Dragon Advance Tech

Microsoft Sentinel:

Use Case for Microsoft 365 Incident Response on Business Email Compromise

A field guide for deploying of Microsoft Sentinel's Analytic Rules, Workbooks, and Logic Apps for BEC investigators

Version: Draft 1.0
Release date: August 2022

Frankie Li, Ken Ma
ir@dragonadvancetech.com

Contents

About this whitepaper

This whitepaper provides a field guide for deploying Microsoft Sentinel's Analytic Rules, Workbooks, and Logic Apps for Business Email Compromise (BEC) investigators. We intend to provide this guide as a reference example by applying an ATT&CK-based approach to handling BEC and phishing attacks.

In Sept 2021, we developed three use cases by referring to practical scenarios from our incident response task assignments in Microsoft hybrid-cloud environment. You could download a copy at https://github.com/DATCResearch, if you missed this paper.

In the past two years, we have handled a few BEC/Phishing scam incidents from our clients, who are international fund management firms. We also remembered three years ago. We have meetings with other business clients' IT team and their management, who are handling cybersecurity issues on selecting vendors to provide services on the cloud-security matter. In those meetings, people usually ask us a simple question: "Are there any perfect security solutions we can use to prevent BEC/phishing attacks?"

Immediately after those meetings, we were invited to talk to the technical staff handling infrastructure or cybersecurity issues. We tried to explain to them that they are using a "not-so-bad" email SaaS application, and they may not require to buy an additional "plug-in solution" to prevent BEC or phishing attacks. What they need to do at first is to configure and manage the application properly. We usually got replies like these:

- *We have bought E5 licenses for our tenant members, and the reseller should be responsible for configuring our tenant correctly. We have paid them.*
- *We have bought Business Premium licenses; the reseller said we could turn on the MFA to prevent BEC attacks, and the default threat policy will automatically protect us. Please don't give the "turn-on MFA" recommendation to our management because that may create additional works for us.*
- *We have only bought a few E5 licenses, 30% Office E3 licenses, and hundreds of Business Standard licenses. We cannot turn on MFA because our management doesn't want to use MFA, and the Business Standard licenses users cannot use MFA. What threat policies do we need to turn on? Another vendor told us we need to buy an AI-enabled email security solution because our existing email SaaS application requires more workload.*

We had been asked to give "friendly" training or advice on configuring their Microsoft 365 tenant. We usually provide them with online materials and advise them to consult an appropriate technical staff from their security vendors who are the email security domain expert or consult their regional Microsoft solution advisors.

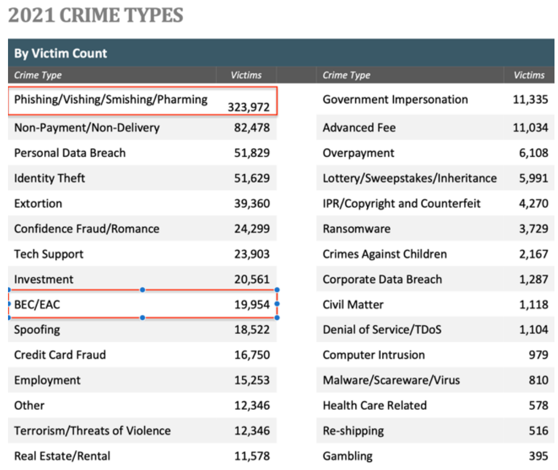
We want to provide a use case for making use of Microsoft Sentinel, ***in a budget way,*** to the community to help them to monitor their tenants and provide a set of practical tools to allow analysts to investigate phishing attacks in the near real-time manner for their tenant.

What is Business Email Compromise (BEC)?

According to the 2021 Internet Crime Report[1] (IC3) from the FBI, BEC/EAC (Email account compromise) has defined a sophisticated scam targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized funds transfers.

The FBI reported[2] on May 4, 2022, that $43 billion in scams continue to grow and evolve, targeting small local businesses to more giant corporations, and found a 65% increase in identified global exposed losses during the COVID-19 pandemic. Even though INTERPOL[3] and US DOJ[4] announced the arrest and charging of some prominent fraudsters, phishing scam activities are expanding in Hong Kong, especially among the local office of investment funds. On March 22, 2022, the Securities and Future Commission ("SFC") published circular[5] about BEC duping unwary staff of licensed corporations (LCs) into sending money and sensitive information.

2021 Crime Types (by Victim Count)

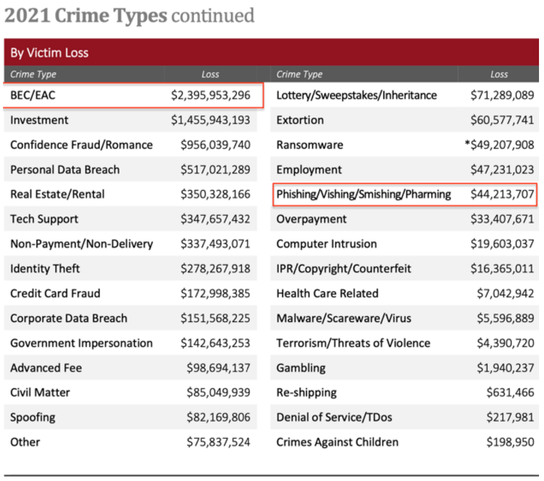


2021 CRIME TYPES

By Victim Count

Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	323,972	Government Impersonation	11,335
Non-Payment/Non-Delivery	82,478	Advanced Fee	11,034
Personal Data Breach	51,829	Overpayment	6,108
Identity Theft	51,629	Lottery/Sweepstakes/Inheritance	5,991
Extortion	39,360	IPR/Copyright and Counterfeit	4,270
Confidence Fraud/Romance	24,299	Ransomware	3,729
Tech Support	23,903	Crimes Against Children	2,167
Investment	20,561	Corporate Data Breach	1,287
BEC/EAC	19,954	Civil Matter	1,118
Spoofing	18,522	Denial of Service/TDoS	1,104
Credit Card Fraud	16,750	Computer Intrusion	979
Employment	15,253	Malware/Scareware/Virus	810
Other	12,346	Health Care Related	578
Terrorism/Threats of Violence	12,346	Re-shipping	516
Real Estate/Rental	11,578	Gambling	395

2021 Crime Types (by Victim Loss)



2021 Crime Types continued

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$2,395,953,296	Lottery/Sweepstakes/Inheritance	$71,289,089
Investment	$1,455,943,193	Extortion	$60,577,741
Confidence Fraud/Romance	$956,039,740	Ransomware	*$49,207,908
Personal Data Breach	$517,021,289	Employment	$47,231,023
Real Estate/Rental	$350,328,166	Phishing/Vishing/Smishing/Pharming	$44,213,707
Tech Support	$347,657,432	Overpayment	$33,407,671
Non-Payment/Non-Delivery	$337,493,071	Computer Intrusion	$19,603,037
Identity Theft	$278,267,918	IPR/Copyright/Counterfeit	$16,365,011
Credit Card Fraud	$172,998,385	Health Care Related	$7,042,942
Corporate Data Breach	$151,568,225	Malware/Scareware/Virus	$5,596,889
Government Impersonation	$142,643,253	Terrorism/Threats of Violence	$4,390,720
Advanced Fee	$98,694,137	Gambling	$1,940,237
Civil Matter	$85,049,939	Re-shipping	$631,466
Spoofing	$82,169,806	Denial of Service/TDos	$217,981
Other	$75,837,524	Crimes Against Children	$198,950

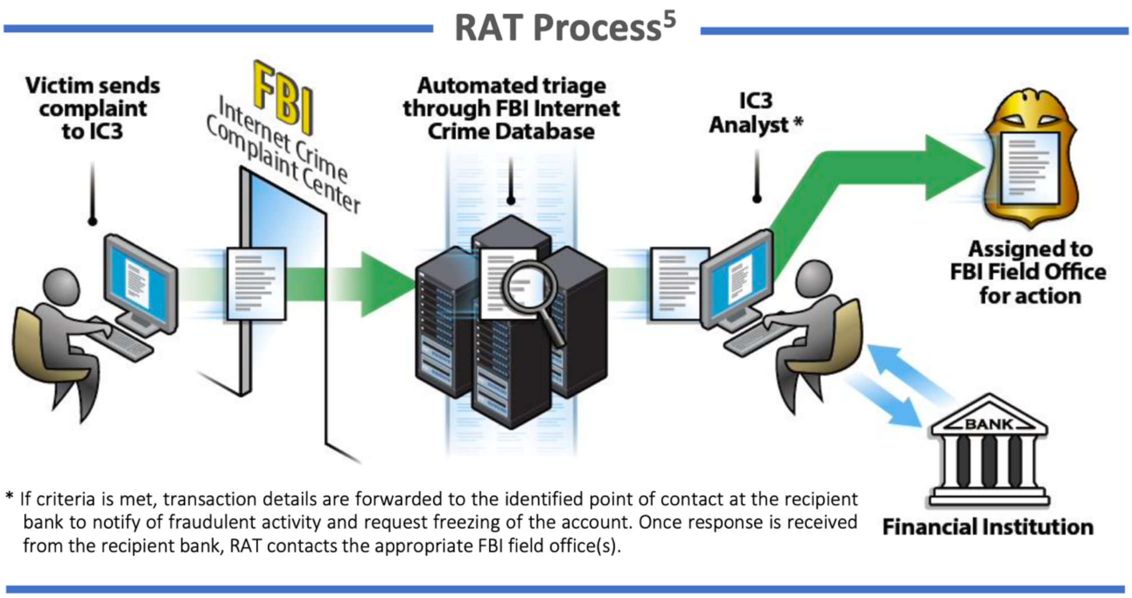
Figures extracted from the 2021 Internet Crime Report (IC3)

Back in August 2017, Andy Robinson of the University of Portsmouth – Institute of Criminal Justice Studies published an in-depth study of BEC attacks entitled "Hacking the Boardroom: Business Email Compromise More than CEO Fraud," in which he evaluates the UK Government "4-P's" approach to cybercrime, how this is currently applied to BEC threats, threat mitigation, and future threat predictions. This research also examines the

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
[2] https://www.ic3.gov/Media/Y2022/PSA220504
[3] https://unit42.paloaltonetworks.com/operation-delilah-business-email-compromise-actor/
[4] https://www.justice.gov/usao-sdny/pr/nigerian-man-extradited-united-kingdom-participating-business-email-compromise-scams
[5] https://apps.sfc.hk/edistributionWeb/api/circular/openFile?lang=EN&refNo=22EC25

cybersecurity practices of those targeted by BEC cybercriminals and how those at the top of the organizations can be the biggest weakness. The paper also created a threat intelligence term for BEC - "Financial Fraud Kill Chain" (FFKC), which was adopted and used by various financial institutions[6].

The IC3 Report disclosed that fraudsters have become more sophisticated, and the BEC/EAC scheme has continually evolved in covid pandemic. The IC3 has observed an emergence of newer BEC/EAC schemes that exploit this reliance on virtual meetings to instruct victims to send fraudulent wire transfers. The fraudster would insert a still picture of the CEO with no audio or a "deep fake" audio through which fraudsters, acting as business executives, would then claim their audio/video was not working correctly. "Based on the financial data reported to the IC3 for 2021, banks in Thailand and Hong Kong were the primary international destinations of fraudulent funds," the FBI said.


RAT Process[5]
Victim sends complaint to IC3
FBI
Internet Crime Complaint Center
Automated triage through FBI Internet Crime Database
IC3 Analyst *
Assigned to FBI Field Office for action
BANK
Financial Institution

* If criteria is met, transaction details are forwarded to the identified point of contact at the recipient bank to notify of fraudulent activity and request freezing of the account. Once response is received from the recipient bank, RAT contacts the appropriate FBI field office(s).

Automated triage and RAT Process adopted by FBI

[6] https://www.abais.com/blogs/detail/blog/2022/02/04/financial-fraud-kill-chain-may-prevent-wire-transfer-fraud

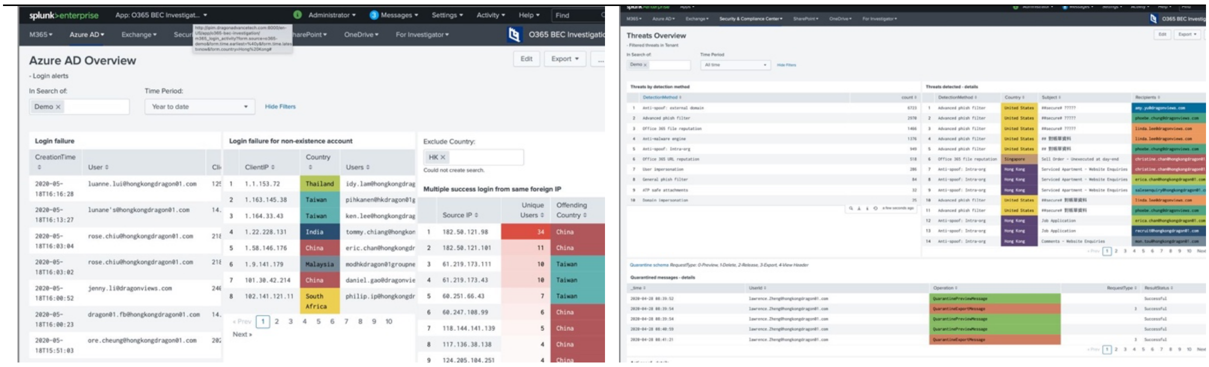
Why use Microsoft Sentinel?

Since 2018, we have started publishing cybersecurity alerts[7] and white papers[8] on BEC incidents in Hong Kong. In the past three years, we have handled several BEC/Phishing scam incidents from various clients, including a few international fund management firms. We believe this business segment is under targeted attacks because most of them do not have designated professionals handling the email security issue, and these firms handle a high frequency of wires or remittances to their business partners or investors all around the world.

In the past, most IR cases we handled were not using Microsoft Sentinel. We collected the Unified Audit Logs (UAL) from the victim tenants and used eDiscovery features to obtain the affected mailbox for our investigations. The detailed procedures on how we collect the forensic evidence were described in our latest paper – Microsoft 365 Forensics Playbook[9]. After obtaining the UAL, we performed the same procedures described in a BEC investigation guide by the PwC UK[10]. Instead of parsing the required UAL by the Search-UnifiedAuditLog cmdlet or using Office 365 Management API, we ingested the downloaded UAL into our O365 BEC Investigation Dashboards in speed up our investigation.

Azure AD Overview

Threat Overview



Azure AD Overview

- Login alerts

In Search of: Demo ×

Time Period: Year to date

Hide Filters

Login failure

CreationTime	User	Cli
2020-05-18T16:16:28	luanne.lui@hongkongdragon01.com	125
2020-05-18T16:13:27	lunane's@hongkongdragon01.com	14.
2020-05-18T16:03:04	rose.chiu@hongkongdragon01.com	218
2020-05-18T16:03:02	rose.chiu@hongkongdragon01.com	218
2020-05-18T16:00:52	jenny.li@dragonviews.com	246
2020-05-18T16:00:23	dragon01.fb@hongkongdragon01.com	14.
2020-05-18T15:51:03	ore.cheung@hongkongdragon01.com	202

Login failure for non-existence account

	ClientIP	Country	Users
1	1.1.153.72	Thailand	idy.lam@hongkongdrag
2	1.163.145.38	Taiwan	pihkanen@hkdragon01g
3	1.164.33.43	Taiwan	ken.lee@hongkongdrag
4	1.22.228.131	India	tommy.chiang@hongkon
5	1.58.146.176	China	eric.chan@hongkongdr
6	1.9.141.179	Malaysia	modhkdragon01groupne
7	101.30.42.214	China	daniel.gao@dragonvie
8	102.141.121.11	South Africa	philip.ip@hongkongdr

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Exclude Country: HK ×

Could not create search.

Multiple success login from same foreign IP

	Source IP	Unique Users	Offending Country
1	182.50.121.98	34	China
2	182.50.121.101	11	China
3	61.219.173.111	10	Taiwan
4	61.219.173.43	10	Taiwan
5	60.251.66.43	7	Taiwan
6	60.247.108.99	6	China
7	118.144.141.139	5	China
8	117.136.38.138	4	China
9	124.205.104.251	4	China

Threats Overview

- Filtered threats in Tenant

In Search of: Demo ×

Time Period: All time

Hide Filters

Threats by detection method

	DetectionMethod	count
1	Anti-spoof: external domain	6723
2	Advanced phish filter	2970
3	Office 365 file reputation	1466
4	Anti-malware engine	1376
5	Anti-spoof: Intra-org	949
6	Office 365 URL reputation	518
7	User impersonation	286
8	General phish filter	84
9	ATP safe attachments	32
10	Domain impersonation	25

Threats detected - details

	DetectionMethod	Country	Subject	Recipients
1	Advanced phish filter	United States	##secure# ?????	amy.yu@dragonviews.com
2	Advanced phish filter	United States	##secure# ?????	phoebe.chung@dragonviews.com
3	Advanced phish filter	United States	##secure# ?????	linda.lee@dragonviews.com
4	Advanced phish filter	United States	## 對帳單資料	linda.lee@dragonviews.com
5	Advanced phish filter	United States	## 對帳單資料	phoebe.chung@dragonviews.com
6	Office 365 file reputation	Singapore	Sell Order - Unexecuted at day-end	christine.chan@hongkongdragon01
7	Anti-spoof: Intra-org	Hong Kong	Serviced Apartment - Website Enquiries	christine.chan@hongkongdragon01
8	Anti-spoof: Intra-org	Hong Kong	Serviced Apartment - Website Enquiries	erica.chan@hongkongdragon01.com
9	Anti-spoof: Intra-org	Hong Kong	Serviced Apartment - Website Enquiries	salesenquiry@hongkongdragon01.c
10	Advanced phish filter	United States	##secure# 對帳單資料	linda.lee@dragonviews.com
11	Advanced phish filter	United States	##secure# 對帳單資料	phoebe.chung@dragonviews.com
12	Anti-spoof: Intra-org	Hong Kong	Job Application	erica.chan@hongkongdragon01.com
13	Anti-spoof: Intra-org	Hong Kong	Job Application	recruit@hongkongdragon01.com
14	Anti-spoof: Intra-org	Hong Kong	Comments - Website Enquiries	mon.tou@hongkongdragon01.com

« Prev 1 2 3 4 5 6 7 8 9 10 Next

Quarantine schema RequestType: 0-Preview, 1-Delete, 2-Release, 3-Export, 4-View Header

Quarantined messages - details

_time	UserId	Operation	RequestType	ResultStatus
2020-04-28 08:39:52	lawrence.Zheng@hongkongdragon01.com	QuarantinePreviewMessage		Successful
2020-04-28 08:39:54	lawrence.Zheng@hongkongdragon01.com	QuarantineExportMessage	3	Successful
2020-04-28 08:39:54	lawrence.Zheng@hongkongdragon01.com	QuarantinePreviewMessage		Successful
2020-04-28 08:40:59	lawrence.Zheng@hongkongdragon01.com	QuarantinePreviewMessage		Successful
2020-04-28 08:41:21	lawrence.Zheng@hongkongdragon01.com	QuarantineExportMessage	3	Successful

« Prev 1 2 3 4 5 6 7 8 9 10 Next

O365 BEC Investigation Dashboards

We ingest the UAL by using Office 365 Management API to keep monitoring our client's tenants' phishing landscape.

After we published our Sentinel use cases white paper, we started working on the possibility of collecting OfficeActivity and AAD SignInLogs instead of UAL for our near real-time monitoring of the threat landscape of our client's tenants.

[7] https://www.dragonadvancetech.com/reports/Business-Email-Compromise.pdf

[8] https://www.dragonadvancetech.com/reports/Security-White-Paper-on-BEC.pdf & https://www.dragonadvancetech.com/reports/O365-IR%20Playbook_v1.0.pdf

[9] https://dragonadvancetech.com/reports/M365%20Forensics%20Playbook_v3.pdf

[10] https://github.com/PwC-IR

Microsoft Sentinel Data Connectors

Subject to some prerequisites, the first data connector you should add is User and Entity Behavior Analytics (UEBA)[11]. Microsoft Sentinel will analyze the sign-in activities and the audit logs generated from the Azure Active Directory and builds a baseline for the UEBA-enabled tenant to identify anomalous activity to evaluate the potential impact of any given compromised asset.

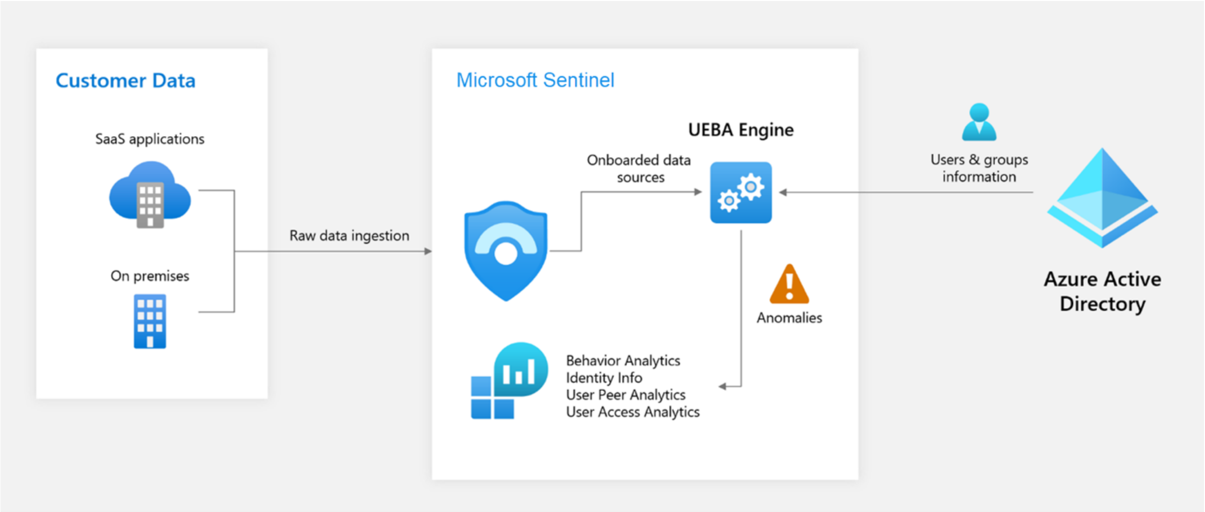
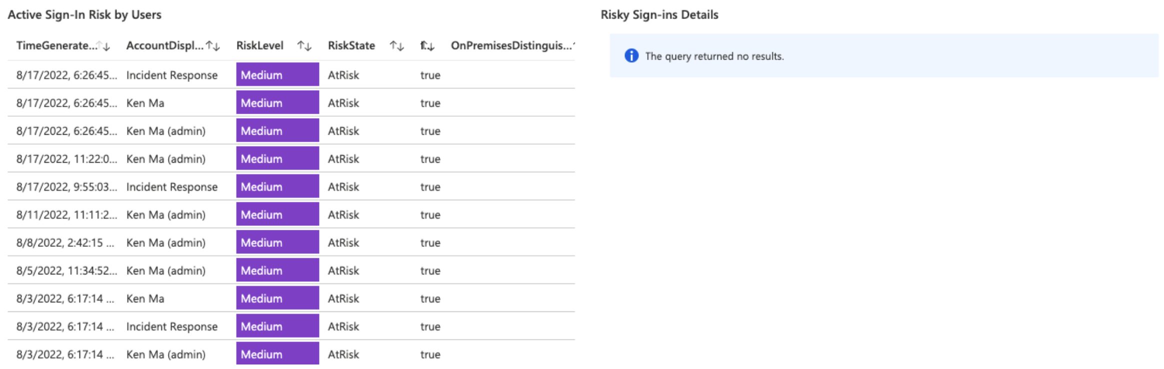


Figure extracted from Microsoft 365 documentation

After you set up the connection, Microsoft Sentinel will store the "non-billable" Azure Active Directory information in an internal database visible through the *IdentityInfo* table in Log Analytics. This table provides information of Risk Level (such as: Low, Medium, High, or None) and Risk State (such as: AtRisk, Remediated, or Dismissed) of the tenant users to the Sentinel. Combine with the "AI-enabled" (we guess) *AADUserRiskEvents* table, we can generate a highly valuable Workbook contents on users' Risk Detail (such as aiConfirmedSigninSafe, userPerformedSecuredPasswordReset, hidden, or none) and Risk Event Type (such as unfamiliarFeatures, unlikelyTravel, or generic) for further analysis.



Active Sign-In Risk by Users

TimeGenerate... ↑↓	AccountDispl... ↑↓	RiskLevel ↑↓	RiskState ↑↓	↑↓	OnPremisesDistinguis...
8/17/2022, 6:26:45...	Incident Response	Medium	AtRisk	true	
8/17/2022, 6:26:45...	Ken Ma	Medium	AtRisk	true	
8/17/2022, 6:26:45...	Ken Ma (admin)	Medium	AtRisk	true	
8/17/2022, 11:22:0...	Ken Ma (admin)	Medium	AtRisk	true	
8/17/2022, 9:55:03...	Incident Response	Medium	AtRisk	true	
8/11/2022, 11:11:2...	Ken Ma (admin)	Medium	AtRisk	true	
8/8/2022, 2:42:15 ...	Ken Ma (admin)	Medium	AtRisk	true	
8/5/2022, 11:34:52...	Ken Ma (admin)	Medium	AtRisk	true	
8/3/2022, 6:17:14 ...	Ken Ma	Medium	AtRisk	true	
8/3/2022, 6:17:14 ...	Incident Response	Medium	AtRisk	true	
8/3/2022, 6:17:14 ...	Ken Ma (admin)	Medium	AtRisk	true	

Risky Sign-ins Details

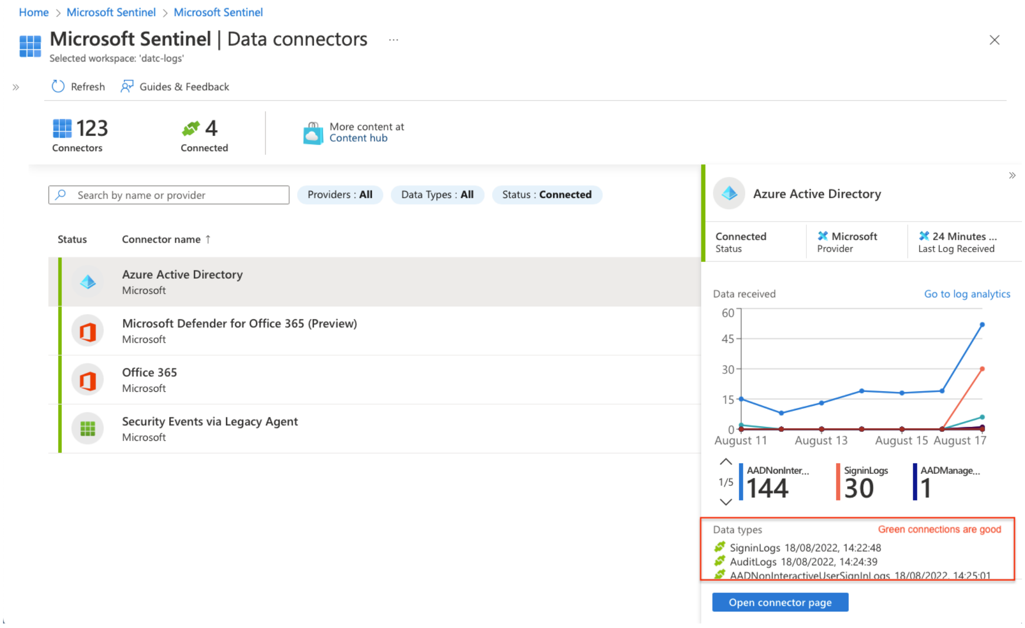
The query returned no results.

Figure extracted from Workbook of [DATC] – Azure AD > (User Identity Assessment)

[11] https://docs.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics

We assume normal community users only bought a few Office E3 licenses or Business Premium licenses, and we hope our use case can be applied for a large segment of entities in a budget (***non-billable***[12]) way, we only connect the following data sources to the Microsoft Sentinel (if you ingest Security Events from endpoint, you must at least buy a basic Sentinel subscription):

- Azure Active Directory (tables of: *SigninLogs, AuditLogs, AADNonInteractiveUserSignInLogs, AADUserRiskEvents*)
- Office 365 (tables of *OfficeActivity*)
- Optional: Microsoft 365 Defender (table of *SecurityIncident, SecurityAlert, EmailEvents, EmailUrlInfo, EmailAttachmentInfo, AlertEvidenc*e)



Microsoft Sentinel | Data connectors

Selected workspace: 'datc-logs'

123 Connectors

4 Connected

Providers : **All** Data Types : **All** Status : **Connected**

Status	Connector name ↑
	Azure Active Directory Microsoft
	Microsoft Defender for Office 365 (Preview) Microsoft
	Office 365 Microsoft
	Security Events via Legacy Agent Microsoft

Azure Active Directory

Connected	Microsoft	24 Minutes ...
Status	Provider	Last Log Received

Data received

AADNonInter...	SigninLogs	AADManage...
144	30	1

Data types

Green connections are good

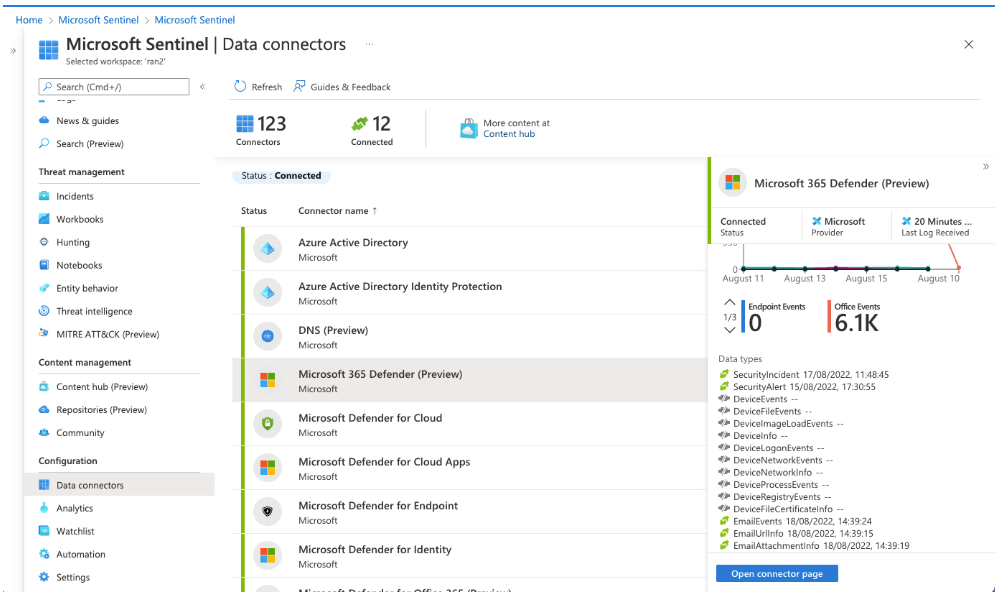
SigninLogs 18/08/2022, 14:22:48

AuditLogs 18/08/2022, 14:24:39

AADNonInteractiveUserSignInLogs 18/08/2022, 14:25:01

Figure extracted from Data connectors of DATC tenant, with only E3 licenses

[12] https://docs.microsoft.com/en-us/azure/sentinel/billing?tabs=commitment-tier



Status	Connector name ↑
	Azure Active Directory Microsoft
	Azure Active Directory Identity Protection Microsoft
	DNS (Preview) Microsoft
	Microsoft 365 Defender (Preview) Microsoft
	Microsoft Defender for Cloud Microsoft
	Microsoft Defender for Cloud Apps Microsoft
	Microsoft Defender for Endpoint Microsoft
	Microsoft Defender for Identity Microsoft

Microsoft 365 Defender (Preview)

Status	Provider	Last Log Received
Connected	Microsoft	20 Minutes ...

Endpoint Events 0

Office Events 6.1K

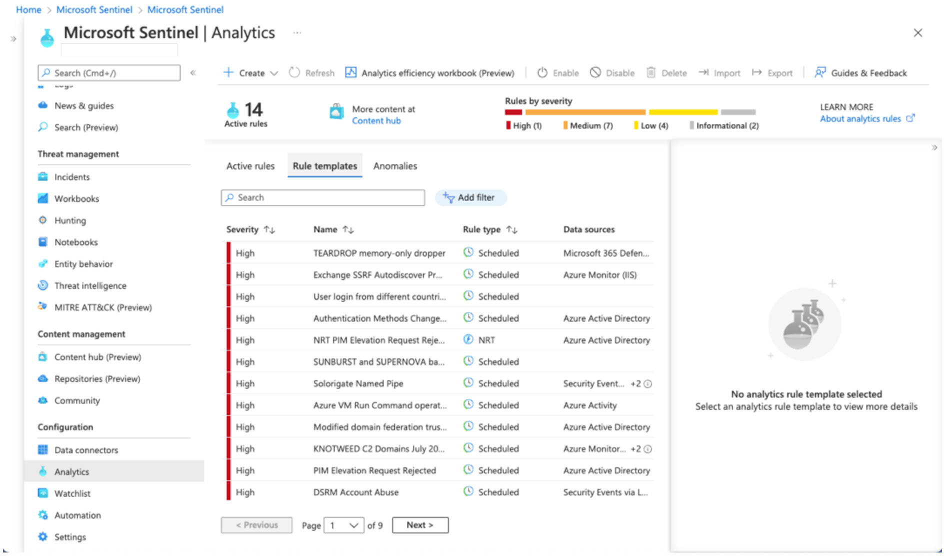
Data types

SecurityIncident 17/08/2022, 11:48:45
SecurityAlert 15/08/2022, 17:30:55
DeviceEvents --
DeviceFileEvents --
DeviceImageLoadEvents --
DeviceInfo --
DeviceLogonEvents --
DeviceNetworkEvents --
DeviceNetworkInfo --
DeviceProcessEvents --
DeviceRegistryEvents --
DeviceFileCertificateInfo --
EmailEvents 18/08/2022, 14:39:24
EmailUrlInfo 18/08/2022, 14:39:15
EmailAttachmentInfo 18/08/2022, 14:39:19

Figure extracted from Data connectors of DATC tenant, with E5 licenses

Microsoft Sentinel Analytics Rules

According to Microsoft documentation, after you've connected your data sources to Microsoft Sentinel, you'll want to be notified when something suspicious occurs. There are many out-of-the-box threat detection rules[13] and anomaly detection rules[14] that can be deployed and customized at your option.

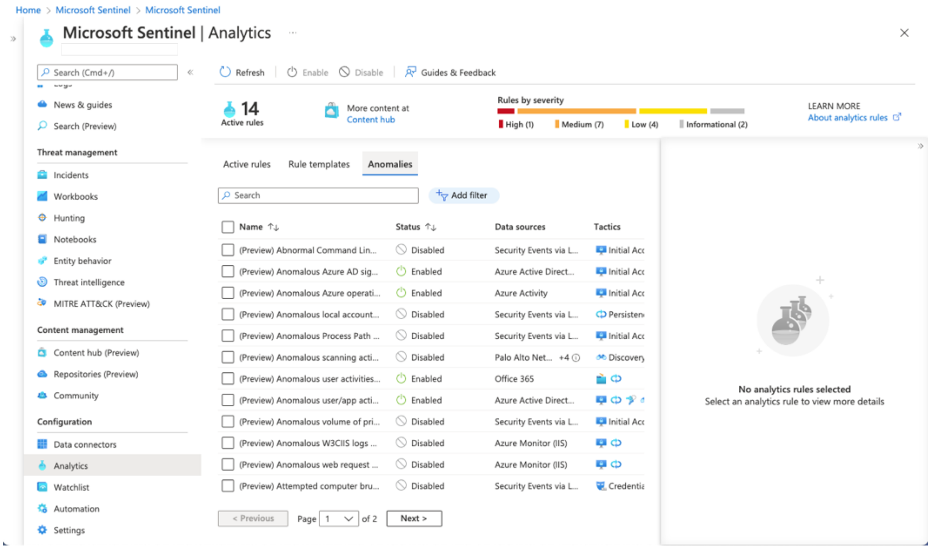


Severity ↑↓	Name ↑↓	Rule type ↑↓	Data sources
High	TEARDROP memory-only dropper	Scheduled	Microsoft 365 Defen...
High	Exchange SSRF Autodiscover Pr...	Scheduled	Azure Monitor (IIS)
High	User login from different countri...	Scheduled	
High	Authentication Methods Change...	Scheduled	Azure Active Directory
High	NRT PIM Elevation Request Reje...	NRT	Azure Active Directory
High	SUNBURST and SUPERNOVA ba...	Scheduled	
High	Solorigate Named Pipe	Scheduled	Security Event... +2
High	Azure VM Run Command operat...	Scheduled	Azure Activity
High	Modified domain federation trus...	Scheduled	Azure Active Directory
High	KNOTWEED C2 Domains July 20...	Scheduled	Azure Monitor... +2
High	PIM Elevation Request Rejected	Scheduled	Azure Active Directory
High	DSRM Account Abuse	Scheduled	Security Events via L...

Figure extracted from Rule templates

[13] https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-built-in

[14] https://docs.microsoft.com/en-us/azure/sentinel/work-with-anomaly-rules



Name	Status	Data sources	Tactics
(Preview) Abnormal Command Lin...	Disabled	Security Events via L...	Initial Acc
(Preview) Anomalous Azure AD sig...	Enabled	Azure Active Direct...	Initial Acc
(Preview) Anomalous Azure operati...	Enabled	Azure Activity	Initial Acc
(Preview) Anomalous local account...	Disabled	Security Events via L...	Persisten
(Preview) Anomalous Process Path ...	Disabled	Security Events via L...	Initial Acc
(Preview) Anomalous scanning acti...	Disabled	Palo Alto Net... +4	Discovery
(Preview) Anomalous user activities...	Enabled	Office 365	
(Preview) Anomalous user/app acti...	Enabled	Azure Active Direct...	
(Preview) Anomalous volume of pri...	Disabled	Security Events via L...	Initial Acc
(Preview) Anomalous W3CIIS logs ...	Disabled	Azure Monitor (IIS)	
(Preview) Anomalous web request ...	Disabled	Azure Monitor (IIS)	
(Preview) Attempted computer bru...	Disabled	Security Events via L...	Credentia

Figure extracted from Anomalies Rules

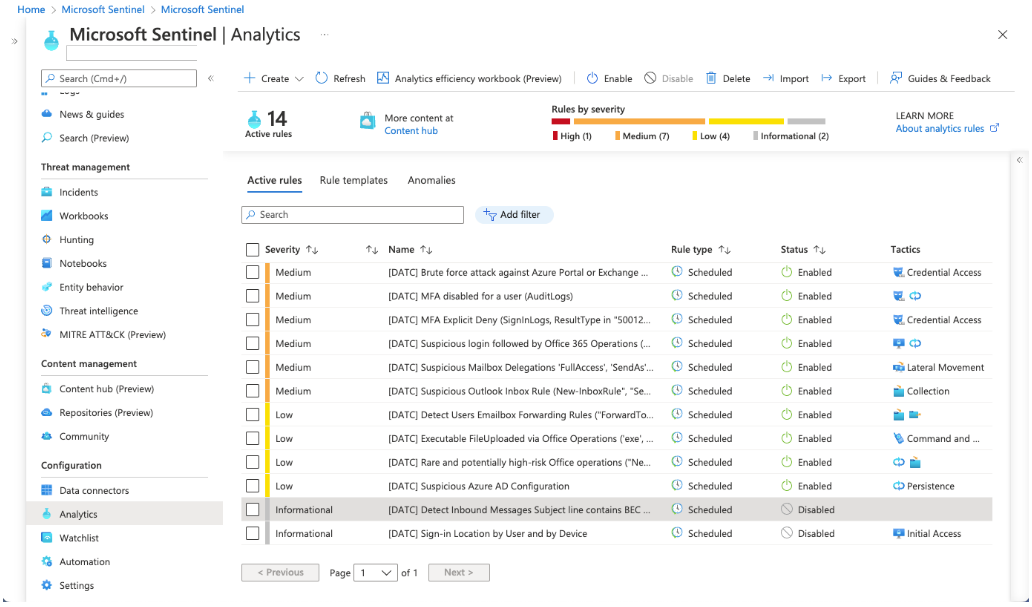
Most rules are significant and valuable for a full scale implementation which can generate detection alerts when a suspicious event occurs. However, we found most of them are not helpful for our target tenant users because of the following reasons:

- The rules only work for the suitable data sources, but the tenant only ingests a few
- The rules generate many alerts that a traditional IT Help Desk does not understand
- Under the Rule templates, there are many rules designed to detect a unique threat
- Some Anomalies Rules easy to generate false positive alerts
- Some schedule rules provide insight for a particular data source but can be modified to generate meaningful alerts when applied to another ingested data source

In our opinion, all Rule templates or Anomalies Rules are good but not always suitable for Sentinel users in the early deployment stage. We recommend that new Sentinel users carefully select the appropriate rules for their use, try to deploy a few first then add later. Select the rules that you have already ingested the right data sources. Or otherwise, you see nothing from the deployed rules. Tune the Severity of the rules to your needs and make sure the scheduled tasks are configured to run at the right frequency at your tenant's requirements (running the schedule rules will cost you more and will generate more alerts if not properly configured – aka alert fatigue).

Because this use case is designed to detect and generate alerts on suspicious BEC or Phishing activities, we modified some of the rules provided by the content hub. We added a few to ourselves to our tenant. We carefully configured the schedule frequency and modified the rule names with a few addon notes so that anyone on our team knows what it means without the need to check the KQL query when handling an alert. Some detection alerts should be reclassified to a combination of more medium and less High and Informational for prioritization.

We prefer not to provide detailed explanations of why and how we create these rules. Please feel free to study and modify our rules for your use. You can find our rules at https://github.com/DATCResearch/Sentinel-UseCase-BEC365-IR.



Severity	Name	Rule type	Status	Tactics
Medium	[DATC] Brute force attack against Azure Portal or Exchange ...	Scheduled	Enabled	Credential Access
Medium	[DATC] MFA disabled for a user (AuditLogs)	Scheduled	Enabled	
Medium	[DATC] MFA Explicit Deny (SignInLogs, ResultType in "50012...	Scheduled	Enabled	Credential Access
Medium	[DATC] Suspicious login followed by Office 365 Operations (...	Scheduled	Enabled	
Medium	[DATC] Suspicious Mailbox Delegations 'FullAccess', 'SendAs'...	Scheduled	Enabled	Lateral Movement
Medium	[DATC] Suspicious Outlook Inbox Rule (New-InboxRule", "Se...	Scheduled	Enabled	Collection
Low	[DATC] Detect Users Emailbox Forwarding Rules ("ForwardTo...	Scheduled	Enabled	
Low	[DATC] Executable FileUploaded via Office Operations ('exe', ...	Scheduled	Enabled	Command and ...
Low	[DATC] Rare and potentially high-risk Office operations ("Ne...	Scheduled	Enabled	
Low	[DATC] Suspicious Azure AD Configuration	Scheduled	Enabled	Persistence
Informational	[DATC] Detect Inbound Messages Subject line contains BEC ...	Scheduled	Disabled	
Informational	[DATC] Sign-in Location by User and by Device	Scheduled	Disabled	Initial Access

Figure extracted from our designed 14-Rules for Phishing/BEC detections

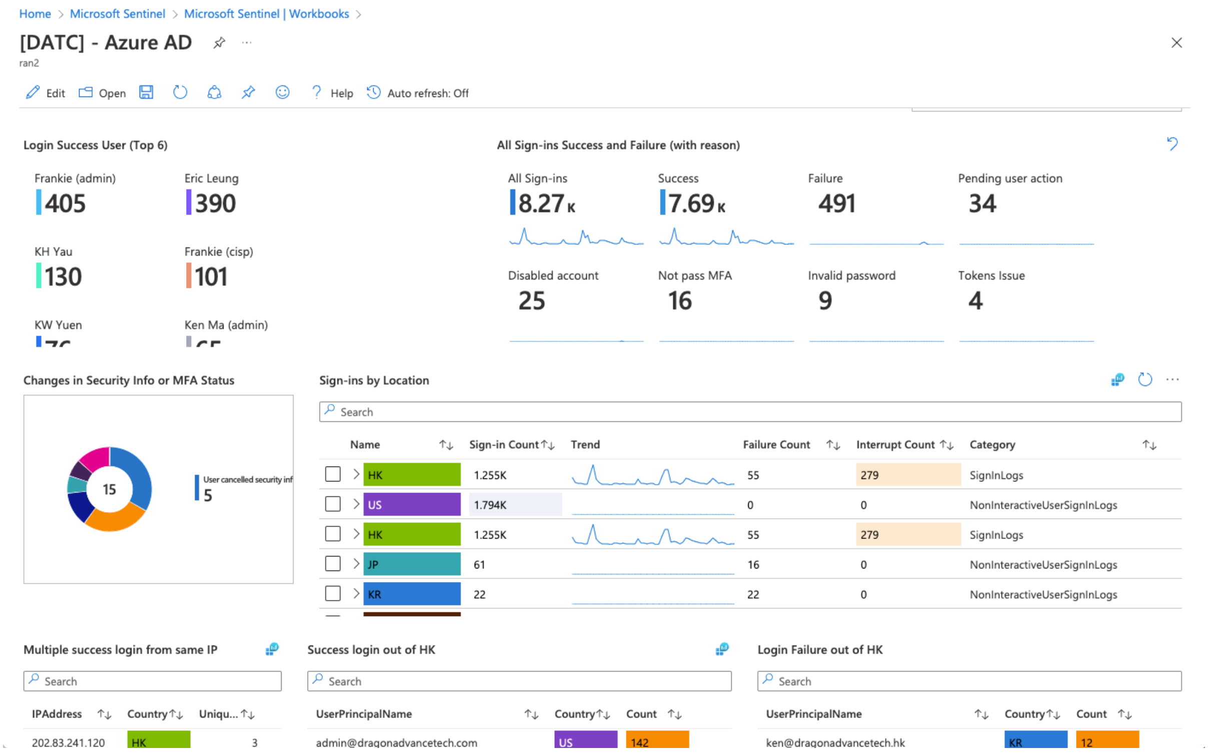
Microsoft Sentinel Workbooks

After connecting the data sources to Microsoft Sentinel, you can visualize and monitor the data with Microsoft Sentinel Workbooks. At first, we treat the Workbooks the same as Dashboards. However, we believe that if we can have a better design of the Workbooks, we can use Workbooks as interactive tools to help investigate incidents or alerts.

Same as the analytic rules template, Microsoft Sentinel provided a content hub to allow users to download for use. We spent a great deal of time modifying and developing our Workbooks to help our team to detect, monitor, mitigate, and contain incidents in BEC and phishing attacks.

We designed two Workbooks as a demo for community users. If MSP, especially for those who are in my region, wants to use our Workbooks for commercial use, please notify us ir@dragonadvancetech.com.

We prefer not the provide detailed explanations of why and how we create these Workbooks. However, we screen shots some parts of the Workbooks, which are attached in the appendix as a reference. We also keep copies of our full workbooks in pdf format at https://github.com/DATCResearch/Sentinel-UseCase-BEC365-IR. Please feel free to study and modify our Workbooks for your.


Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >
Edit
Open
Help
Auto refresh: Off
Search

[DATC] - Azure AD

ran2

Login Success User (Top 6)

Frankie (admin) 405	Eric Leung 390
KH Yau 130	Frankie (cisp) 101
KW Yuen 76	Ken Ma (admin) 65

All Sign-ins Success and Failure (with reason)

All Sign-ins 8.27K	Success 7.69K	Failure 491	Pending user action 34
Disabled account 25	Not pass MFA 16	Invalid password 9	Tokens Issue 4

Changes in Security Info or MFA Status

15
User cancelled security inf
5

Sign-ins by Location

Name	Sign-in Count	Trend	Failure Count	Interrupt Count	Category
HK	1.255K		55	279	SignInLogs
US	1.794K		0	0	NonInteractiveUserSignInLogs
HK	1.255K		55	279	SignInLogs
JP	61		16	0	NonInteractiveUserSignInLogs
KR	22		22	0	NonInteractiveUserSignInLogs

Multiple success login from same IP

IPAddress	Country	Uniqu...
202.83.241.120	HK	3

Success login out of HK

UserPrincipalName	Country	Count
admin@dragonadvancetech.com	US	142

Login Failure out of HK

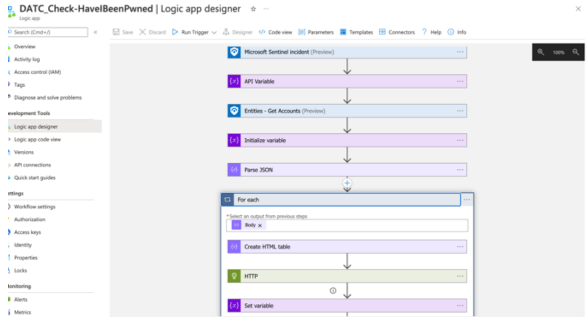
UserPrincipalName	Country	Count
ken@dragonadvancetech.hk	KR	12

Figure extracted AAD – Overview Workbook

Microsoft Sentinel Logic Apps

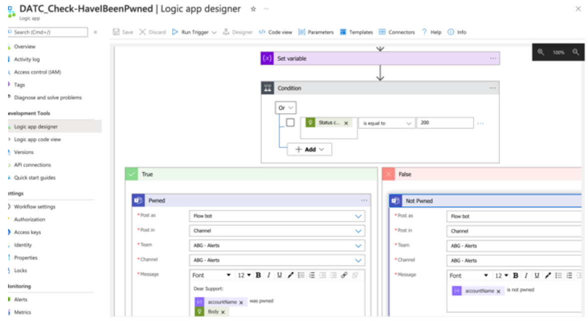
The rules can be configured to generate alerts and incidents to the Sentinel, and it is great to have the SOAR function to automate some standardized incident response processes. The Playbook features provide a great option when handling the enrichment, mitigation, eradiation, and response functions in an ideal way.

However, we hope our use case be used in a budget way. Therefore, we only implemented two incident trigger Automation Playbooks as an example. We believe you can depooy them easily by clicking the “Deploy to Azure” button.



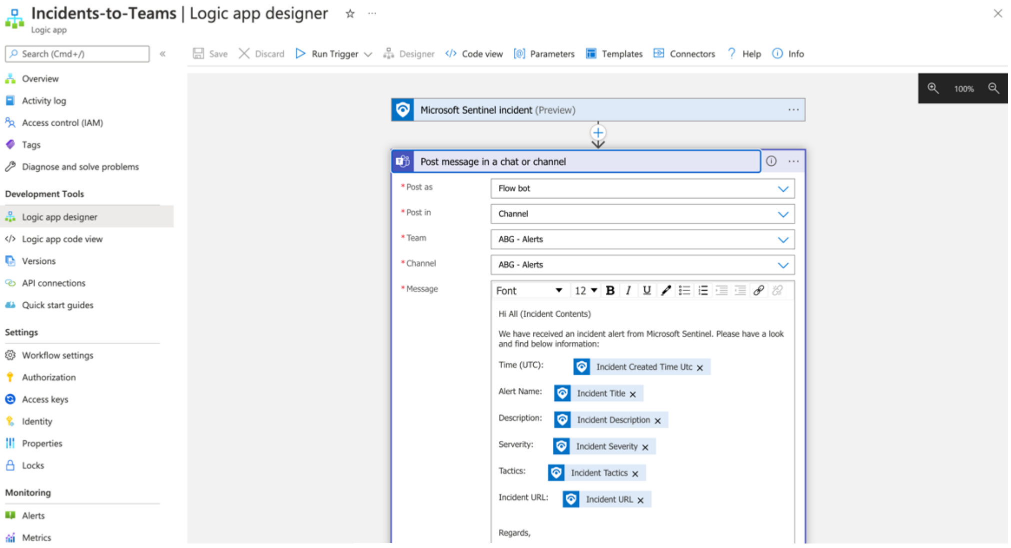
Microsoft Sentinel incident (Preview)
API Variable
Entities - Get Accounts (Preview)
Initialize variable
Parse JSON
For each
*Select an output from previous steps: Body
Create HTML table
HTTP
Set variable

HaveIBeenPwned-1



Set variable
Condition
Or
Status c... is equal to 200
Add
True
Pwned
*Post as: Flow bot
*Post in: Channel
*Team: ABG - Alerts
*Channel: ABG - Alerts
*Message: Font 12
Dear Support:
accountName was pwned
Body
False
Not Pwned
*Post as: Flow bot
*Post in: Channel
*Team: ABG - Alerts
*Channel: ABG - Alerts
*Message: Font 12
accountName is not pwned

HaveIBeenPwned-2



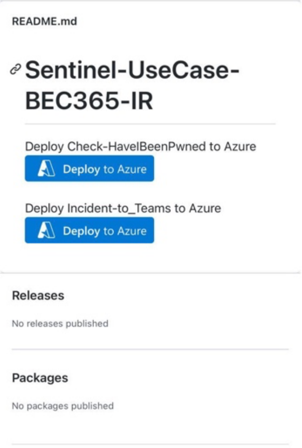
Microsoft Sentinel incident (Preview)
Post message in a chat or channel
*Post as: Flow bot
*Post in: Channel
*Team: ABG - Alerts
*Channel: ABG - Alerts
*Message: Font 12

Hi All (Incident Contents)

We have received an incident alert from Microsoft Sentinel. Please have a look and find below information:

Time (UTC): Incident Created Time Utc
Alert Name: Incident Title
Description: Incident Description
Serverity: Incident Severity
Tactics: Incident Tactics
Incident URL: Incident URL

Regards,


README.md

Sentinel-UseCase-BEC365-IR

Deploy Check-HaveIBeenPwned to Azure

Deploy to Azure

Deploy Incident-to_Teams to Azure

Deploy to Azure

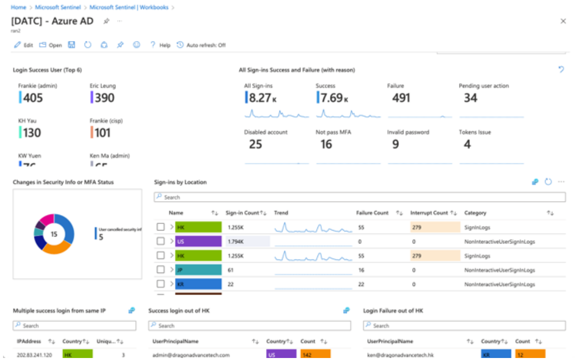
Releases

No releases published

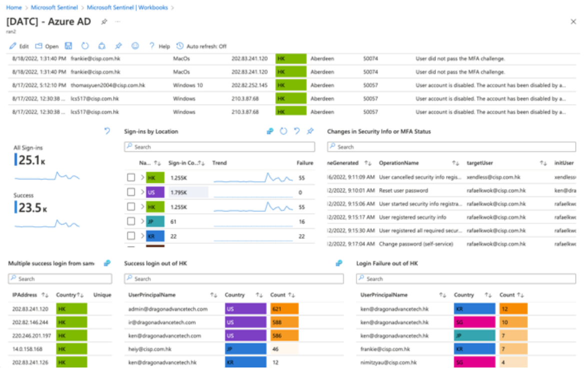
Packages

No packages published

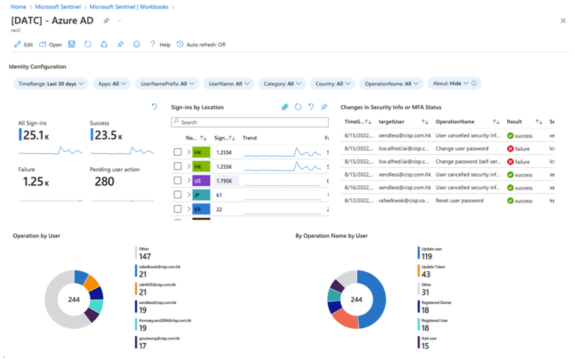
Appendix I: Workbooks


Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >
[DATC] - Azure AD
Login Success User (Top 6)
All Sign-ins Success and Failure (with reason)
Changes in Security Info or MFA Status
Sign-ins by Location
Multiple success login from same IP
Success login out of HK
Login Failure out of HK

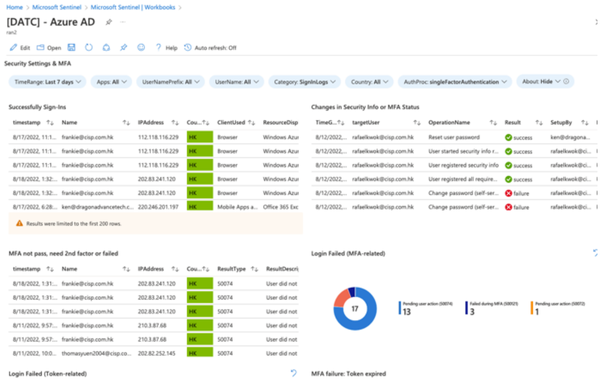
AAD - Overview


Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >
[DATC] - Azure AD
Sign-ins by Location
Changes in Security Info or MFA Status
Multiple success login from same
Success login out of HK
Login Failure out of HK

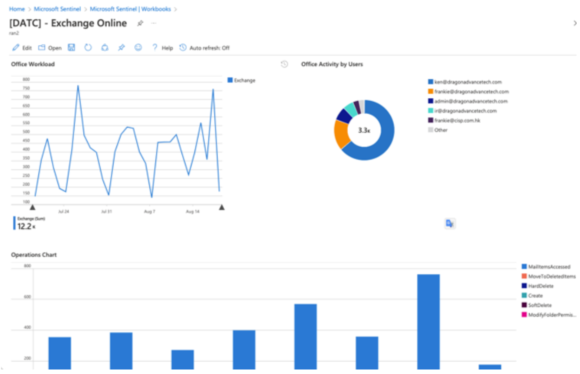
AAD – User Identity Assessment


Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >
[DATC] - Azure AD
Identity Configuration
Sign-ins by Location
Changes in Security Info or MFA Status
Operation by User
By Operation Name by User

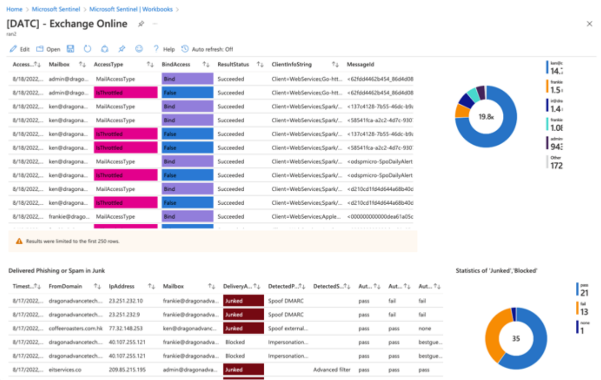
AAD – Identify Configuration


Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >
[DATC] - Azure AD
Security Settings & MFA
Successfully Sign-ins
Changes in Security Info or MFA Status
MFA not pass, need 2nd factor or failed
Login Failed (MFA-related)
Login Failed (Token-related)
MFA failure: Token expired

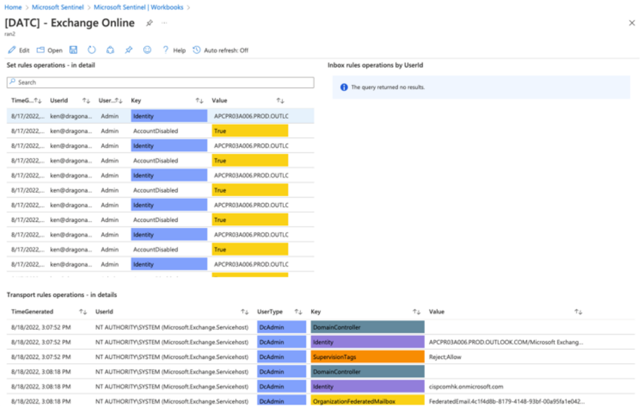
AAD – MFA Status



EXO - Overview


Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >
[DATC] - Exchange Online
Delivered Phishing or Spam in Junk
Statistics of 'Junked','Blocked'

EXO – Mailbox Activities


Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >
[DATC] - Exchange Online
Set rules operations - in detail
Inbox rules operations by UserId
The query returned no results.
Transport rules operations - in details

EXO – Mailbox Suspicious Activities

Appendix II: Services Offered

Sample organization, 50-2500 employees		
Resource type/Function	**Key tasks**	**Benchmark duration (days)**
Project manager	• Planning • Stakeholder engagement • Resource planning • Project management	
Security architect	• Data ingestion strategy • RBAC controls • Access control • Log source to be ingested • Use case development • Identify gaps with MITRE ATT&CK log source	
Azure Cloud engineer	• Managing permission/RBAC in Azure tenant • Provision Azure resources • Configure Azure AD service accounts • Configure Azure AD groups and membership	
Engineering system owner	• Configuring log forwarding on assets • IT sysadmin: deploying monitoring agents • Deploy on-perm Azure Sentinel log collector • Provide expertise on application logging by mapping to critical assets • Configuring application logging • Assist n validation of alert rules and SOAR playbooks	
SIEM engineering	• Developing custom KQL detection rules • Developing custom workbooks for data visualization • Creating Azure function for data parsing • Creating playbooks for IR automation	
Security operations	• Documentation of detection use cases and detection rules	

	• Documentation of detection parameters and threat intelligence sources	
MDR for Endpoint	• Gain threat context: Our threat intelligence enriches alerts to inform decision making • 24x7 coverage • Hunting for stealthy threat for mapping into MITRE ATT&CK® framework • Advices on contain impacted hosts • Rapid Response: Our experts quickly assess and contain threats, helping you resolve incidents without the added cost of full incident response • Effective remediation: We perform rapid investigation and remediation based on the collective knowledge of our experts • Elevate your defenses: Improve your security posture with ongoing assessment and • real-world strategies	
MDR for Office 365 Activity	• Monitor and alert against security threats • Monitor business data against leaks • Know what is happening in organization’s Office 365 • Build on Azure Cloud Services, Office 365 Activity Security Monitoring is a managed security service using the power of Azure Sentinel platform and benefits of Azure Logic Apps • Fast delivery • 7x24 coverage • On-site incident response service package	
Azure Sentinel MSSP Service	• Fast delivery • 7x24 coverage • Deployment and configuration of Azure Sentinel SIEM in customer	

	Azure subscription and activation of the Office 365 Data Connector. Our team will assist customer to enable auditing in Office 365 • Configuration of more than 25 alert rules related to Office 365 data source for monitoring activities to Sharepoint Online, Exchange Online and OneDrive • SIEM support during security incidents: Managed Sentinel has extensive hands-on experience managing complex security breaches and will support the customer during security incidents with analytics, threat hunting and custom reporting. • Teams and DLP Security Monitoring: Configure a custom API function to extract events related to these workloads and publish it into Azure Sentinel Log Analytics. Additional alert rules will be configured for these events. • Continuous Use Case Tuning: The most valuable component of a managed SIEM service consists in the continuous alerts and playbooks tune-up in order to stay aligned with the current threat landscape. Managed Sentinel has over 20 years of experience in cybersecurity monitoring. • Embedded Threat Intelligence: Our proprietary machine learning algorithm and dark web discovery are leveraged to enrich the collected data and expedite cybersecurity investigations. • Regular Service Review: Managed Sentinel SOC team meets regularly the customer to review and collect feedback and new requirements on alerts, playbooks and workbooks.	

	○ Note 1: This service will run in customer Azure subscription ○ Note 2: This service is restricted to Office Activity events only	
Azure Sentinel SIEM Managed Service (Full SOC)	• Azure Sentinel MSSP Services as described above, plus: • Develop practical use cases according to your unique IT infrastructure • Our Tier-2 & Tier-3 advisors with experience and skills and using our threat intelligence feeds and risk & threat modelling to provide assurance to prevent modern threats and prioritise cyber threats to your business and work with you to prevent those threats becoming a reality. • We address your issues business face the most: ○ Ever-evolving threats, offensive techniques and technologies ○ Constant firefighting, point solutions and incident response overheads ○ Corporate reputation, brand protection, “insider threat” and regulatory compliance ○ Perimeter-less networks, cloud and SaaS solutions combined with employee mobility ○ Budget constraints, difficulty in recruitment and retaining skilled resource • Unique SOC service plan with unique SLA will be provided after consultation	