You Moved to Office 365 Now What?





Sean Metcalf Founder, Trimarc

ABOUT

- Founder Trimarc (Trimarc.io), a professional services company that helps organizations better secure their Microsoft platform, including the Microsoft Cloud.
- Microsoft Certified Master (MCM) Directory Services
- Microsoft MVP (2018)
- Speaker: Black Hat, Blue Hat, BSides, DEF CON, DerbyCon, Shakacon, Sp4rkCon, Troopers
- Security Consultant / Researcher
- AD Enthusiast Own & Operate <u>ADSecurity.org</u> (Microsoft platform security info) Sean Metcalf (@PyroTek3) TrimarcSecurity.com



AGENDA

- The "Cloud"
- Attacking the Cloud
- Auditing
- Administration
- Cloud Security Controls
- Controlling Access
- Password Insight
- Cloud Security "Tune Up"
- Office 365 Subscriptions & Capability
- Best Practices & Wrap-up
- BONUS: Testing Defenses

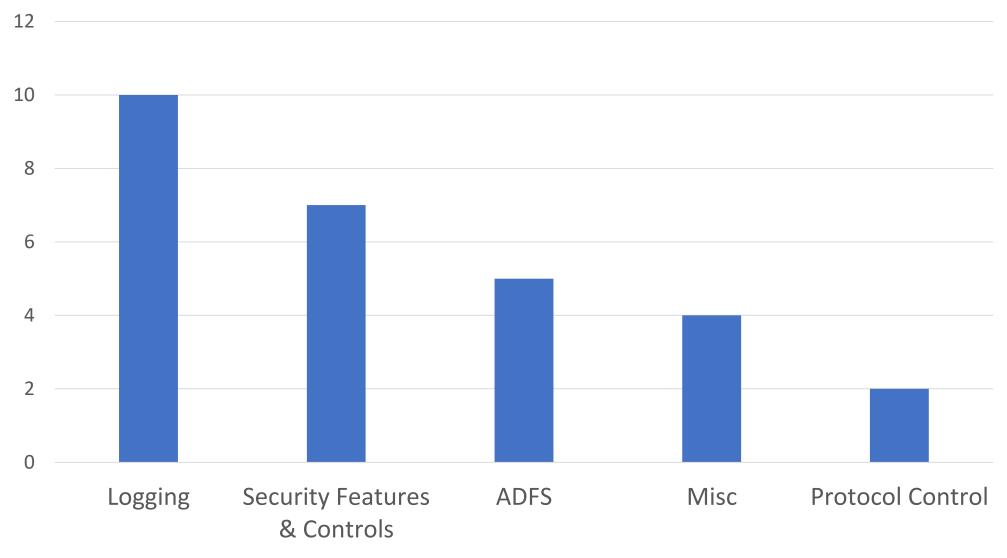


Sean Metcalf @PyroTek3 · Apr 11 I'm working on slides for my @BSidesCharm talk called "You moved to Office 365, Now What?" What would you like me to include?

Yeah I do cloud stuff too. It's like AD, just in Azure 😀



Responses by Category



```
[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
```

Moving to the Microsoft Cloud

- Sign up for Office 365 first one in gets Global Admin!
- Configure Azure AD Connect to synchronize users & groups
- Move Exchange mail to Exchange Online (keep 1 Exchange server on-prem for management)
- Update mail flow

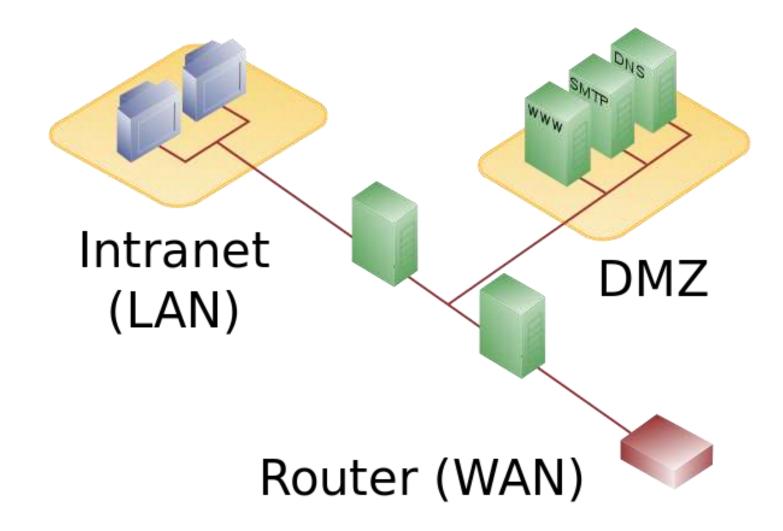
• . .

The Cloud Is Magic!

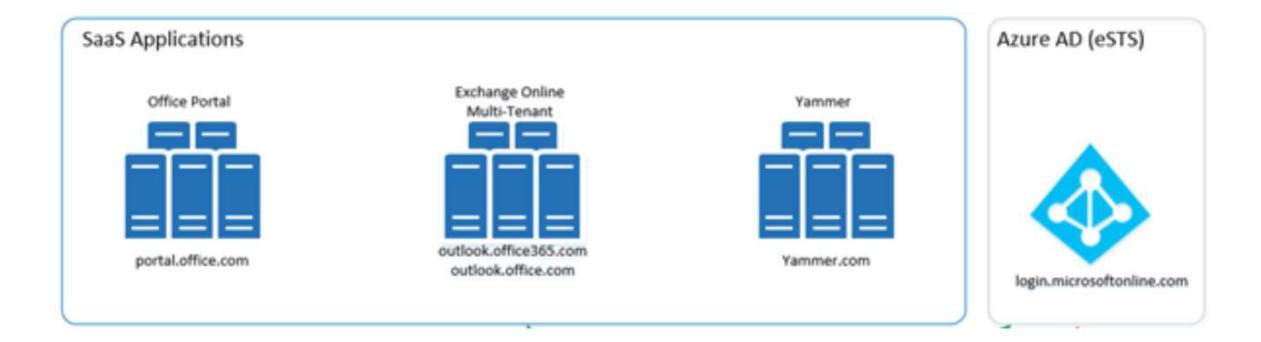


"The cloud is more secure since ______ spends millions every year on cloud security"

Internal Network



Anywhere Cloud Access





Azure Active Directory in the Marketplace

Every Office 365 and Microsoft Azure customer uses Azure Active Directory



Source: Microsoft Ignite Conference 2018

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com] https://myignite.techcommunity.microsoft.com/sessions/64565?source=sessions

Cloud Active Directory?

On-premises Active Directory

- Authentication, Directory, & Management
- AD Forest for single entity
- Internal corporate network
- Authentication
 - Kerberos
 - NTLM
- LDAP
- Group Policy

Azure AD (Office 365)

- Identity
- Designed for multi-tenant
- Cloud/web-focused
- Authentication
 - SAML 2.0
 - OpenID Connect
 - OAuth 2.0
 - WS-Federation
- REST API: AD Graph API

Attackers Love the Cloud

Common Passwords Attempted in Password Spray Attacks

Password Spring 2018 Summer September 1234

Winter

Football Your Company Name

The threats are real, global, and target all of us

1.29 Billion

Authentications blocked in August 2018



81% of data breaches involved weak, default, or stolen passwords

Source: Microsoft Ignite Conference 2018

Attacks on the Cloud

300% increase in identity attacks over the past year.



Source: Microsoft Ignite Conference 2018

https://myignite.techcommunity.microsoft.com/sessions/64523?source=sessions



Alert (TA18-086A)

More Alerts

Brute Force Attacks Conducted by Cyber Actors

Original release date: March 27, 2018 | Last revised: March 28, 2018



Systems Affected

Networked systems

Overview

According to information derived from FBI investigations, malicious cyber actors are increasingly using a style of brute force attack known as password spraying against organizations in the United States and abroad.

On February 2018, the Department of Justice in the Southern District of New York, indicted nine Iranian nationals, who were associated with the Mabna Institute, for computer intrusion offenses related to activity described in this report. The techniques and activity described herein, while characteristic of Mabna actors, are not limited solely to use by this group.

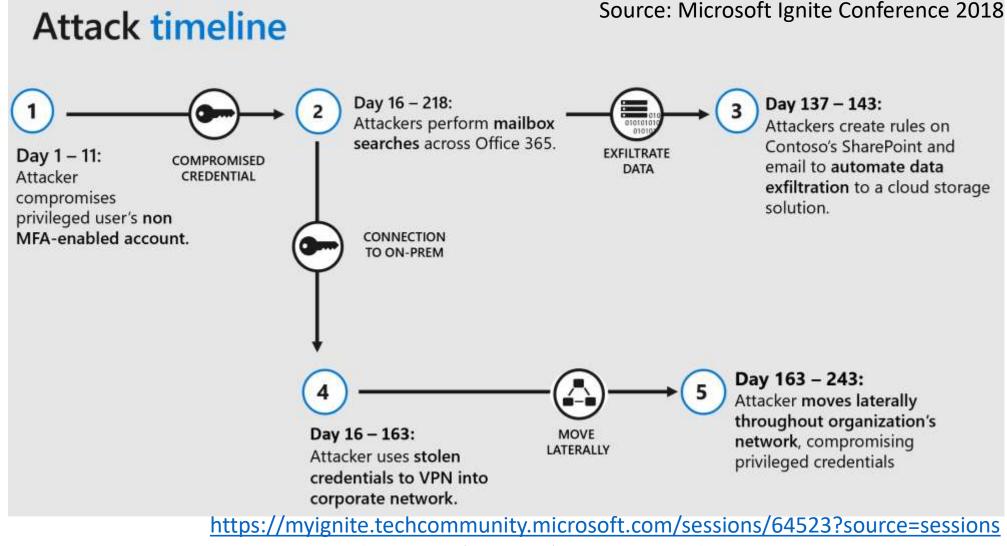
The Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) are releasing this Alert to provide further information on this activity.

Description

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

In a traditional brute-force attack, a malicious actor attempts to gain unauthorized access to a single account by guessing the password. This can quickly result in a targeted account getting locked-out, as commonly used account-lockout policies allow three to five bad attempts during a set period of time. During a password-spray attack (also known as the "low-and-slow" method), the malicious actor attempts a single password against many accounts before moving on to attempt a

Cloud Attack Timeline



MailSniper

https://github.com/dafthack/MailSniper

MailSniper is a penetration testing tool for searching through email in a Microsoft Exchange environment for specific terms (passwords, insider intel, network architecture information, etc.). It can be used as a non-administrative user to search their own email, or by an Exchange administrator to search the mailboxes of every user in a domain.

MailSniper also includes additional modules for password spraying, enumerating users/domains, gathering the Global Address List from OWA and EWS, and checking mailbox permissions for every Exchange user at an organization.

For more information about the primary MailSniper functionality check out this blog post.

For more information about additional MailSniper modules check out these blog posts:

- GAL & Password Spraying
- Invoke-OpenInboxFinder

Download the MailSniper Field Manual to quickly reference various MailSniper functions.

Password Spraying the OWA portal at https://outlook.office365.com/owa/. Sit tight... 5 threads remaining

[*] Now spraying the OWA portal at https://outlook.office365.com/owa/
[*] Current date and time: 11/04/2018 09:59:26

EWS Capability

- Availability
- Bulk Transfer
- Delegate Management
- Exchange Store Search
- Exchange Search
 Federated Sharing Folder
- Inbox Rules Item

- Mail Tips Messaging
- Records Management
- Message Tracking Notification
- Service Configuration
 Synchronization
- Unified Messaging User Configuration Utility

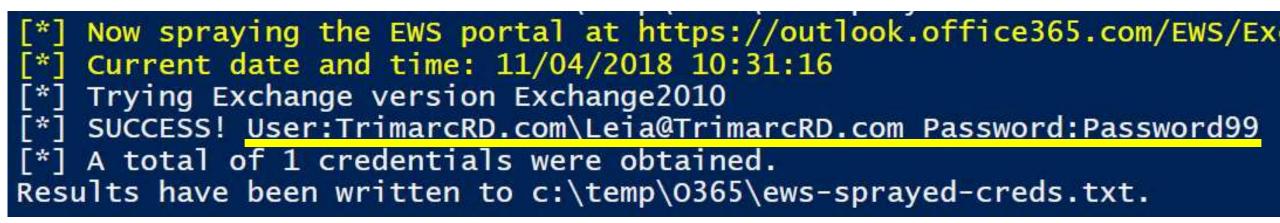
Password Spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx. Sit tight... 5 threads remaining

>> -userlist 'C:\Temp\0365\UserList.txt' -OutFile 'c:\temp\0365\ews-sprayed-creds.txt' -password 'Password99!' [*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx [*] Current date and time: 11/04/2018 09:56:01 [*] Trying Exchange version Exchange2010

Password Spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx. Sit tight....

5 threads remaining.

A total of 1 credentials were obtained. Results have been written to c:\temp\0365\ews-sprayed-creds.txt. Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx Current date and time: 11/04/2018 10:30:20 Trying Exchange version Exchange2010 SUCCESS! User:TrimarcRD.com\DarthVader@TrimarcRD.com Password:Summer2018! A total of 1 credentials were obtained. Results have been written to c:\temp\0365\ews-sprayed-creds.txt. Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx Current date and time: 11/04/2018 10:30:34 Trying Exchange version Exchange2010 SUCCESS! User:TrimarcRD.com\HanSolo@TrimarcRD.com Password:Password99! A total of 1 credentials were obtained. Results have been written to c:\temp\0365\ews-sprayed-creds.txt. Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx Current date and time: 11/04/2018 10:30:48 Trying Exchange version Exchange2010 [*] SUCCESS! User:TrimarcRD.com\JangoFett@TrimarcRD.com Password:Password#99 A total of 1 credentials were obtained. Results have been written to c:\temp\0365\ews-sprayed-creds.txt. Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx Current date and time: 11/04/2018 10:31:01 [*] Trying Exchange version Exchange2010



11/4/2018, 10:31:29 AM	Leia	Office 365 Exchange Online	Success
11/4/2018, 10:31:29 AM	Yoda	Office 365 Exchange Online	Failure
11/4/2018, 10:31:29 AM	ObiWan Kenobi	Office 365 Exchange Online	Failure
11/4/2018, 10:31:23 AM	Han Solo	Office 365 Exchange Online	Failure
11/4/2018, 10:31:23 AM	Bailey	Office 365 Exchange Online	Failure
11/4/2018, 10:31:23 AM	Boba Fett	Office 365 Exchange Online	Failure
11/4/2018, 10:31:23 AM	Jango Fett	Office 365 Exchange Online	Failure
11/4/2018, 10:31:23 AM	Darth Vader	Office 365 Exchange Online	Failure
11/4/2018, 10:31:11 AM	ObiWan Kenobi	Office 365 Exchange Online	Failure
11/4/2018, 10:31:11 AM	Yoda	Office 365 Exchange Online	Failure
11/4/2018, 10:31:11 AM	Leia	Office 365 Exchange Online	Failure

Basic info	Device info	MFA info	Conditional Access	
------------	-------------	----------	---------------------------	--

Request Id b6c4fd5c-a7b0-4d75-ba65-5ba429789700	IP address	137.1
---	------------	-------

Correlation Id c8dec77b-2c4c-4071-8a7c-4bed95359c01

User Leia

Username leia@trimarcrd.com

User ID 2a8165e3-296c-4168-aa52-968bce5f1ef0

Application Office 365 Exchange Online

Application ID 0000002-0000-0ff1-ce00-0000000000

IP address	137.135.
Location	Washington, Virginia, US
Date	11/4/2018, 10:31:29 AM
Status	Success
Client App	Other clients: Older Office clients

Basic info Device info MFA info Conditional Access Troubleshooting and support

Request Id	b6c4fd5c-a7b0-4d75-ba65-5ba475769700	IP address	137.135.
Correlation Id	8603d100-6135-45d1-956b-e8f360d99e6f	Location	Washington, Virginia, US
User	Leia	Date	11/4/2018, 10:31:11 AM
Username	leia@trimarcrd.com	Status	Failure
User ID	2a8165e3-296c-4168-aa52-968bce5f1ef0	Sign-in error code	50126
Application	Office 365 Exchange Online	Failure reason	Invalid username or password or Invalid on-premise username or password.
Application ID 0000002-0000-0ff1-ce00-00000000000			password.
Application is		Client App	

ISP: Microsoft Corporation

IP Geolocation Information

Continent: North America (NA) Country: United States (US) = City: Washington

Cloud Auditing



[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

Microsoft Cloud Auditing

Audit Item	Category	Enabled by Default	Retention
User Activity	Office 365 Security & Compliance Center	No	90 days
Admin Activity	Office 365 Security & Compliance Center	No	90 days
Mailbox Auditing	Exchange Online	No*	90 days
Sign-in Activity	Azure AD	Yes	30 days (AAD P1)
Users at Risk	Azure AD	Yes	7 days 30 days (AAD P1) 90 days (AAD P2)
Risky Sign-ins	Azure AD	Yes	7 days 30 days (AAD P1) 90 days (AAD P2)
Azure MFA Usage	Azure AD	Yes	30 days
Directory Audit	Azure AD	Yes	7 days 30 days (Azure AD P1/P2)

* Microsoft is gradually enabling mailbox auditing for tenants.

Enable User & Admin Activity Auditing

Home > Audit log search

Audit log search

To use this feature, turn on auditing so we can start recording user and admin activity in your organization. When you turn this on, activity will be recorded to the Office 365 audit log and available to view in a report.

Turn on auditing

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Search		9 Clear		Results					
Activities				Date 🔻	IP address	User	Activity	Item	Detail
Show results fo	or all activ	ities 👻							
Start date					Ru	n a seai	rch to view	results	
2018-10-20		00:00	~						
End date									
2018-10-28		00:00	~	[Sean Metcalf @	PyroTek3 TrimarcS	ecurity.com]			

Enable User & Admin Activity Auditing

Home > Audit log search

Audit log search

! We're preparing the Office 365 audit log. You'll be able to search for user and admin activity in a couple of hours.

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Search Clear	Results					
Activities	Date 💌	IP address	User	Activity	Item	Detail
Show results for all activities 👻						
Start date		Ru	n a sea	rch to viev	v results	
2018-10-20 🗰 00:00 ~						
End date						
2018-10-28 🗰 00:00 ~	[Soon Motcolf]	@PyroTek3 Trimar	eSecurity com 1			

Get Mailbox Auditing

PS C:\> Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} `
 | FL Name,Audit*

Name	eanMetcalf	
AuditEnabled	alse	
AuditLogAgeLimit	0.00:00:00	
AuditAdmin	Update, MoveToDeletedItems, SoftDelete, HardDel	ete}
AuditDelegate	Update, MoveToDeletedItems, SoftDelete, HardDel	ete}
AuditOwner	Update, MoveToDeletedItems, SoftDelete, HardDel	ete}
Name	ailev	
AuditEnabled	alse	
AUGITLOGAGELIMIT	<mark>0.00:</mark> 00:00	
AuditAdmin	Update, MoveToDeletedItems, SoftDelete, HardDel	
AuditDelegate	Update, MoveToDeletedItems, SoftDelete, HardDel	ete}
AuditOwner	Update, MoveToDeletedItems, SoftDelete, HardDel	ete}

Enable Mailbox Auditing

PS C:\> Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} | Set-Mailbox -AuditEnabled \$true -AuditOwner MailboxLogin,HardDelete,SoftDelete

PS C:\> Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} |` FL Name,Audit*

Name	:	SeanMetcalf
AuditEnabled	8	True
AuditLogAgeLimit	:	90.00:00:00
AuditAdmin	2	{Update, MoveToDeletedItems, SoftDelete, HardDelete}
AuditDelegate	:	{Update, MoveToDeletedItems, SoftDelete, HardDelete}
AuditOwner	-	{SoftDelete, HardDelete, MailboxLogin}
Name		bailey
Name AuditEnabled		bailey True
	:	True
AuditEnabled	:	True
AuditEnabled AuditLogAgeLimit	:	True 90.00:00:00
AuditEnabled AuditLogAgeLimit AuditAdmin	::	True 90.00:00:00 {Update, MoveToDeletedItems, SoftDelete, HardDelete}



Getting Office 365 Logs in Your SIEM

https://docs.microsoft.com/en-us/office365/securitycompliance/siem-server-integration

SIEM server integration Microsoft 365

A SIEM server can receive data from a wide variety of Microsoft 365 services and applications. The following table lists several Microsoft 365 services and applications along with SIEM server inputs and where to go to learn more about SIEM server integration.

Microsoft 365 Service or Application	SIEM server inputs	Resources to learn more
Office 365 Advanced Threat	Audit logs	SIEM integration with Office 365
Protection		Advanced Threat Protection
or		
Office 365 Threat Intelligence		
Microsoft Cloud App Security	Log	SIEM integration with Microsoft Cloud
	integration	App Security
Office 365 Cloud App Security	Log	Integrate your SIEM server with Office
	integration	365 Cloud App Security
Windows Defender Advanced	Log	Pull alerts to your SIEM tools
Threat Protection	integration	
Azure Security Center (Threat	Alerts	Azure Security data export to SIEM -
Protection and Threat Detection)		Pipeline Configuration - Preview
Azure Active Directory Identity	Audit logs	Integrate Azure Active Directory audit
Protection	0-400000000000000000000000000000000000	logs
Azure Advanced Threat Analytics	Log	ATA SIEM log reference
	integration	

Getting Office 365 Logs in Your SIEM

SIEM server integration Microsoft 365

A SIEM server can receive data from a wide variety of Microsoft 365 services and applications. The following table lists several Microsoft 365 services and applications along with SIEM server inputs and where to go to learn more about SIEM server integration.

(i) Important

- You must be an Office 365 global administrator or have the security administrator role assigned for the Security & Compliance Center to set up SIEM integration with Office 365 Advanced Threat Protection.
- Audit logging must be turned on for your Office 365 environment. To get help with this, see <u>Turn Office 365 audit log search on or off</u>.

	Protection and Threat Detection)		Pipeline Configuration - Preview
<u>https://docs.microsoft.com/en-</u> us/office365/securitycompliance/siem-server-integration	Azure Active Directory Identity Protection	Audit logs	Integrate Azure Active Directory audit logs
[Sean Metcalf @Py	Azure Advanced Threat Analytics	Log integration	ATA SIEM log reference

Azure Sentinel (Preview)

- Cloud native SIEM
- Aggregates data from various sources (on-prem & multiple clouds)
- Microsoft analytics to help detect threats
- Built-in orchestration with connectors to other systems.

Azure Sentinel

A cloud-native SIEM to help you focus on what matters most

Collect and analyze data from any source, cloud or on-premises, in any format, at cloud scale. With Al on your side, find, investigate, and respond to real threats in minutes, with built-in knowledge and intelligence from decades of Microsoft security experience.



3. Automate & orchestrate

Create

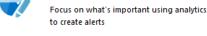
Use or customize built-in playbooks to auton



1. Collect data

Connect

Collect data at cloud scale across the enterprise both on-premises and in multiple clouds





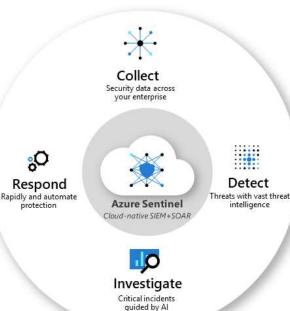
Create

2. Create security alerts

common tasks

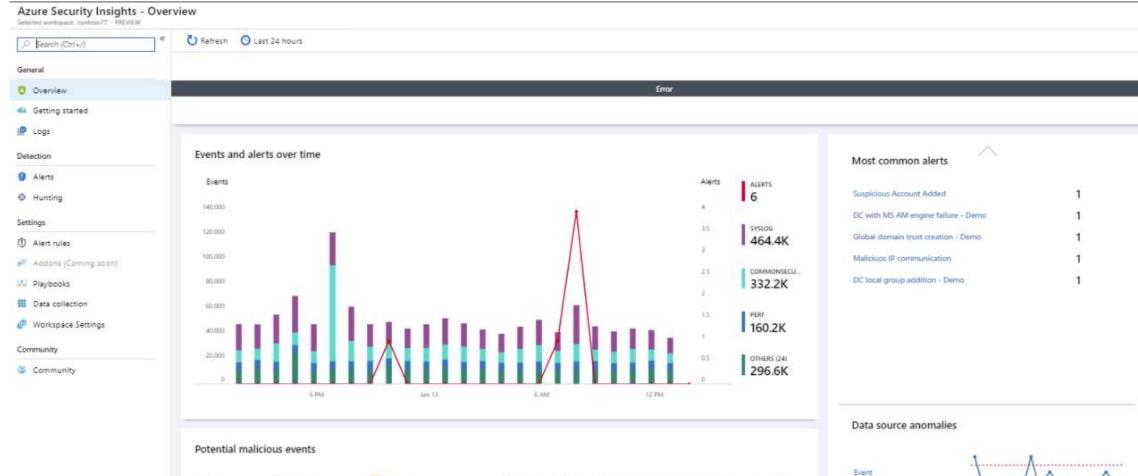


 \mathbf{n}



Azure Sentinel - Data connectors Selected workspace 'CyberSecurityDemo' - PREVIEW

	Azure Active	Azure AD Identity	Office 365	Microsoft Cloud	Azure Advanced	SE Security Event
eneral	Directory	Protection		App Security	Threat Protection	SE Security Event
Overview	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT
Logs						
reat management	CONFIGURE	CONFIGURE	CONFIGURE	CONFIGURE	CONFIGURE	CONFIGURE
Cases						
Dashboards					-	-
Hunting	Azure Security Center	Azure Activity	Azure Information Protection	WAF	WF Windows Firewall	AWS AWS
Notebooks	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	MICROSOFT	AMAZON
onfiguration						
Getting started	CONFIGURE	CONFIGURE	CONFIGURE	CONFIGURE	CONFIGURE	CONFIGURE
Data connectors						
Analytics						
1 Playbooks	CEF Common Event Format	palo Alto Networks	cisco ASA	Check Point	Former Fortinet	(5) F 5
Community	ANY PUBLISHER	PALO ALTO NETWORKS	cisco	CHECK POINT	FORTINET	F5
Workspace settings						
	CONFIGURE	CONFIGURE	CONFIGURE	CONFIGURE	CONFIGURE	CONFIGURE
	Barracuda	S Syslog	DNS	Threat Intelligence	Symantec ICDX	
	MICROSOFT	MICROSOFT	MICROSOFT	ANY PUBLISHER	SYMANTEC	
	CONFIGURE	CONFIGURE	CONFIGURE	CONFIGURE	CONFIGURE	







Azure Security Insights community



Visit the Azure Security Insights community GitHub repo to explore sample content for alert rules. Add-ons, playbooks and more

Open Azure Security Insights community >

Azure Sentinel Detection via GitHub

Azure / Azure-Sentinel	• Watch	62	★ Star	140	₿ Fo	rk 32	
<> Code () Issues (4) (1)	Pull requests 4 III Projects 0 III Insights						
Branch: master - Azure-Sentin	el / Detections /		C	reate new fi	e Fin	d file	History
shainw and timbMSFT OfficeAct	ivity detections and hunting from ashwin (#141)		L	atest comn	nit 07c14	a5 11 d	ays ago
AWSCloudTrail	change technique to tactic					a mor	nth ago
AzureActivity	change technique to tactic					a mor	nth ago
CommonSecurityLog	change technique to tactic					a mor	nth ago
DnsEvents	change technique to tactic					a mor	nth ago
MultipleDataSources	Adding in Ajeet's for March					25 da	ays ago
OfficeActivity	OfficeActivity detections and hunting from ashwin (#141)					11 da	ays ago
SecurityEvent	Updateing list of WellKnownGroupSID to include DNSAdmins and D	nsUpdat (23 da	ays ago
SigninLogs	Azure portal brute foce (#136)					24 da	ays ago
Syslog	change technique to tactic					a mor	nth ago
VMConnection	Adding a couple of interesting queries I threw together while doing	r (11 da	ays ago
W3CIISLog	pushing initial version of PrivAccountTracking and some minor fixes					28 da	ays ago
readme.md	Updating Detections Readme					2 mon	ths ago

Search (Ctri+/)	🕂 New Query 😭 Bookmark Logs 💍 Refres	sh 🕒 Last 24 hours											
neral		=											
Overview		94 🛛 🗖 4		R 0									
Logs	Total Queries Total	I Results Total Bo	okmarks	My Book	marks								
at management	Queries Bookmarks												
Alerts													
Dashboards	,C Search queries		AII DATA SOURC	S: All CTACTICS:	: All)				Uncom	mon process	es/files - botto	m 5%	
User profiles (Coming soon)	QUERY	DESCRIPTION	PROVIDER	DATA SOURCE	ES .	TACTICS			Microsoft	31	2	E SecurityEven	
Hunting	/#32005					0 1 c)	-	- 10 as 2 a	Provider	Result		Data Source	
Notebooks	Uncommon processes/files - bottom 5%	Shows the rarest processes seen running for th		SecurityEvent 12		1977	222	· E & & &	Description				
figuration	Script usage summary (cscript.exe)	Daily summary of vbs scripts run across the en	1109911210128200930	SecurityEvent 2				1 K - G -	Shows the		unning for the first time. Th		
Getting started	Summary of users created using uncommon	. Summarizes users of uncommon & undocument	nted Microsoft	SecurityEvent 0	6			1 2 m 6 6	*** stable envir	stable environments, these new processes could provide an indication of a			
Data collection	Office365 authentications	Shows authentication volume by user agent an	nd IP Microsoft	OfficeActivity 0	E.			1月10日	*** context of t		hich these binaries ran can		
Security analytics	New processes observed in last 24 hours	Shows new processes observed in the last 24 h	ours Microsoft	SecurityEvent B	0	0.0		1萬四日本		ne for identifying poss-	Die allacity.		
Playbooks	Summary of failed user logons by reason of f	. A summary of failed logons can be used to infi	er lat Microsoft	SecurityEvent 0	Č.	Q 🕻 🗘	•		··· Query Infor	rmation			
Community	* Anomalous Azure AD apps based on authent.	This query over Azure AD sign-in activity highl	lights Microsoft	SigninLogs -	5	Q 1 🗢					("2019-02-19T18:	and the second se	
Workspace Settings	* Processes executed from base-encoded PE fil.	Finding base64 encoded PE files header seen in	n the Microsoft	SecurityEvent	2	🛡 💈 🗠	1	8年4月6日		let processEvents=SecurityEvent where TimeGenerated > start and TimeGene where EventID==4688			
	+ Processes executed from binaries hidden in	Process executed from binary hidden in Base6	4 enc Microsoft	SecurityEvent	2	Q 1 🔿	1	12-16-6					
	★ Summary of users creating new user accounts	New user accounts may be an attacker providi	ng th Microsoft	OfficeActivity	22	0 t c	1						
	* User and Group enumeration	The query finds attempts to list users or group	is usi Microsoft	SecurityEvent		0 ° C	1		View query	result >			
	* Hosts with new logons	Shows new accounts that have logged onto a l	host f Microsoft	SecurityEvent	4			1					
	* Malware in the recycle bin	Finding attackers hiding malware in the recycle		SecurityEvent		010	-		Timestamp	Since			
	★ Masguerading files	Maiware writers often use windows system pro		SecurityEvent			_		Tactics				
	134 - OMM2801017484730	. Summary of users/user agents associated with		OfficeActivity					Execution		tion tactic represents tech of adversary-controlled co		
				0.403030643						system. read more			
	Azure AD signins from new locations	New AzureAD signin locations today versus his		SigninLogs		The second		12002		use to gai	access tactic represents th n an initial foothold within		
	★ Powershell downloads	Finds PowerShell execution events that could i		SecurityEvent	*	Q : c)		NK OG G	Persistence		e is any access, action, or o		
	* Sharepoint downloads	Shows volume of documents uploaded to or d	owni Microsoft	OfficeActivity	9			120.00		a system t that system	that gives an adversary a p m.	rsistent presence on	
	★ Summary of user logons by logon type	Comparing succesful and nonsuccessful logon	atte Microsoft	SecurityEvent		0		· · · · ·		read more. coe Escalation Privilege escalation is the result of actions that allo			

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

Run Query

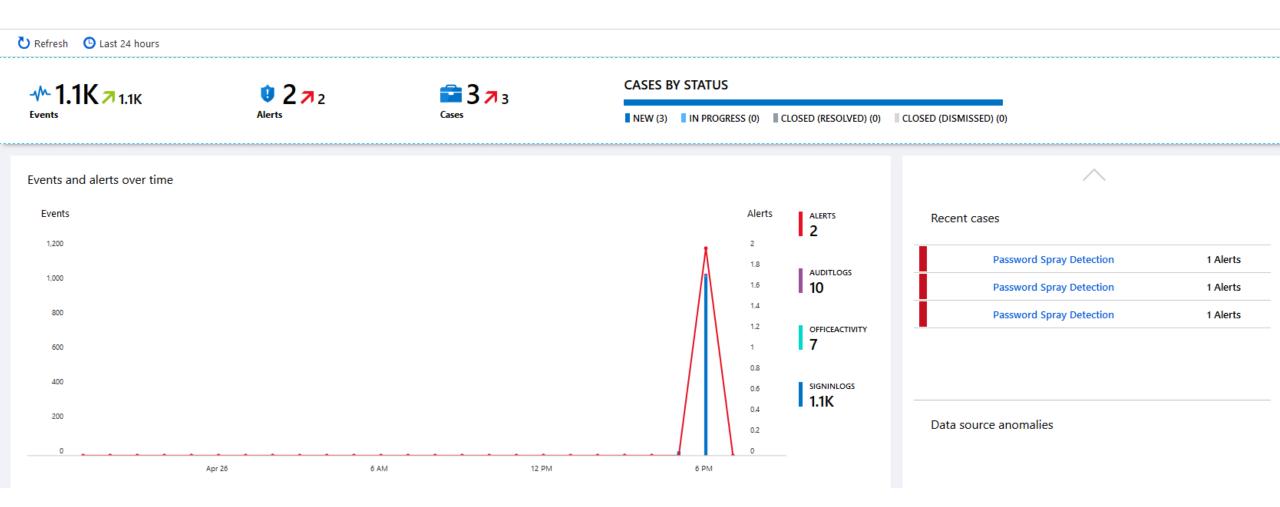
Azure Sentinel Hunting via GitHub

Azure / Azure-Sentinel		• Watch	62	★ Star	140	¥ Fork	32
<>Code (!) Issues (4) (*	Pull requests 4 III Projects 0 III Insights						
Branch: master - Azure-Sentir	nel / Hunting Queries /		C	reate new file	e Fin	d file His	story
juliango2100 Merge pull request	#138 from Azure/deploy_hunting_queries			Latest comr	nit 897t	oc22 9 days	ago
AWSCloudTrail	Changed technique to tactic in hunting queries					a month	ago
AzureActivity	Changed technique to tactic in hunting queries					a month	ago
DnsEvents	Events Adding in Ajeet's for March				25 days ago		
Hunting_Scripts	Update ssh_brute_force.md					29 days	ago
MultipleDataSources	Tracking priv account update (#144)					19 days	ago
OfficeActivity	OfficeActivity detections and hunting from ashwin (#141)					11 days	ago
SecurityEvent	Merge pull request #138 from Azure/deploy_hunting_queries					9 days	ago
SigninLogs	Revert changes					19 days	ago
Syslog	Changed technique to tactic in hunting queries					a month	ago
W3CIISLog	I think I got them to remove this time					26 days	ago
DeployedQueries.json	Fix detections report					12 days	ago
DeployedQueries.txt	Deploy hunting queries					23 days	ago
QUERY_TEMPLATE.md	pushing initial version of PrivAccountTracking and some minor fix	es				28 days	ago
deploy.ps1	Fix detections report					12 days	ago
readme.md	Deploy hunting queries [Sean Metcalf @PyroTek3 TrimarcSecurity.c	com]				23 days	ago

Azure Sentinel Password Spray

[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx [*] Current date and time: 04/26/2019 18:41:34 [*] Trying Exchange version Exchange2010 [*] SUCCESS! User:TrimarcRD.com\ObiWanKenobi@trimarcrd.com Password:WinterisComing19! [*] A total of 1 credentials were obtained. Results have been written to C:\Temp\CloudAttackScripts\owa-sprayed-creds.txt. [*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx [*] Current date and time: 04/26/2019 18:41:54 [*] Trying Exchange version Exchange2010 [*] SUCCESS! User:TrimarcRD.com\BobaFett@trimarcrd.com Password:Mandalorian19! [*] SUCCESS! User:TrimarcRD.com\JangoFett@trimarcrd.com Password:Mandalorian19! [*] A total of 2 credentials were obtained. Results have been written to C:\Temp\CloudAttackScripts\owa-sprayed-creds.txt. [*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx [*] Current date and time: 04/26/2019 18:42:16 [*] Trying Exchange version Exchange2010 [*] SUCCESS! User:TrimarcRD.com\DarthVader@trimarcrd.com Password:TheForce19 [*] A total of 1 credentials were obtained. Results have been written to C:\Temp\CloudAttackScripts\owa-sprayed-creds.txt. [*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx [*] Current date and time: 04/26/2019 18:42:36 [*] Trying Exchange version Exchange2010 [*] SUCCESS! User:TrimarcRD.com\HanSolo@trimarcrd.com Password:LeiaIKnow19! A total of 1 credentials were obtained.

Azure Sentinel Password Spray Detection



Azure Sentinel Password Spray Detection

Case Case ID f9133657-a852-4873-ab85-85f36eec1d27 - PRI	EVIEW							
💼 Password Spray De	tection	Alerts Entities						
High SEVERITY STATUS	✓ Superstand ✓ OWNER	<i>P</i> Search	×	: Informational, Low, Medium, High, C	ritical			
DESCRIPTION		₩ ALERT NAME	↑↓ ALERT ID	PRODUCT NAME	↑↓ CREATION TIME ↑↓	TIME FRAME	↑↓ NUMBER OF ENTITIES ↑↓	HITS
LAST UPDATE TIME		Password Spray Detection	69c577dc-dc2f-4475-83c1-3695	2 Azure Sentinel	04/26/19, 6:52 PM	4/26/2019 - 4/26/2019	11	330
04/26/19, 6:52 PM								
CREATION TIME 04/26/19, 6:52 PM								
EVIDENCE	▶ Run T	ime range: Custom	\supset					
9 1								
Alerts	SigninLogs							
ENTITIES 10 20 1 Account Host IP	where ClientAp extend Account	pe != 0 scription == "Inv pUsed == "Other c CustomEntity = Us mEntity = IPAddre	lients; Older O erPrincipalName		walid on-pr	emise username	e or password	1."
	Excend IPCusco	increase = iPAddre	22					

Azure Sentinel Password Spray Detection

TimeGenerated [UTC 🗸	Source ∇	OperationName 🖓	Identity 🛛 🖓	ResultDescription	7 ClientAppUsed	Location ∇	IPAdd 🏹	AppDisplayName
2019-04-26T22:45:33.674	Azure AD	Sign-in activity	Han Solo	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:43:29.129	Azure AD	Sign-in activity	Lando Calrission	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:43:08.325	Azure AD	Sign-in activity	Lando Calrission	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:41:17.777	Azure AD	Sign-in activity	Bailey	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:41:03.764	Azure AD	Sign-in activity	Lando Calrission	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:40:55.091	Azure AD	Sign-in activity	Bailey	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:40:41.185	Azure AD	Sign-in activity	Han Solo	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:40:17.015	Azure AD	Sign-in activity	Han Solo	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:39:32.634	Azure AD	Sign-in activity	ObiWan Kenobi	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:39:29.039	Azure AD	Sign-in activity	Lando Calrission	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:39:29.039	Azure AD	Sign-in activity	Lando Calrission	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:39:27.047	Azure AD	Sign-in activity	Han Solo	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:39:27.047	Azure AD	Sign-in activity	Han Solo	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:39:20.268	Azure AD	Sign-in activity	Bailey	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:39:20.268	Azure AD	Sign-in activity	Bailey	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:36:03.266	Azure AD	Sign-in activity	Han Solo	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:36:03.266	Azure AD	Sign-in activity	Han Solo	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:35:45.788	Azure AD	Sign-in activity	ObiWan Kenobi	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365
2019-04-26T22:35:45.788	Azure AD	Sign-in activity	ObiWan Kenobi	Invalid username or password or Invalid on-premise username or pass	Other clients; Older Office clients	US	69.13	Office 365

Azure Sentinel Pricing

Pricing details

There will be no charges specific to Azure Sentinel during the preview. Pricing for Azure Sentinel will be announced in the future and a notice will be provided prior to the end of the preview. Should you choose to continue using Azure Sentinel after the notice period, you will be billed at the applicable rates.

Data import from Office 365 is free. You need to be a licensed customer of Office 365 for this data import. Even during preview additional charges may be incurred related to data ingestion, automation workflows or customization of machine learning models. <u>https://azure.microsoft.com/en-us/pricing/details/azure-sentinel/</u>

Log Analytics

Log Analytics is billed per gigabyte (GB) of data ingested into the service.

FEATURE	FREE UNITS INCLUDED	PRICE
Data Ingestion	5 GB per customer per month ¹	\$2.30 per GB
Data Retention	31 days²	\$0.10 per GB per month

¹The first 5 GB of data ingested per customer to the Azure Log Analytics service every month is offered free.

²Every GB of data ingested into your Azure Log Analytics workspace is retained at no charge for the first 31 days.

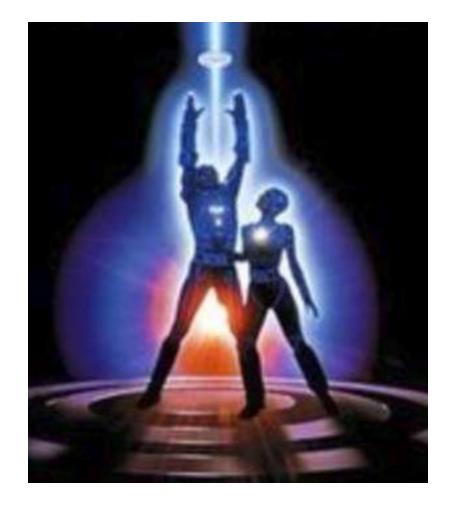
Please note: Service Map solution is billed for data ingested by the Dependency Agent into the Service Map platform and the Log Analytics service. Data ingested by the Dependency Agent is billed per Log analytics prices listed above. Billing for data ingested into the Service Map platform is not enabled yet and will be billed starting August 1, 2019.

(Google) Chronicle Backstory

- Runs on Google infrastructure.
- No charges based on data volume.
- Designed for multipetabyte analytics.

10.50.27.25	Orenicte Refler X +			
4 + C	· https://demoders.backstory.chru	scie.security/www.fiew.its?assetIdentifier+10.50.23	25BrahmanceTime=2018-02-05104%3A00%5A00.0002BrawLogsTaken=1	laenstad, ist-AssetVewTerstinsEpressionoeFilter-356ata. 🔅 😔 🔘
(i) 3819-	RINE FARE DITO 45-45784-08-08-0842 2-0704-0600002	Q 18.56.22.35	0	
194 Events Prevalence: 30	s of 620 Total	Contraction Institute account		s Sen, Jess Secol www.efficiencestation.com enformer 1
Q Seething		201		()**
2 2065	10000			
> ========	retained by the standard ave			
> +0.07.10	a chainman agus an 20 an thairt ann			
> ======	attantelevisystext/igesplete.com	2		
> =======	er (wholes/system30)gesidets.eve			
3 0100120	er (arielikas) (system)2'(seches), ere	12	11.00 12.15 12.30 20.41	04/05 04/15 04/30
3 81/09/28	(em) er(ansbar).system(2).sector(2619-62-65 62/48/88 (27		2019-02-05 04/46(00 (172)
> =====	a (and and a systemic) unclust and	1 FORWARDED ALERTS	1 DOMAINS NEW TO THE 2 LOW PREVALE DOMAINS	ACE 2 US DHS AIS
> =====	a r ha makasi / isan kan ka sa ma	www.office-revisi	on.com @ 03:56:00	
> #1.55-38	ageterfer. It te	And a Charles of the Annual States of the Annual St	Charge of Langeline and Millionskilling Department with the	mand for the 2018 Languagest for the 2018 Linking for the 2018
> #8135125	grant and	E en.effice.	existences formations a service age / 12 structure age (south second for interaction age (formations) a service age / 12 structure age (south second for)	c atria damain (3
5-1111-10	and office overlappenent	a Childheathar		
> min.m	(Provent Sectority) #2 SectorInguistics	E T		
> +1.54.45	(registry)methine's an finance's anni 412	makinten.		
>	www.offlige-certatum.com	0417 G120 G1	28 พลัสร พลัสร หลังร หลังร กลังร กลังร กลังร	Dec 31 Jan 08 Jan 18 Jan 24 Feb 01 Feb 28 Feb 28
	Arternee that			
******	AUNT Pale Alto Motsoria Alert	VIRUSTOTAL INSIGHTS	US DHS AIS	
>	and office restators and	Annual An	- Astadra-Disarvettan - Astralya-Disarvettan - APT-Actfaity	•

https://chronicle.security/products/backstory/



Protecting Cloud Administration

According to Microsoft, Only <u>%</u> of ALL (Office 365/Azure AD) Admin Accounts require MFA.

As of September 2018

According to Microsoft, Only **1.8%** of ALL (Office 365/Azure AD) Admin Accounts require MFA.

As of September 2018

Cloud Administration Protection

- Only cloud admin accounts are in privileged groups.
- Require all cloud admin accounts to use MFA (Microsoft Authenticator only).

```
$UserCredential = Get-Credential
Import-Module MSOnline
Connect-MsolService -Credential $UserCredential
```

```
$auth = New-Object -TypeName Microsoft.Online.Administration.StrongAuthenticationRequirement
$auth.RelyingParty = "*"
```

```
$auth.State = "Enabled"
```

```
$auth.RememberDevicesNotIssuedBefore = (Get-Date)
```

```
# Enable MFA on all Users
Get-MsolUser -All | where {$_.userprincipalname -like "*admin*"} | `
Foreach {Set-MsolUser -UserPrincipalName $_.UserPrincipalName -StrongAuthenticationRequirements $auth }
```

Cloud Administration Protection via Baseline Policy



While managing custom conditional access policies requires an Azure AD Premium license, baseline policies are available in all editions of Azure AD. Baseline policy: Require M... \Box \times

Name

Baseline policy: Require MFA for admins (Pre ...

This policy requires **multi-factor authentication (MFA)** for the following directory roles:

- Global Administrator
- SharePoint Administrator
- Exchange Administrator
- Conditional Access Administrator
- Security Administrator
- Helpdesk Administrator/Password
 Administrator
- Billing Administrator
- User Account Administrator

This policy also blocks legacy authentication.

Learn more

Enable policy

Use policy immediately
 Do not use policy

Users **1** Select the users to exempt from ...

"Break Glass" Cloud Admin Account

- New account designated as the Microsoft Cloud Admin account.
- Has permanent membership in the most privileged groups.
- Is excluded from most security controls: MFA and Conditional Access policies.
- Has a strong password (16 characters, for now).
- Only used in emergencies.
- All other cloud admin accounts have strong security controls (MFA, etc.)

Security administrator - Try out PIM



Try out PIM

- Members
- Description

Troubleshooting + Support

- 🗙 Troubleshoot
- New support request



«

Azure AD Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more. Learn more



Limit standing access

PIM allows you to make users eligible for roles, which means they only have access when necessary.



Discover who has access

Using the built-in wizard, you can easily discover users with permanent privileged role assignments and make them eligible.



Review privileged access

With Access Reviews, you can choose delegates or have users attest for themselves if they still need access to privileged roles.

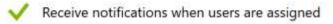


Do more with Azure AD Privileged Identity Management



- Log service/ticket numbers when activating
- Schedule activations for a specific date

/ Require approval workflow to activate



Configure and resolve alerts for privileged roles

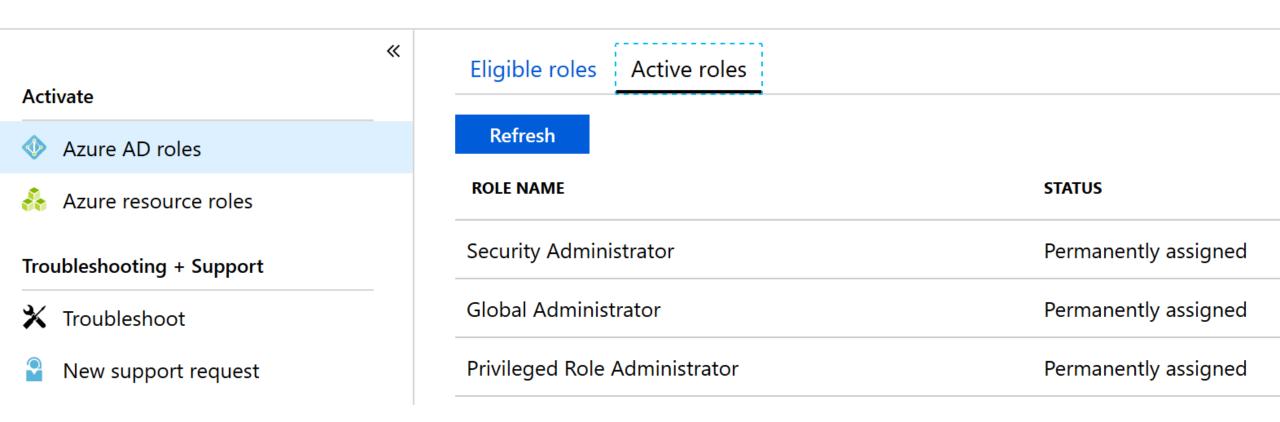
Leverage PIM to Minimize Admin Rights

Azure AD directory roles - Ov international genetic technologies	erview			* ×
Overview	O Refresh			
Quick start	Admin view My view			
TASKS	My Activation history for the past 7 days		My roles	
🗲 My roles	2	SECURITY AD		
Approve requests (preview)		GLOBAL AD	Eligible role assignments	^
My requests (preview)	1.5		ROLE NAME STATUS	ACTION
E Review access			No roles found	
MANAGE	0.5	X	Active role assignments	^
🔓 Roles			ROLE NAME STATUS	ACTION
			Security Administrate Permanently assigned	
			Global Administrator Permanently assigned	
Wizard	•		🍰 Privileged Role Admi Permanently assigned	
I Settings	Approve requests			
④ Sign up PIM for Azure AD Dir	Approve Deny Refresh			
ACTIVITY	REQUESTOR ROLE REASO	N REQUEST RECEI	[Sean Metcalf @PyroTek3 Trir	marcSecurity.com
ACTIVITY	No approval requests			

Leverage PIM to Minimize Admin Rights

Home > Trimarc R&D - Overview > Privileged Identity Management > My roles - Azure AD roles

My roles - Azure AD roles



Leverage PIM to Minimize Admin Rights

🕂 Add member 💙 Filter 💍 Refres	sh 📕 Group 🎽 Revi	iew 🞍 Export
✓ Search		
ROLE	ACTIVATION	
DARTH VADER [DARTHVADER@TRIMARCRD.COM]		
Exchange Administrator	Eligible	
Conditional Access Administrator	Eligible	
EXADMIN [EXADMIN@TRIMARCRD.COM]		
Exchange Administrator	Permanent	
Teams Service Administrator	Permanent	
Skype for Business Administrator	Permanent	
Teams Communications Administrat	tor Permanent	
SharePoint Service Administrator	Permanent	[Sean Metcalf @

Microsoft Cloud Security Controls



Microsoft Cloud Security Controls

Security Control	Required Subscription
Multi-Factor Authentication for Office 365	Office 365
Azure Multi-Factor Authentication	Azure AD P1 or Additional cost per user/ per authentication
Conditional Access	Azure AD P1
Privileged Identity Management (PIM)	Azure AD P2 (only admin accounts need this)
Azure AD Password Protection (On-Prem or custom banned password list)	Azure AD P1
Azure Identity Protection	Azure AD P2
Azure ATP (for on-prem AD)	Enterprise Mobility + Security 5 suite (EMS E5)

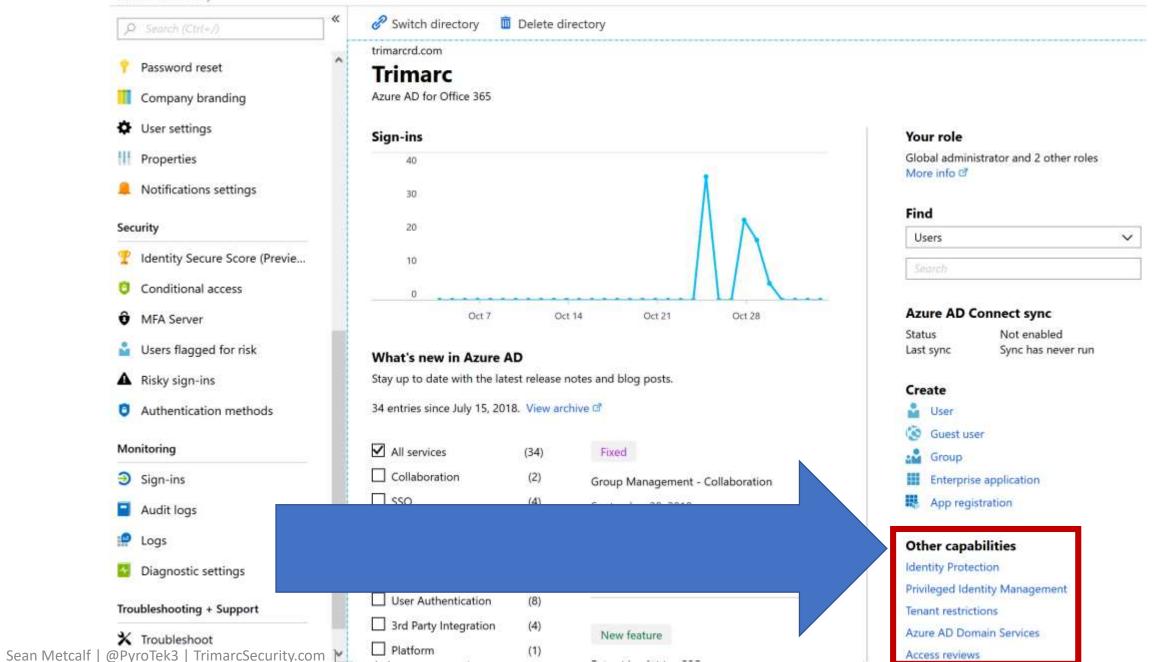
Office 365 E5 does not provide Azure AD Premium features

Enterprise Mobility + Security 5 suite (EMS E5) does

Home > Trimarc - Overview

Trimarc - Overview

Azure Active Directory



-

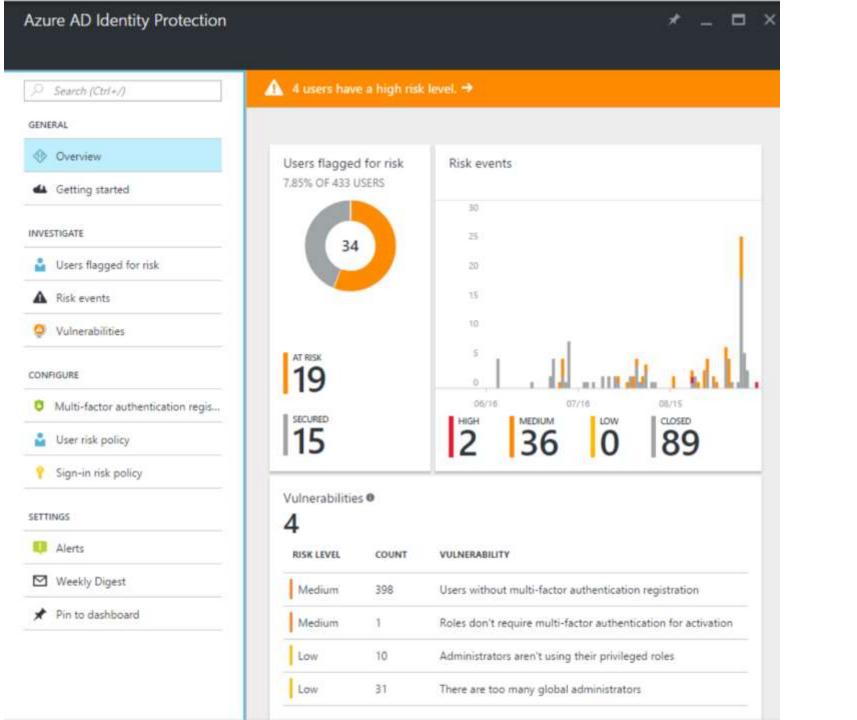
Azure Identity Protection

- Included with Azure AD Premium (P2)
- Have to "install" via the Azure Marketplace (portal.azure.com)
- Dashboard covering identity risk.
- Provides automatic remediation of "risky" sign-ins



Microsoft

Identity



Enable Risk-based Policies

- Requires Azure Identity Protection (Azure AD P2)
- Assigns a risk level during sign-in
- Risk level determines action
 - Force password change
 - Require MFA registration
 - MFA for higher risk authentication

Enable Sign-in Risk Policy

Policy name

Sign-in risk remediation policy

Assignments	
users 🙃 All users	>
Conditions Sign-in risk	>

Controls

Access 🔊	
Require multi-factor authentication	

Review

Estimated impact Number of sign-ins impacted

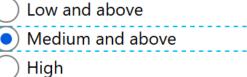
Is this a "risky sign-in"?

- Anonymous IP
- Unfamiliar location

Sign-in risk

1 Info

Select the sign-in risk level



Enforce Policy



>

>

Enable User Risk Remediation Policy

Policy name

User risk remediation policy

🖓 Users 🚯	>
All users	/
🖉 Conditions 🚯	``
User risk	
Controls	
H Access O	>
Require password change	
Review	
🛍 Estimated impact	>
Number of users impacted	/

What's the chance the account is compromised?

- Some detected in real-time
- ~14 day learning period

Sign-in risk

i Info

Select the sign-in risk level

Low and above
Medium and above
High

Enforce Policy



Enable User Risk Remediation Policy

If you want to require MFA for risky sign-ins, you should:

- 1. Enable the <u>multi-factor authentication registration policy</u> for the affected users.
- Require the affected users to sign in to a non-risky session to perform an MFA registration.

Completing these steps ensures that multi-factor authentication is required for a risky sign-in.

The sign-in risk policy is:

- Applied to all browser traffic and sign-ins using modern authentication.
- Not applied to applications using older security protocols by disabling the WS-Trust endpoint at the federated IDP, such as ADFS.

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy
[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

Controlling Access



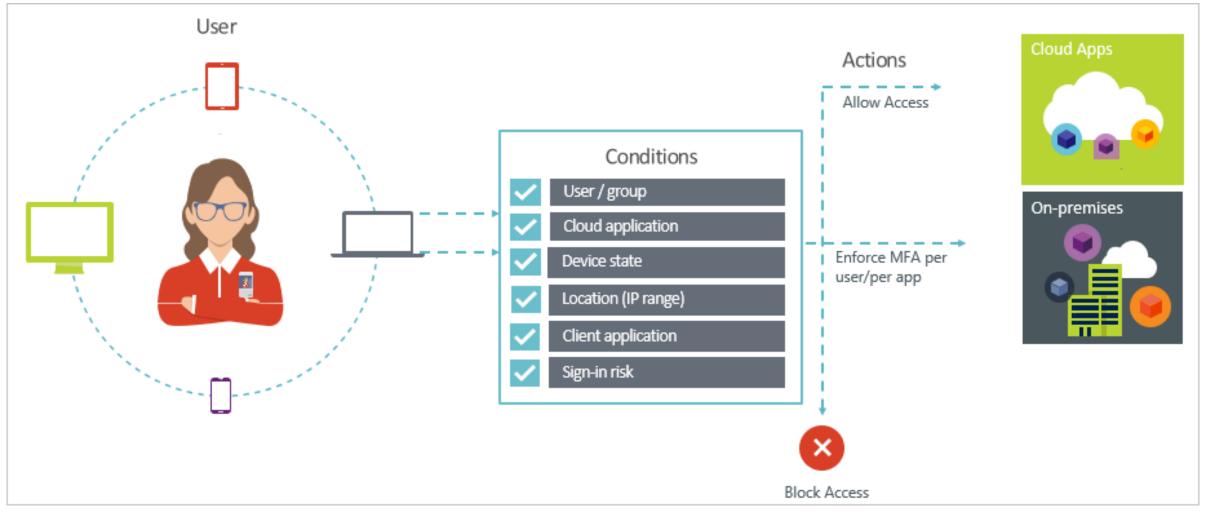


Azure AD Conditional Access

- Enforce different rules on authentication/access based on a variety of conditions.
- Control access based on:
 - Sign-in activity (anomalies?)
 - Network location (corporate network vs internet)
 - Device (AAD Joined?)
 - Application
- Requires Azure AD P1

When this happens	Then do this	Conditional access policy	
[Sean Metcalf @PyroTek3 TrimarcSecurity.com]		Conditions	Access controls

Conditional Access



https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Baseline Protection (Preview)

- Set of predefined conditional access policies.
- First Baseline Protection Policy: Require MFA for admins
- While baseline policies are in preview, enable "Automatically enable policy in the future" so the policy is automatically enabled once the policy reaches General Availability.
- Available for all Azure AD users (AAD Premium not required).

Legacy Authentication

Why Block Legacy Authentication?

- 350K compromised accounts in April 2018 due to password spray, 200K in the last month.
- Nearly 100% of password spray attacks we see are from legacy authentication
- Blocking legacy authentication reduces compromise rate by 66%
- <u>https://aka.ms/PasswordSprayBestPractices</u>

Source: Microsoft Ignite Conference 2018

Legacy vs Modern Authentication

Legacy Auth

- Office 2010 and older
- Office 2013 (requires patch + reg key to support modern auth)
- Clients that use mail protocols such as IMAP/SMTP/POP
- Older PowerShell modules

Modern Auth

- Office 2013 (requires enabling)
- Office 2016 (PC & Mac)
- Outlook Mobile
- iOS 11 Mail app

Step 1: Understand the usage of Legacy Authentication in your organization

- Use sign in logs to examine current usage. Filter by Client App (add column if you do not see it)
- POP, IMAP, MAPI, SMTP and ActiveSync go to Exchange Online
- "Other Clients" shows SharePoint and Exchange Web Services
- You can export/download the sign in logs, sort by Client App and identify the top offenders

Source: Microsoft Ignite Conference 2018

ign-In Events						
∎ Columns 🖸 Refi	resh 👱 Dow	vnload 🛨 Script 🗗 F	Power BI 🗙 Troubleshoot			
	tive and suppor	ts "starts with" operator				
er	201	Username	Application		Sign-in status	has
Filter by name or object	117	Filter by UPN	Fatter by app	name or application	All	~
ent App Any	^	Conditional Access	~			
1111/11	~	Show dates as:				
Any Browser		Local UTC				
ixchange ActiveSync						
ana See an See an						
xchange ActiveSync (s	108280210101010101010					
xchange ActiveSync (u	an a	USERNAME	APPLICATION	SIGN-IN STATUS	CLIENT APP	CONDITIONAL ACC.
Nobile Apps and Deskt	op clients	5203429-2239-16-5				
Other clients		audrey.oliver@w	ingt Azure Portal	Success	Browser	Success
Other clients; IMAP		audrey oliver@w	ingt Azure Portal	Failure	Browser	Success
Other clients; MAPI		uddrey.onver.en	ingen Paule Fortai	rundre	biotiser	Juccess
Other clients; Older Off	ice clients	audrey.oliver@w	ingt Azure Portal	Failure	Browser	Failure
Other clients; POP		audrey olivor@w	ingt Azure Portal	Failure	Unknown	Not Applied
Other clients; SMTP		audrey.onver@w	ing Azure Fortai	rdifure	UNKNOWN	Not Applied
/17/2018, 1:15:08 AM	Hannah Han	hannahhanhaha	@wi Microsoft App Acce.	Success	Browser	Success
/16/2018, 11:11:35 PM	Barbara Kess	barbarak@wingt	ipt Azure Portal	Success	Browser	Not Applied
/16/2018, 11:11:24 PM	Barbara Kess	barbarak@wingt	ipt Azure Portal	Failure	Unknown	Not Applied
/16/2018, 11:10:58 PM	Barbara Kess	barbarak@wingt	ipt Azure Portal	Failure	Unknown	Not Applied

Disable Legacy Auth

Home > Conditional access - Policies	> Block Lega	acy Access > Conditions > Client apps (pr	eview)	
Block Legacy Access	×	Conditions	×	Client apps (preview) \Box ×
🚺 Info 📋 Delete		1 Info		Configure 0
* Name Block Legacy Access		Sign-in risk 🛛 Not configured	>	Yes No Select the client apps this policy will apply to
Assignments	- 1	Device platforms ① All platforms (including unsuppo	>	 Browser Mobile apps and desktop clients
Users and groups ① Specific users included	>	Locations 🛛 Not configured	>	Modern authentication clients
Cloud apps 🛛 All cloud apps included and 1	>	Client apps (preview) 💿 1 included	>	Exchange ActiveSync clients Other clients
Conditions ① 2 conditions selected	>	Device state (preview) 0 Not configured	>	
Access controls		а		
Grant 🔀 Block access	>			
Session 0 controls selected	>			
Enable policy On Off		[Sean Metcalf @Py	/roTek3	TrimarcSecurity.com]

Disable Service Access

- Outlook on the Web (OWA)
- Outlook desktop (MAPI)
- Exchange Web Services (EWS)
- Mobile (Exchange ActiveSync)
- IMAP
- POP

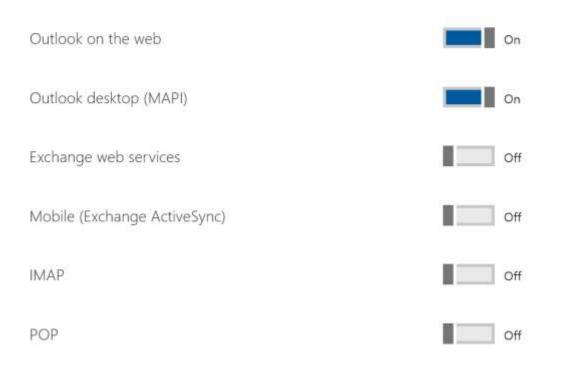
Email apps

MB

Bailey

bailey@trimarcrd.com

Choose the apps the user can use to access their Office 365 email.



Save Cancel

Azure AD Connect Health - ADFS

Home > Azure Active Directory Connect Health - AD FS services > fs.fabidentity.com > Risky IP [Preview]

Risky	IP	[Preview]
the table to be	1111.1 000	Care I

Home > Azure Active Directory Connect Health > Io Risky IP [Preview] Iogin.fabtoso.com		🛓 Download 🛛 🕅 N	lotification Settings	🔅 Threshold Settings			
		€ Learn more about this report notifications and solution recommendations →					
🛨 Download 🖾 Not	ification Settings	TIMESTAMP	TRIGGER TYPE	IP ADDRESS	BAD PASSWORD ERROR CO	EXTRANET LOCKOUT ERROR	UNIQUE USERS ATTEMPTE
1 Learn more about th	is report notifications a	9/26/2018 6:00 PM	hour	52.231.77.95	0	1728	3
TIMESTAMP	TRUCCES TUBE	9/26/2018 5:00 PM	hour	52.231.77.95	0	1728	3
TIMESTAMP	TRIGGER TYPE	9/26/2018 4:00 PM	hour	52.231.77.95	0	1728	3
3/5/2018 11:00 PM	hour	9/26/2018 3:00 PM	hour	52.231.77.95	0	2939	3
3/5/2018 10:00 PM	hour	9/26/2018 2:00 PM	hour	52.231.77.95	0	2245	3
3/5/2018 4:00 PM	hour	9/26/2018 1:00 PM	hour	52.231.77.95	0	1728	3
5.17.17.61.0 L 60. PM 1		9/26/2018 12:00 PM	hour	52.231.77.95	0	2090	3
3/5/2018 4:00 PM	day	9/26/2018 11:00 AM	hour	52.231.77.95	0	3068	3
		9/26/2018 10:00 AM	hour	52.231.77.95	0	1754	3

https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Monitor-your-ADFS-sign-inactivity-using-Azure-AD-Connect-Health/ba-p/245395



ADFS External Smart Lockout

- Update ADFS servers to Windows Server 2016 (or 2019).
- Provides enhanced protection against on-prem AD lockouts during external password spray attacks.
- External Smart Lockout: Locks out attackers while allows valid users access.
- ADFS 2019
 - Independent lockout thresholds for familiar & unfamiliar locations.
 - Smart lockout audit mode while still leveraging soft lockout.
- External Lockout Best Practice Configuration (ADFS 2016):
 - Set-AdfsProperties -EnableExtranetLockout \$true -ExtranetLockoutThreshold 15 -ExtranetObservationWindow (new-timespan -Minutes 30) -ExtranetLockoutRequirePDC \$false

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-extranet-smart-lockout-protection
[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

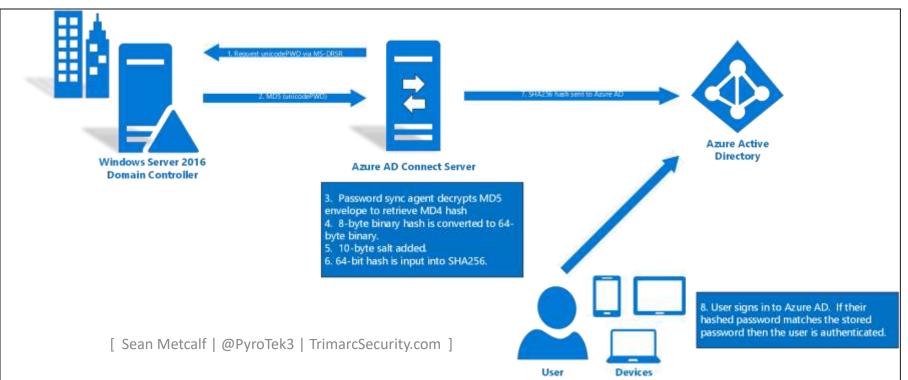
Gaining Password Insight



[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

Password Hash Sync, What & Why?

- Azure AD Connect provides capability.
- Requests password hashes from Active Directory Domain Controllers on-prem.
- Hashes these hashes (MD4+salt+PBKDF2+HMAC-SHA256)
- Sends to Azure AD tenant.
- Microsoft can identify & flag Azure AD users with bad passwords (& Dark Web).



Azure AD Smart Lockout

- Smart lockout uses cloud intelligence to identify & lockout attackers guessing passwords.
- Determines logon activity differences between valid users & attackers.
- Included in all versions of Azure AD ("free").

https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Password-Protection-and-Smart-Lockout-are-now-in-Public/ba-p/245423

Azure AD Password Protection

- Global banned password list (All users)
- Custom banned password list (Azure AD P1)
- Dynamic banned passwords (All Users)
 - Letter substitution
 - Fuzzy matching (shorter versions of banned passwords)
 - Substring matching
 - Scoring: <5 points = blocked

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad

Azure AD Premium Password Protection

- On-prem Active Directory solution.
- Requires Azure AD P1, DCs running 2012+, & DFSR (SYSVOL replication).
- Microsoft Password Filter deployed to DCs.
- 1-2 Proxy servers configured in the AD forest.
- Blocks >500 commonly used passwords (plus > 1M pw character substitution).
- Audit or Enforce password restrictions.
- Usage reporting (Get-AzureADPasswordProtectionSummaryReport)

SYSVOL > trimarcresearch.com > Policies > {4A9AB66B-4365-4C2A-996C-58ED9927332D} > AzureADPasswordProtection >						
Name	Date modified	Туре	Size			
Azure	11/3/2018 10:57 PM	File folder				
📙 Configuration	11/3/2018 10:57 PM	File folder				
PasswordPolicies	11/3/2018 10:57 PM	File folder				

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises

Azure AD Premium Password Protection

Authentication methods (Preview) - Password protection (Preview)

Trimarc R&D - Azure AD Security

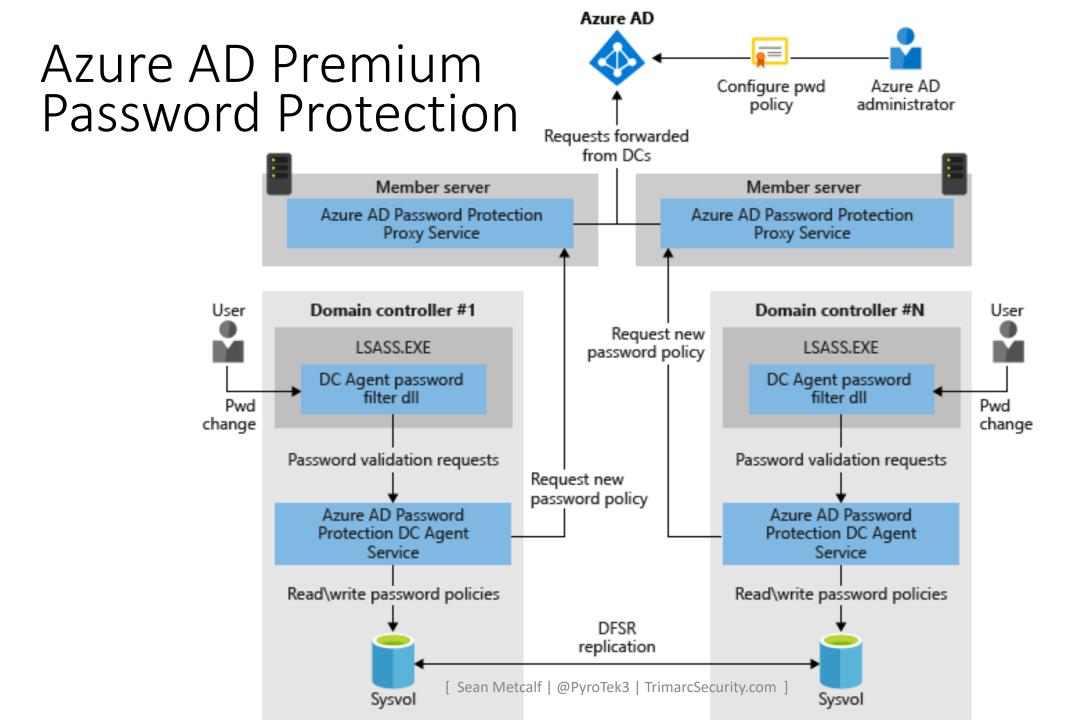
Lockout threshold ① Lockout duration in seconds ① Custom banned passwor	10 60 rds	~
Custom banned passwor		~
	ds	
Enforce custom list 🕤	Yes	No
	Trimarc Washington DCUnited	~
Custom banned password list (
Password protection for	Windows Server Active Directo	ry
	Password protection for	Washington DCUnited

Mode 0

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com

Enforced

Audit

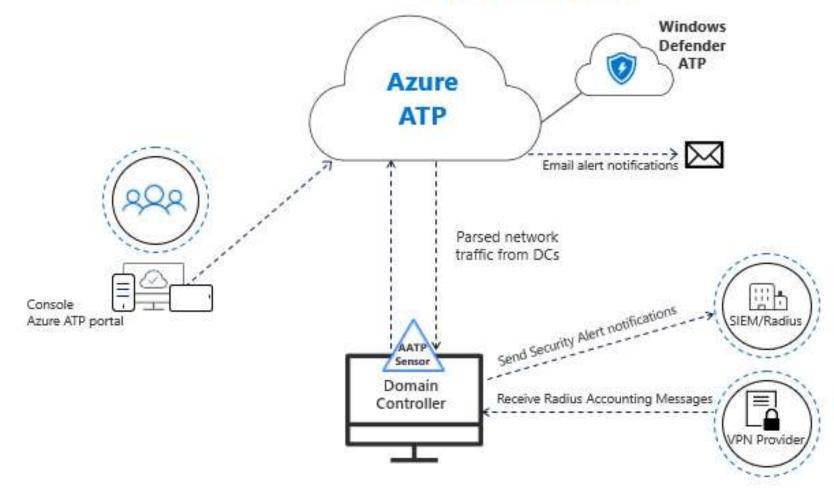


Azure ATP

- Cloud based security solution for on-prem Active Directory.
- Requires licensing (Enterprise Mobility + Security 5 suite (EMS E5))
- Effectively Microsoft Advanced Threat Analytics (ATA) in the cloud.
- Azure ATP client "sensor" installed on Domain Controllers.

Azure ATP

Azure ATP Architecture



Microsoft Cloud Security "Tune Up"



[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

Secure Score



Your Secure Score

Secure Score figures out what Office 365 services you are using, then looks at your configuration and behaviors and compares it to a baseline asserted by Microsoft. If your configuration and behaviors are in line with best practices, you will get points, which you can track over time. More importantly, you will be able to quick determine what things you can do to reduce their risk

Secure Score

Enable MFA for Azure AD privileged roles

You should enable MFA for all of your Azure AD privileged roles because a breach of any of those accounts can lead to a breach of any of your data. We found that you had 1 admins out of 1 that did not have MFA enabled. If you enable MFA for those 1 admin accounts, your score will go up 50 points.

Action Category	
User Impact	

Implementation Cost

Action Score

37 31 64 0 Office 365 Office 365 Office 365 Please Seat Size Select Average Secure Score Average Industry Secure Score Type Score

Compare your score

 \sim

Identity

Low

Low

0/50

Threats

- Password Cracking
- Account Breach
- Elevation of Privilege

Compliance Controls

ISO 27018:2014; Control C.9.4.2, A.10.8

Ignore

Third Party

- CSA CCM301; Control DSI-02
- GDPR; Control 6.6.5

Show more +





Seat size this tenant belongs to is 6 - 99 seats

Enable Client Rules Forwarding Block

What am I about to change?

There are several ways today that a bad actor can use external mail forwarding to exfiltrate data.

- 1. Client created external mail forwarding Rules, such as the Outlook desktop client.
- Admins can set up external mail forwarding for a user via setting ForwardingSmtpAddress on a user object.
- 3. Admins can create external transport rules to forward messages.
- 4. Client created ForwardingSmtpAddress via Outlook Web Access interface

This Security Control action will help mitigate Client created external mail forwarding rules.

A simple mitigation is to, on each Remote Domain, including the Default to disallow Auto-Forwarding. This is a global setting and applies to every email sent from within a Tenant, as a result it is a very broad approach, which does not allow white listing. More details can be found here. RBAC roles can be used to achieve a similar result.

Using a properly configured Transport Rule we can control the impact of data exfiltration via Client created external mail forwarding rules. This approach has a couple of advantages:

- Clients will receive a custom NDR message, useful for highlighting to end users external forwarding rules they may have not known existed (accidental exfiltration), or external forwarding rules created by a bad actor on a compromised mailbox.
- 2. Allows a whitelist of users or groups to be configured to allow business approved exceptions to the policy.
- Provides some mitigation, for when an Admin account has been used to create a Remote Domain with auto-forwarding enabled to specific namespace to exfiltrate data.
- 4. Provides some mitigation, for when an Admin account has been used to alter the Default Remote Domain settings.

This Security Control will create a transport the type AutoForward, mitigating the use c

Enable Client Rules Forwarding Block Complete

able Olient Rules FO



Apply More 🗗 Cancel

You have successfully created the transport rule that blocks the use of client-side forwarding rules. We found that you had 0 Rules out of 0 that did have blocks enabled.

Your score will increase by 20 points within 24 hours. We found that you had 0 Rules out of 0 that did have blocks enabled. [Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

X

×

Secure Score – Highest Priority Items

Recommended

ASAP

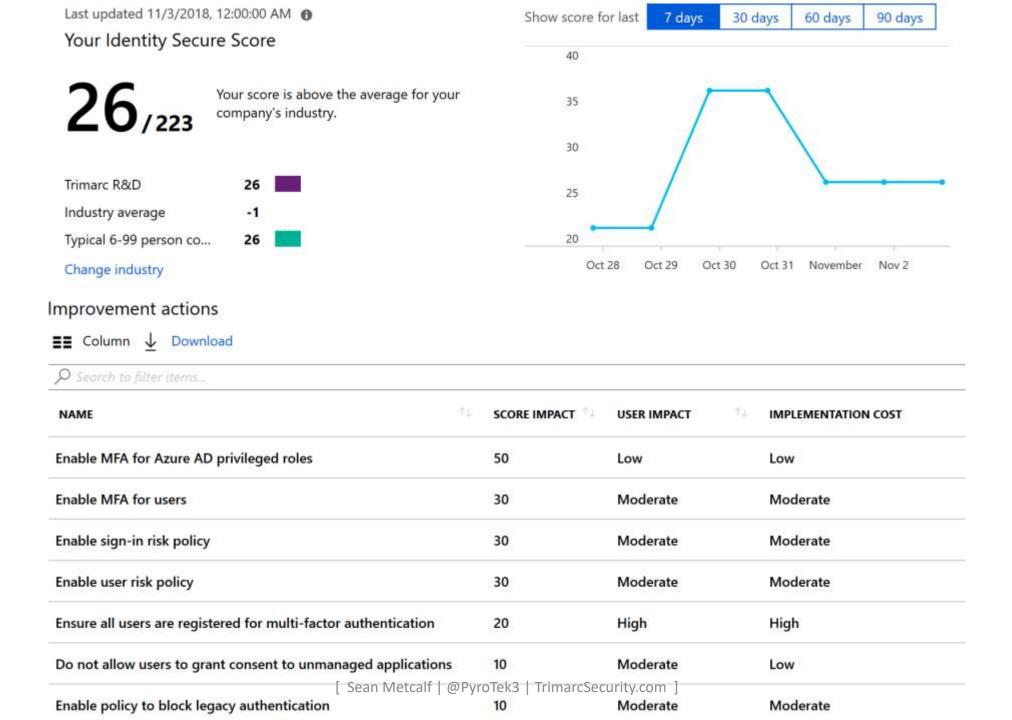
Additional

required

subscription

Action	Score Increase
Enable MFA for Azure AD privileged roles	50
Enable MFA for users	30
Enable sign-in risk policy	30
Enable user risk policy	30
Enable Client Rules Forwarding Block	20
Enable Cloud App Security Console	20
Enable Data Loss Prevention policies	20
Enable Microsoft Intune Mobile Device Management	20
Enable policy to block legacy authentication	20
Ensure all users are registered for multi-factor authentication	20
Review permissions & block risky OAuth applications connected	20
Set automated notification for new OAuth applications connected	20
Set automated notifications for new and trending cloud applications	20

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



Home > Manage advanced alerts

Manage advanced alerts



Your subscription allows you to use Office 365 Cloud App Security!

Take advantage of features such as:

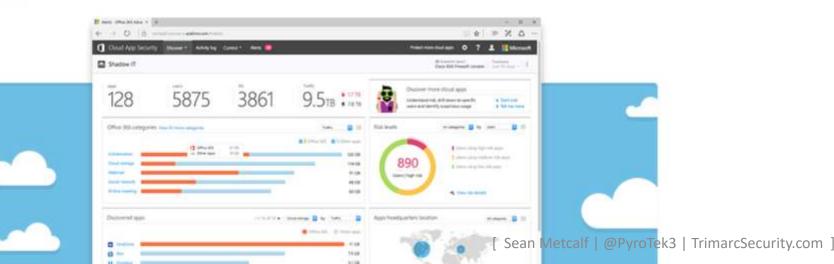
Turn on Office 365 Cloud App Security

- Alerts Create alerts and investigate anomalous and suspicious behavior
- Productivity app discovery Gain visibility into how Office 365 and other productivity cloud services are being used
- App permissions View and control which apps have been granted permissions to your Office 365 environment

Investigate identity behavior across cloud apps

Microsoft Cloud app security Go to Office 365 Cloud App Security
Learn more about Office 365 Cloud App Security
Office 365 Cloud App Security is powered by Microsoft Cloud App Security service which is a separate online service



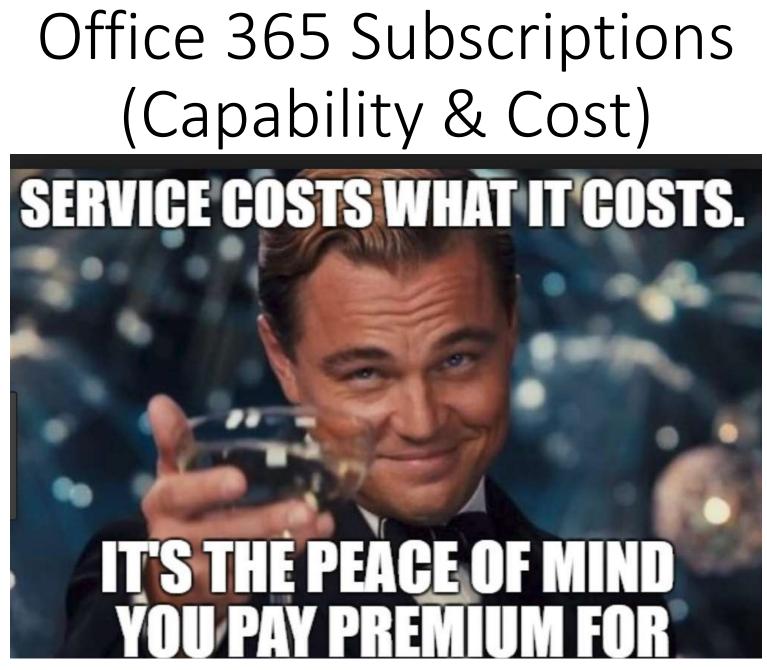


Privileged accounts

Get started with Cloud App Security Create a Cloud Discovery report Connect apps (III) Create policies | Learn more... General dashboard General dashboard > 9 178 10 177activities monitored files monitored accounts monitored View dashboard for a specific app ŝ Discover your cloud apps 6:0) upload traffic logs user notifications sent governance actions taken Office 365 Microsoft OneDrive for **Business** BY ALERT TYPE 0 BY SEVERITY Open alerts Microsoft SharePoint New over the last month -Online High Custom Microsoft Azure Medium RECENT ALERTS Built-in No data No data Low Microsoft Cloud App Security Microsoft Exchange Online Top 3 alert types View all apps... View dashboard for a specific risk type Threat detection Sean Metcalf | @PyroTek3 | TrimarcSecurity.com] View all alerts..

Q

	Cloud App Security						☺ ?	ŝ	e N
	Policies								
Č.	NAME TYPE	STATUS	SEV	ERITY	CATEGORY			¥ A	Advance
	Policy nameSelect type ~	ACTIVE DI	SABLED		Select risk ca	tegory	~		
	1	- 17 of 17 Policies				Create p	olicy -		٣
	Policy	Count	Severity 🗸	Category	Action	Modified			
	Unusual file share activity (by user)	0 open alerts		# Threat detection	0	Oct 24, 2018	\$	i=	:
	This policy profiles your environment and triggers alerts when users .	••							
	Unusual file download (by user)	0 open alerts		Threat detection	0	Oct 24, 2018	0	lΞ	:
	This policy profiles your environment and triggers alerts when users .	##. 							
	Multiple failed login attempts	0 open alerts		Threat detection	0	Oct 24, 2018	\$	ίΞ	÷
	This policy profiles your environment and triggers alerts when users	14.							
	Unusual file deletion activity (by user)	0 open alerts		# Threat detection	0	Oct 24, 2018	0	i=	÷
	This policy profiles your environment and triggers alerts when users .	H.							
	Activity from suspicious IP addresses	0 open alerts		# Threat detection	0	Oct 24, 2018	¢	13	-
	This policy profiles your environment and triggers alerts when activit.								
		" Metcalf @PyroTek 0 open alerts	3 TrimarcSec	urity.com]	0	Oct 24, 2018	0	IE	



[[] Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

Office 365 Enterprise Tiers

Enterprise 1 (E1) - \$8 user/month	Enterprise 3 (E3) - \$20 user/month	Enterprise 5 (E5) - \$35 user/month
50 GB mailbox	50 GB mailbox	100 GB mailbox
File storage and sharing with 1 TB OneDrive storage	Unlimited personal cloud storage	Unlimited personal cloud storage
No Office installed apps	Desktop versions of Office applications (One license covers 5 phones, 5 tablets, and 5 PCs or Macs per user)	Desktop versions of Office applications (One license covers 5 phones, 5 tablets, and 5 PCs or Macs per user)
	eDiscovery with in-place search, hold, and export	eDiscovery with in-place search, hold, and export
		Customer Lockbox
		Office ATP Auto classification, smart import, and more with Advanced Data Governance
	[Sean Metcalf @PyroTek3 TrimarcSecurity.com]	Office 365 Cloud App Security

Azure Active Directory Options

- Free
- Basic: \$1 per user monthly
 - No object limit & Basic reports
- P1: \$6 per user monthly
 - Self-Service Group and app Management
 - Self Service Password Reset/Change/Unlock
 - Two-way sync between on-prem & Azure AD
 - Multi-Factor Authentication (Cloud and On-premises (MFA Server))
 - Cloud App Discovery
 - Conditional Access based on group, location, and device state
 - Connect Health
 - Microsoft Cloud App Security integration
 - MDM auto-enrollment

• P2: \$9 per user monthly

- Includes P1 features
- Identity Protection
- Privileged Identity Management
- Access Reviews

https://azure.microsoft.com/en-us/pricing/details/active-directory/

Enterprise Mobility + Security Options

Enterprise Mobility + Security

E3

Azure AD P1: \$6

Azure Active Directory Premium P1

- Intune
- Azure Information Protection P1

\$874**

per user per month

• Advanced Threat Analytics

Enterprise Mobility + Security



- Azure Active Directory Premium P2
- Intune
- Azure Information Protection P2
- Advanced Threat Analytics
- Cloud App Security
- Azure Advanced Threat Protection

\$14.80**

Azure AD P2: \$9

Approximate Microsoft Cloud Cost (\$26 - \$50 user/month)

- Office 365 E3 & Azure AD
 - Office 365 E3 (\$20) + Azure AD P1 (\$6) = \$26/user/month
 - Office 365 E3 (\$20) + Azure AD P2 (\$9) = \$29/user/month
- Office 365 E5 & Azure AD
 - Office 365 E5 (\$35) + Azure AD P1 (\$6) = \$41/user/month
 - Office 365 E5 (\$35) + Azure AD P2 (\$9) = \$44/user/month
- Office 365 E3 & Enterprise Mobility + Security
 - Office 365 E3 (\$20) + Enterprise Mobility + Security E3 (\$8.74) = ~\$29/user/month
 - Office 365 E3 (\$20) + Enterprise Mobility + Security E5 (\$14.80) = ~\$35/user/month
- Office 365 E5 & Enterprise Mobility + Security
 - Office 365 E5 (\$35) + Enterprise Mobility + Security E3 (\$8.74) = ~\$44/user/month
 - Office 365 E5 (\$35) + Enterprise Mobility + Security E5 (\$14.80) = ~\$50/user/month

Note: Plan for Azure AD P2 for all admin accounts to leverage PIM

Mini Celebration Time!



[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



@markmorow can we get more than 16 character passwords in Azure AD? Like maybe 30? cc: @NerdPyle

Sean Metcalf @PyroTek3 · Oct 26, 2016 Replying to @PyroTek3 .@blueMahakala @NerdPyle Active Directory supports ~128 char passwords msdn.microsoft.com/en-us/library/... Azure AD, not so much: 16 characters maximum

- 8 characters minimum and 16 characters maximu
- Strong passwords only: Requires 3 out of 4 of th
 - Lowercase characters
 - Uppercase characters
 - Numbers (0-9)
 - Symbols (see password restrictions above)

Note:

I wasn't the only one asking for this. Though I did pester Microsoft a lot...

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com

Reset password

Password

Admin-created

Auto-generate password

Let me create the password

Password *

..........

Weak

Make this user change their password when they first sign in

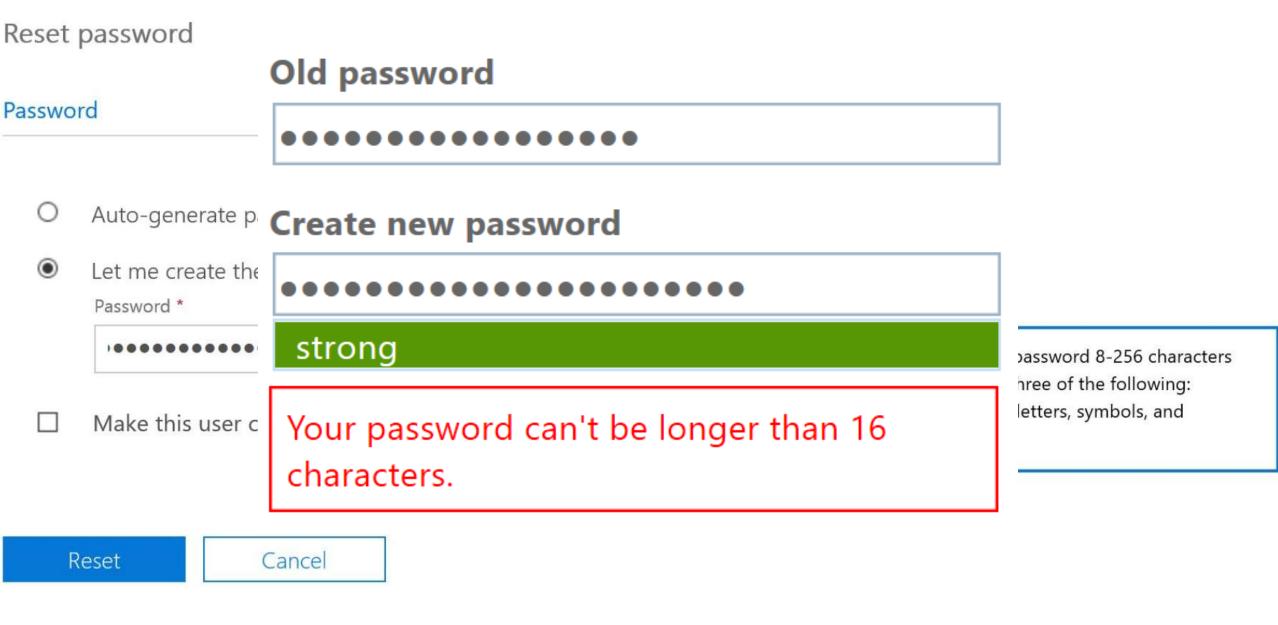
You need to create a strong password 8-256 characters long that combines at least three of the following: uppercase letters, lowercase letters, symbols, and numbers.

Reset Cancel

Reset password

Passwo	ord	Admin-created
○ ●	Auto-generate Let me create Password *	You need to create a strong password 8-256 characters long that combines at least three of the following: uppercase letters, lowercase letters, symbols, and numbers.

Reset Cancel



	Old password				
Reset password	•••••				
Password Adm	Create new password				
	•••••				
O Auto-generate password	strong				
Note:	Your password can't be longer than 16 characters.				
Microsoft has not announced anything about					
this, so the increased password character					
length is likely still being rolled out. Consider this a limited "Preview" ;)					

CLOUD SECURITY

YOU KEEP USING THAT TERM, I DO NOT THINK IT MEANS WHAT YOU THINK IT MEANS memegenerator.net

Cloud Security Best Practices

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

Microsoft Cloud Recommendations Summary

- Disable user access protocols that aren't required goal is Modern Auth with MFA.
- Enable user and admin activity logging in Office 365 (UnifiedAuditLogIngestionEnabled).
- Enable mailbox activity auditing on all O365 mailboxes.
- Review the recommendations in Office Secure Score and implement as many as possible.
- Enable "Password Hash Sync"
- Enable self-service password reset
- Ensure all users are registered for MFA
- Enable MFA for all users
- Enable sign-in & user risk policy
- Conditional Access: Block Legacy Auth (most attacks leverage legacy auth)
- Monitor App registrations.
- Audit consented permissions for apps & user access to apps

Microsoft Cloud: Protecting Admin Accounts

- Enforce MFA on all admin accounts
- Many of the basics remain the same
 - Least privilege is key and poorly understood in many cloud implementations
 - Least access, use the security features provided by the cloud
 - Cloud admin workstations treat same as privileged users
- Limit admin role membership and monitor group membership. PIM can help.

Summary

- The cloud isn't inherently secure.
- There are many security features and controls that are available.
- Security controls need to be researched, tested, and implemented.
- Security in the cloud may cost extra.
- Cloud features change regularly. This talk is likely already out of date...

Sean Metcalf | @PyroTek3 | Trimarcsecurity.com

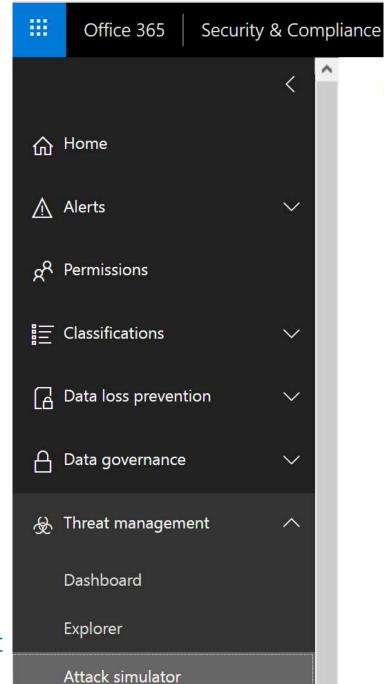
Slides: Presentations.ADSecurity.org



Sean Metcalf (@Pyrotek3) s e a n [@] TrimarcSecurity.com <u>www.ADSecurity.org</u> <u>TrimarcSecurity.com</u>

BONUS: Testing Defenses https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



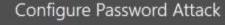
Simulate the Attack: Password Spray

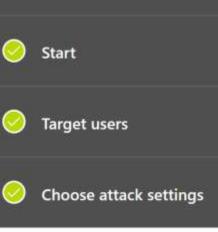
Security & Compliance

🔬 Threat management

Attack simulator

 \sim





Confirm

Please confirm your settings: Users: bailey@trimarcrd.com BobaFett@TrimarcRD.com DarthVader@TrimarcRD.com HanSolo@TrimarcRD.com JangoFett@TrimarcRD.com JoeUser@TrimarcRD.com Leia@TrimarcRD.com ObiWanKenobi@TrimarcRD.com Yoda@TrimarcRD.com Are you sure you want proceed with your password attack?



Confirm

Simulate the Attack : Password Spray

Security & Compliance & Threat management

nt ^

Attack simulator

< Password Spray Attack

Attack Details

A password spray attack against an organization is typically done by running a list of commonly used passwords against a list of valid Office 365 user accounts. Typically, the attacker crafts one password to try against all of the known user accounts. If the attack is not successful, the attacker will try again using another carefully crafted password, usually with a waiting period between attempts to avoid policy-based account lockout triggers. Current Attack Status TrimarcRD Password Spray Attack (Winter2018!) 33% of user accounts attempted 1 of 9 users have been compromised

Terminate Attack

Hybrid Identity Protection

Simulate the Attack: Password Spray

Security & Compliance & Threat management 🔨 🔨

Attack details

< Report: TrimarcRD Password Spray Attack (Winter2018!)</p>

11/3/2018, 8:08:20 PM to 11/3/2018, 8:09:10 PM

The results from the Password Spray attack scenario are shown below. These results indicate the success of the attack and susceptibility of employees to this attack vector.

Attack simulator

Total users targeted 9 Successful attempts 1 Overall Success Rate 11%

For this attack, 1 of 9 users were found to be susceptible to Password Spray attacks.

Compromised Users

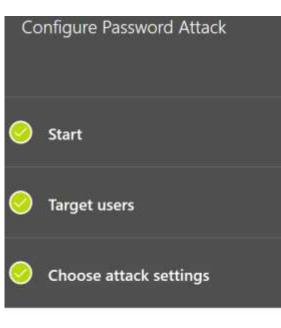
BobaFett@TrimarcRD.com

Security & Compliance

🛞 Threat management

Attack simulator

 \sim



Confirm

Please confirm your settings: Users: bailey@trimarcrd.com BobaFett@TrimarcRD.com DarthVader@TrimarcRD.com HanSolo@TrimarcRD.com JangoFett@TrimarcRD.com JoeUser@TrimarcRD.com Leia@TrimarcRD.com ObiWanKenobi@TrimarcRD.com Yoda@TrimarcRD.com Are you sure you want proceed with your password attack?

Back Finish Cancel

Confirm

Security & Compliance 🛞 Threat management

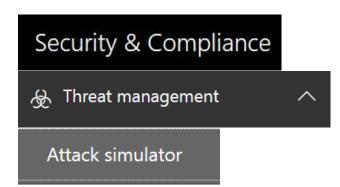
Attack simulator

 \sim

Brute Force Password (Dictionary Attack) Account Breach

A brute-force attack dictionary is an automated, trial-and-error method of generating multiple passwords guesses from a dictionary file against a user's password.

TrimarcRD Password Attack Launch Attack Terminate Attack 22% of user accounts attempted Attack Details 1 of 9 users have been compromised



Attack details

< Brute Force Password (Dictionary Attack)

Attack Details	*
Password cracking techniques are used to guess a user's password by trying many variations with a	Current Attack Status
computer. Once an attacker has the user name and password for a user, the attacker will generally	TrimarcRD Password Attack
be able to sign in to Office 365 and gain access to	initial choir assertion of the ch
additional information, such as other user accounts and sensitive information. Brute-force	
attacks work by calculating every possible	Terminate Attack
combination that could make up a password and	
testing to see if it is the correct password. As the	
password's length increases, the amount of time,	
on average, to find the correct password increases exponentially. This means short passwords can	
usually be discovered rather quickly, but longer	
passwords may take decades to discover. Two	
types of brute-force password attacks exist: a	
dictionary attack using a well-known list of	
passwords, and an exhaustive attack, where	
combinations are tried sequentially. Attack	
simulator uses a dictionary list attack, allowing	
modifications of frequency between attacks and the number of attempts. If a password is	
discovered, the password itself is not shown; only	
an indication that a password was discovered will	
be shown	tcalf @PyroTek3 TrimarcSecurity.com]

Attack details

Report:	TrimarcRD	Password Attack
---------	-----------	-----------------

Security & Compliance

🛞 Threat management

Attack simulator

 11/3/2018, 8:01:54 PM to 11/3/2018, 8:04:41 PM

 The results from the Brute Force Password attack scenario are shown below. These results indicate the success of the attack and susceptibility of employees to this attack vector.

 Total users targeted
 9

 Successful attempts
 For this attack, 6 of 9 users were found to be susceptible to Brute Force Password attacks.

 Overall Success Rate
 For ce Password attacks.

Compromised Users

67%

BobaFett@TrimarcRD.com

DarthVader@TrimarcRD.com

HanSolo@TrimarcRD.com

JangoFett@TrimarcRD.com

JoeUser@TrimarcRD.com

Leia@TrimarcRD.com

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

	Security & Complian	Ce 🔗 Threat management	^	Attack simulator	
C	onfigure Phishing Attack	Provide a name to the o	am	paign	×
	Start	Name Prize Giveaway			
	Target recipients				Use Template
Q	Configure email details	Please select a template in the list Prize Giveaway			
Ď	Compose email	Payroll Update			

Confirm

Please provide email details

From (Name)

TrimarcRD Payroll Update

From (Email)

payrollservices@payrolltooling.com

Phishing Login server Url

http://portal.payrolltooling.com

Custom Landing Page URL

To use a custom landing page for user awareness after an attack, enter your URL here.

Subject

Urgent - Update Your Payroll Details

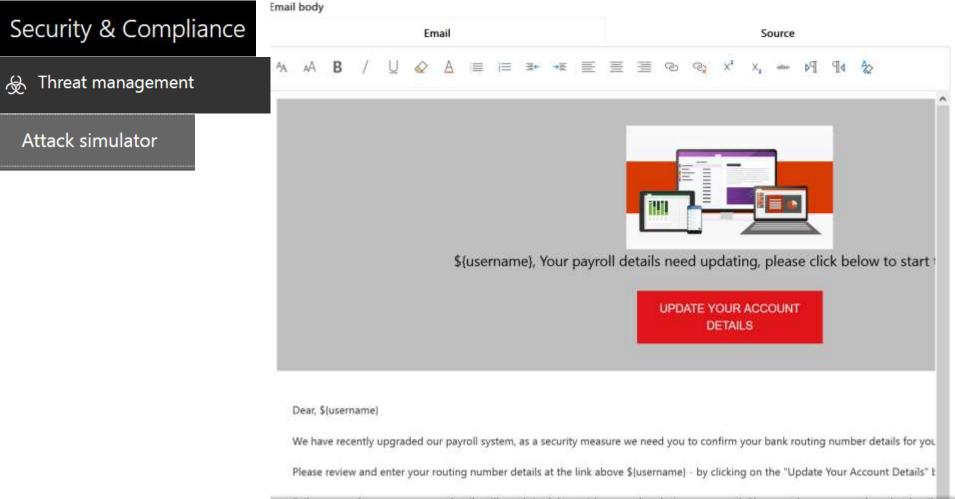


×

-

×

Email body



Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

Security & Compliance \, Security & Compliance

 \bigotimes Threat management

Attack simulator

 \sim

Spear Phishing (Credentials Harvest) Account Breach

A spear-phishing attack is a targeted attempt to acquire sensitive information, such as user names, passwords, and credit card information, by masquerading as a trusted entity. This attack will use a URL to attempt to obtain user names and passwords.

Launch Attack

Attack Details

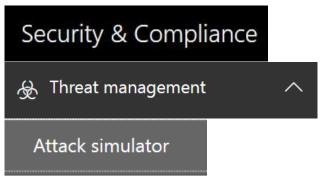
Joe User ∛

Inbox

TrimarcRD Payroll Update

Urgent - Update Your Payroll Details

Joe User, Your payroll details need upc



[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

Urgent - Update Your Payroll Details

TrimarcRD Payroll Update <payrollservices@payrolltooling.com> Today, 8:37 PM



To help protect your privacy, some content in this message has been blocked. To re-enable the blocked features, click here.

To always show content from this sender, click here.

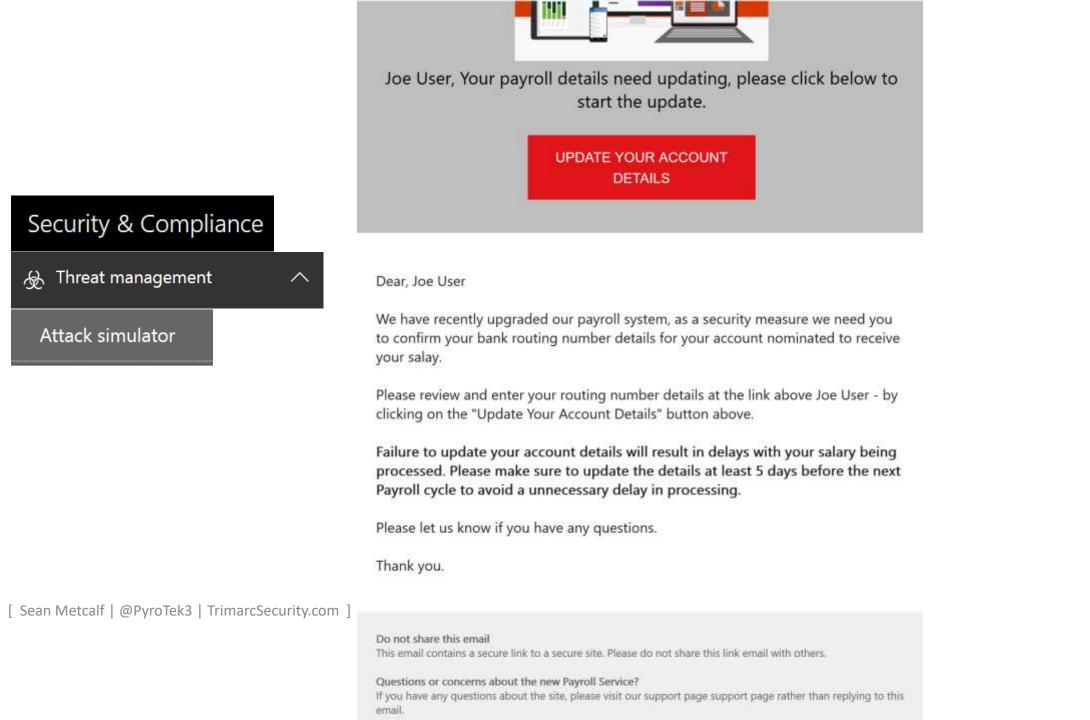


UPDATE YOUR ACCOUNT DETAILS

Dear, Joe User

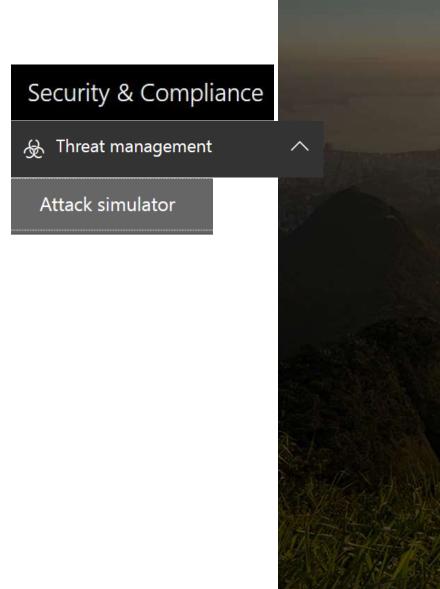
We have recently upgraded our payroll system, as a security measure we need you to confirm your bank routing number details for your account nominated to receive your salay.

Please review and enter your routing number details at the link above Joe User - by





(i) 💋 portal.payrolltooling.com/?id=jmsgrZPD3LnMWsIBJBqcshULfKaufs5z





Sign in

Email, phone, or Skype

Next

No account?Create one!

Can't access your account?

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



Security & Compliance

 \bigotimes Threat management

 \sim

Attack simulator



Sign in

Email, phone, or Skype

This connection is not secure. Logins entered here could be compromised. Learn More

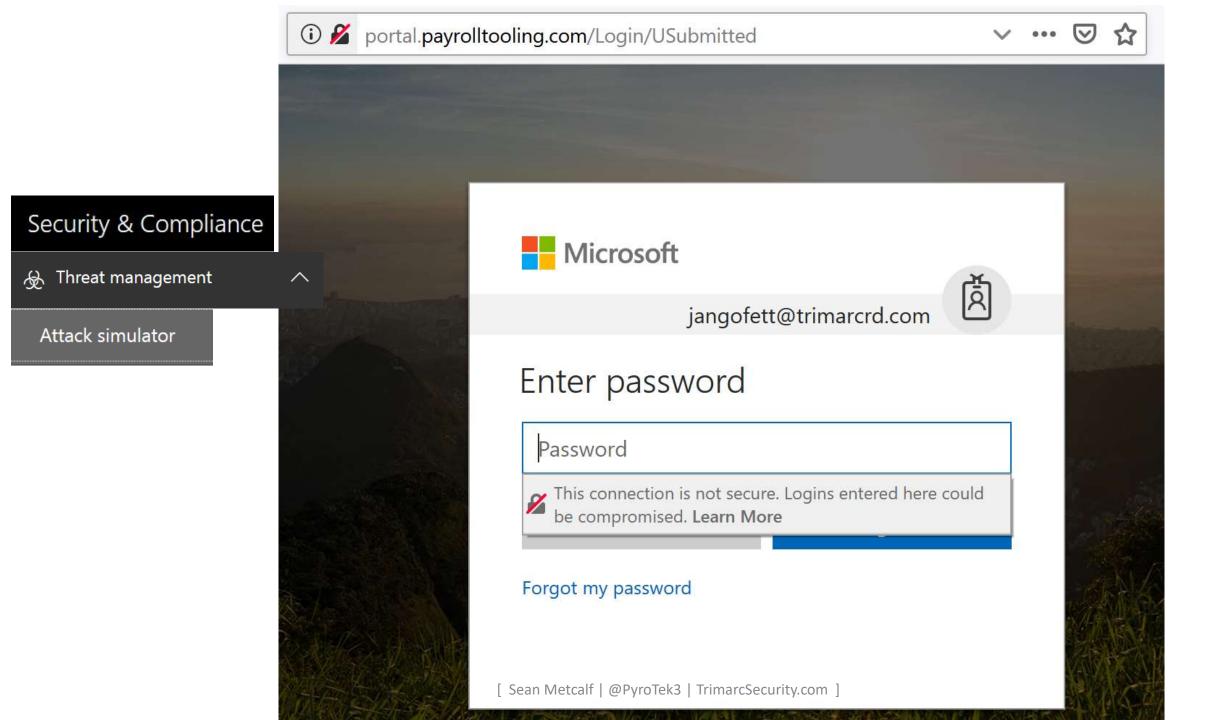
V

...

No account?Create one!

Can't access your account?

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com



III\ 🗊 🤨 📓 🔇



You have been redirected to this web page as a recent message you opened was part of a Phishing awareness test being run by your Organization. You will be contacted shortly by your Administrators for some follow up training on security best practices. In the meantime some high-level information is presented below to help you remain safe.

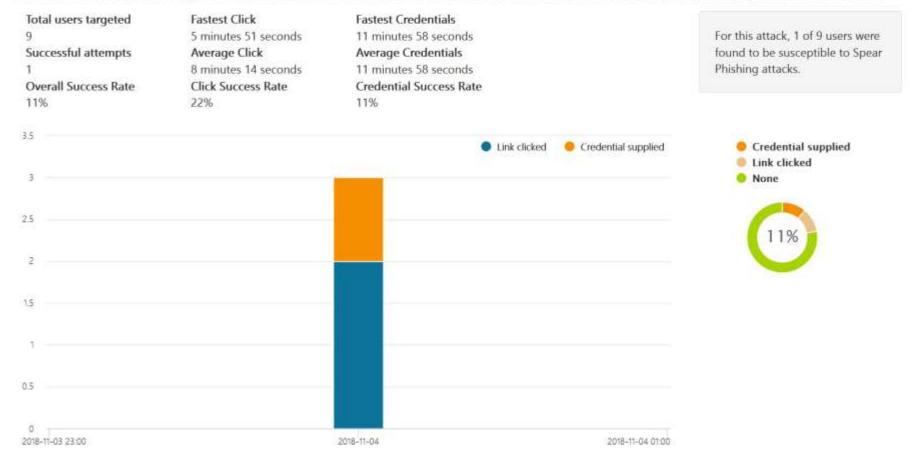
Why are we talking about Phishing?

Phishing happens to everybody. It's a huge problem, and it's getting bigger. In fact, a 2016 study reports that 91% of cyberattacks and the resulting data breach begin with a phishing email. These attacks are becoming more frequent and sophisticated. So much so that one online article states that 97% of people world-wide could not identify a sophisticated phishing attack. And, it's not just your work accounts at risk. These phishers will hack things like your banking, utilities, insurance information and even Facebook, Twitter, and Instagram accounts. [Sean Metcalf]@PyroTek3]TrimarcSecurity.com]

Report: Payroll Update

11/3/2018, 8:37:08 PM to 11/3/2018, 8:37:22 PM

The results from the Spear Phishing attack scenario are shown below. These results indicate the success of the attack and susceptibility of employees to this attack vector.



Compromised Users

JangoFett@TrimarcRD.com Credential supplied: 11/3/2018, 8:49:07 PM Link clicked: 11/3/2018, 8:47:46 PM JoeUser@TrimarcRD.com [Sea Link clicked: 11/3/2018, 8:43:00 PM

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

~