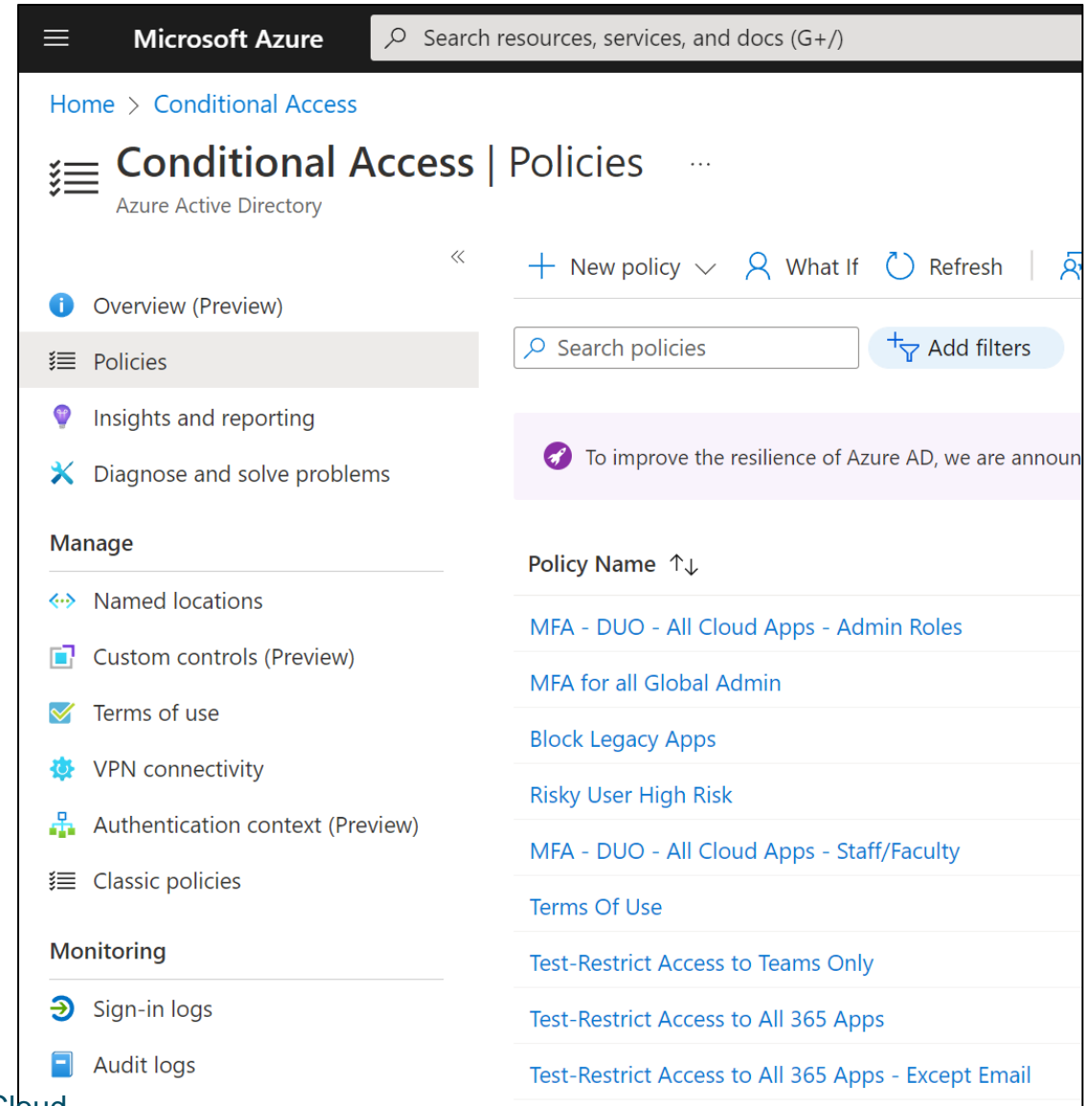
MCAS - Policies

- Gives lots of noise, needs tuning. Where possible

Policy	Count	Severity ▾	Category
 Risky sign-in Azure Active Directory (Azure AD) detects suspicious actions that are related to your user accounts. ...	open alerts	■■■ High	 Threat detection
 Malicious OAuth app consent This policy uses Microsoft Threat Intelligence to scan OAuth apps connected to your environment a...	0 open alerts	■■■ High	 Threat detection
 Suspected Golden Ticket usage (time anomaly) Attackers with domain admin rights can compromise the KRBTGT account. Using the KRBTGT accou...	0 open alerts	■■■ High	 Threat detection
 Suspected identity theft (pass-the-hash) Pass-the-Hash is a lateral movement technique in which attackers steal a user's NTLM hash from on...	0 open alerts	■■■ High	 Threat detection
 Suspected Golden Ticket usage (forged authorization data) Known vulnerabilities in older versions of Windows Server allow attackers to manipulate the Privileg...	0 open alerts	■■■ High	 Threat detection
 Data exfiltration over SMB Domain controllers hold the most sensitive organizational data. For most attackers one of their top ...	0 open alerts	■■■ High	 Threat detection
 Suspected Golden Ticket usage (ticket anomaly) Attackers with domain admin rights can compromise the KRBTGT account. Using the KRBTGT accou...	0 open alerts	■■■ High	 Threat detection
 Suspected DCSync attack (replication of directory services) Active Directory replication is the process by which changes that are made on one domain controll...	0 open alerts	■■■ High	 Threat detection

Azure – Conditional Access


- Critical for MFA implementation
- Useful for locking down access



The screenshot shows the Microsoft Azure portal interface for Conditional Access Policies. The top navigation bar includes the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the path: Home > Conditional Access. The main heading is "Conditional Access | Policies" with a subheading "Azure Active Directory". The left sidebar contains a navigation menu with options: Overview (Preview), Policies (selected), Insights and reporting, Diagnose and solve problems, Manage (with sub-items: Named locations, Custom controls (Preview), Terms of use, VPN connectivity, Authentication context (Preview), Classic policies), and Monitoring (with sub-items: Sign-in logs, Audit logs). The right pane displays a list of policies under the heading "Policy Name ↑↓". The policies listed are: MFA - DUO - All Cloud Apps - Admin Roles, MFA for all Global Admin, Block Legacy Apps, Risky User High Risk, MFA - DUO - All Cloud Apps - Staff/Faculty, Terms Of Use, Test-Restrict Access to Teams Only, Test-Restrict Access to All 365 Apps, and Test-Restrict Access to All 365 Apps - Except Email. At the top of the right pane, there are buttons for "New policy", "What If", "Refresh", and a search bar labeled "Search policies" with an "Add filters" button.

MFA - DUO - All Cloud Apps - Staff/Faculty ...

Conditional Access policy

 Delete

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

MFA - DUO - All Cloud Apps - Staff/Faculty

Assignments

Users or workload identities ⓘ

[Specific users included and specific users excluded](#)

Cloud apps or actions ⓘ

[All cloud apps](#)

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

[Sign-in frequency - 365 days](#)

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk ⓘ

[Not configured](#)

Sign-in risk ⓘ

[Not configured](#)

Device platforms ⓘ

[Not configured](#)

Locations ⓘ

[Any location and all trusted locations excluded](#)

Client apps ⓘ

[Not configured](#)

Filter for devices ⓘ

[Not configured](#)

Control user access based on their physical location. [Learn more](#)

Configure ⓘ

Yes

No

Include

Exclude

Select the locations to exempt from the policy

☒ All trusted locations

☐ Selected locations

Azure – PIM

- Don't walk around with master keys. Put them in a safe with permission to check them out.

Eligible assignments

Active assignments

Expired assignments

Search by role

Role	↑↓	Scope	↑↓	Membership	↑↓	State
Authentication Administrator		Directory		Group		Assigned
Global Reader		Directory		Group		Assigned
Conditional Access Administr...		Directory		Group		Assigned
Security Operator		Directory		Group		Assigned
Security Reader		Directory		Direct		Assigned
Security Reader		Directory		Group		Assigned
Security Administrator		Directory		Group		Assigned

My roles | Privileged access groups (Preview)

Privileged Identity Management | My roles

Refresh

Got feedback?

Activate

Azure AD roles

Privileged access groups (Preview)

Azure resources

Troubleshooting + Support

Troubleshoot

Eligible assignments

Active assignments

Expired assignments

Search by role or group

Role	↑↓	Group	↑↓	Group type	↑↓	Membership	↑↓	End time	Action
Member		PIM Security and Compliance		Security		Direct		Permanent	Activate
Member		PIM Service Desk		Security		Group		Permanent	Activate





BCNET
CONNECT

Moving Forward

Example: Compromise

Before M365

- Receive spam directly or reports from users
- Check header to confirm it was not spoofed
- Lock account and wait for user to call in
- Call mail team to get us numbers and purge the email.
- Slow reaction, no visibility

After M365

- Microsoft sends alert of suspicious access activity
- Team can investigate in near real-time what they are doing
- If the bad actor sends spam from the it can be seen right away and generates another alert
- Accounts can be quickly disabled and sessions revoked
- Added visibility is invaluable

Features to add

- Zero-Hour Auto Purge
 - Automatically delete mass spam from inboxes
- Expand ATP Safe links
 - Block suspicious links from anywhere
- Automated Alert Resolution
 - Block confirmed bad activity
- Data Loss Prevention/Governance
 - Cloud data protection
- Increase Secure Score
- Much More



Discussion

Questions?



BCNET
CONNECT

Thank you!