Sentinel Alert Types and Triage Methods

List of Microsoft Sentinel alerts generated by EPA Microsoft Sentinel From `1/6/2023 - 31/08/2023

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
Okta Signin Burst From Multiple Geo Locations within 12 Hours	150		1. Check locations of signins. 2. Check account involved in the alert. 3. In AAD, check sign in logs of the user/account and under "Device Info" see if the signins are from compliant or non compliant device. Capture IP addresses involved. 4. Check against EPA's Internal IP range if IP addresses belongs to EPA or not(There should be a list of IP address provided to SOC Team). If Yes, check with the user if it was a legitimate activity. 5. If answer to 4 is "No", discuss with Onshore team and get the password for that user/account changed.
User Login from Different Countries within 3 hours	108		1. In AAD, check if user is internal. 2. In AAD, check sign in logs of the user/account and under "Device Info"see if the signins are from compliant or non compliant device. Capture IP addresses involved. 3. Check with Onshore Team if the IP addresses belongs to EPA or not. If Yes, check with the user if it was a legitimate activity. Also check if the user has used VPN 4. If answer to 4 is "No", discuss with Onshore team and get the password for that user/account changed.
User added to Azure Active Directory Privileged Groups	108		1. Check which account performed the action and in AAD under assigned roles, check if role of the user if its Administrator. 2. Review audit log of account activity by checking the time of the alert in AAD to see if activity is legit or suspicious and if any reason behind the action is provided (Generally Servicenow ticket/Reason for PIM activation is mentioned). 3. Also match this activity timestamp with the AAD sign-in logs for the user to check IP used and sign-in status of the user looks non-suspicious. 4. If the activity looks suspicious validate with the user and revert the priviledges assigned.

TI Map IP Entity to SigninLogs	97	For IP blacklist checking:
		https://www.virustotal.com/gui/home/search
		https://mxtoolbox.com/
		https://www.abuseipdb.com/
		https://www.ipvoid.com/ip-blacklist-check/
		
		URL/Domains:
		
		https://mxtoolbox.com/
		https://www.virustotal.com/gui/home/url
		https://urlscan.io/
		https://www.urlvoid.com/
		
		==========
		KQL Queries
		
		CommonSecurityLog
		| where DeviceVendor == "Zscaler"
		//please use IP address in place of x.x.x.x
		| where * has "x.x.x.x"
		
		AzureDiagnostics
		//please use IP address in place of x.x.x.x
		| where * has "x.x.x.x"
			1. Gather all entities mentioned in the alert. Try to find out host associated with the IP by checking Signin logs, Deviceinfo Table and check for device details. If IP is a gateway/proxy, identify real IP/host that initiated connection. Use below queries to check logs.
			
			SigninLogs
			//put the source IP address between""
			| where * has ""
			
			DeviceInfo
			//put the source IP address between""
			| where * has ""
			
			2. Check the External/malicious IP (towards/from which connections are detected) in multiple online Reputation tools and find,
			
			All details of this IP
			Reputation of this IP is clean or categorized as malicious (score).
			No. of websites hosted by this IP
			IP Reputation details updated date Vs Alert date
			
			For IP blacklist checking:
			https://www.virustotal.com/gui/home/search
			https://mxtoolbox.com/
			https://www.abuseipdb.com/
			https://www.ipvoid.com/ip-blacklist-check/
			
			3. Search past 24 hr FW logs from source and Destination IP and check,
			
			Requested connection Type
			Connection observed on which port
			Frequency of those request
			Firewall action(Accept/block)
			No. of return traffic and ports
			
			KQL Queries
			
			CommonSecurityLog
			| where DeviceVendor == "Zscaler"
			//please use IP address in place of x.x.x.x
			| where * has "x.x.x.x"
			
			AzureDiagnostics
			//please use IP address in place of x.x.x.x
			| where * has "x.x.x.x"

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			4. If the connection is http/https, check past 24 hr proxy logs based on source IP and search for requested URL if present. If requested URL is observed, then check its reputation in online tools. Also verify the http response code. If 200 please check all the connections to verify if any upload is happening by verifying sent and received data. If yes and the IP/URL is found malicious please ask Onshore team/EPD Secops team to block IP address by updating the IP/URL detials in SNOW ticket. 5. Check if there is any reverse traffic detected from malicious IP towards internal IPs in past 30 days. Use the queries provided and search with the internal IP to check for any suspicious communication to malicious url/IP. Use tools provided in the list to get the details of IP/Urls. URL/Domain checking tools: https://mxtoolbox.com/ https://www.virustotal.com/gui/home/url https://urlscan.io/ https://www.urlvoid.com/ 6. Check past 12hr windows logs based on source IP to find source user/account associated with this activity. Use below query to get the windows security events. SecurityEvent //put the source IP address between "" | where IpAddress contains "" 7. Check with the respective team for AV status of internal IP/Host reported in the Alert.
A potentially malicious web request was executed against a web server	90		Check IP location and reputation in Abusedb/Cisco Talos Reputation Center to check if IP is flagged as malicious. (https://www.abuseipdb.com) Check the Azure Diagnostics (sentinel logs) by running KQL query selecting the "Time range" matching with alert timeline, to find out outcome of the malicious web requests made by the IP flagged in the alert. AzureDiagnostics | search "IP" | summarize count()by TimeGenerated, Message, requestUri_s, httpMethod_s, httpStatus_d, client_ip_s, host_s, ResourceGroup, WAFMode_s, serverStatus_s, action_s, details_message_s Check targeted resource groups, requested uri, web request methods (Put,Post,Get,Delete) used and header to see if any malicious activity has been observed or not, if observed Notify the team to take necessary actions. Check the Http status codes for the requests in the logs. If the http status codes are 300s or 400s or 500s, then the confidured WAF has detected/matched/blocked the web requests coming out of that IP. If the requests were blocked close the alert as True positive (If IP is malicious) or False Positive (If IP is not malicous). If the Http status codes is 200 success codes, then need to investigate further about which host is affected, if any sign-ins, inbound/outbound traffic is seen coming out of that malicious IP and for how long. If activity is determined malicious, escalate to L2/L3 Security Analyst. Get the IP blocked by adding them in NSG and update malicousIPWatchlist by adding the malicous IP flagged in the alert.
Detect files shared externally	76		1. Check Defender for Cloud Apps for further details. 2. Check what file and domain the file is shared to. Find out the role/department of the user sharing the file to understand if its valid activity for him and if file has any sensitive data. 3.Under Files page, filter out the file involved in alert & check the collaborator details under collaborator column if internal/external members or private (only owner has access). 4. If its private, internal or no collaborator, then close the alert as false positive. 5. Add to exception list in MCAS policy if activity is found to be legitimate. 6. Confirm with user if activity is suspicious.
Failed login attempts to Azure Portal	74		1 Check AAD (Azure Active Directory) sign-in logs, select the Date matching with alert timeline to see where sign-ins are from and if they are successful/failed sign-in attempts. You can use the filters in sign-in logs like "application as azure portal" & "status as failed/interrupted/success" to view different sign-in patterns. 2 Check IP of sign-in attempts to see if malicious (https://www.abuseipdb.com) 3 Check the sign-in pattern details like IP/Geo-location, device used (compliant/non-compliant), Conditional Access Policy Status and Failure reason to understand if its malicious attempts. 4 If the activity looks non-suspicious like sign-in if from expected location or using compliant device or with successful conditional access policy (MFA). And the sign-in pattern looks like user was interrupted to put MFA due to conditional access policy configured and user was later able to sign-in with successful MFA.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			Then can close the alert as benign positive. 5 If the activity is confirmed as malicious then add that IP in IOC (Indicator of Compromise) list. Reset user password if sign-in was successful to any account and close ticket as true positive. (Escalate to L2/L3 for actioning these)
File shared with unauthorized domain	72		1. Check what file and domain the file is shared to. Find out the role/department of the user sharing the file to understand if its valid activity for him and if file has any sensitive data. Check for the domain reputation. 2. Check "MS Defender for Cloud Apps" for further details. a. Login to MS 365 Defender portal. b. Under Cloud Apps, go to Files, search file name and all the detials available for the file will be displayed. Check for collaborator. 3. Check the collaborator details if internal/external members or private (only owner has access). If the domain is other than epa.vic.gov.au treat the collaborator as external if not treat the collaborator as internal. 4. If its private, internal or no collaborator, then close the alert as false positive. 5. Add to exception list in MCAS policy if activity is found to be legitimate. 6. Confirm with user if activity is suspicious. If the File owner/user is not aware of the activity please remove the sharing of the file with the unauthorised domain.
More than 10 failed Okta login attempts In 12hrs	68		1. Collect the user name and Verify the login attempts using Okta_CL and AD logs. Use Below queries to check the login details: Okta_CL //put the source IP address between"" | where * has "" SigninLogs //put the source IP address between"" | where * has "" 2. Check the reason for failure. 3. Check the status of the Source IP and past history to verify the IP being used. For IP blacklist checking: https://www.virustotal.com/gui/home/search https://mxtoolbox.com/ https://www.abuseipdb.com/ https://www.ipvoid.com/ip-blacklist-check/ 4. Please check if there was any password change request made during the failure attempts. Use below query to collect audit logs and check for any password change attempts: AuditLogs //put the source IP address between"" | where * contains "" 5. Check the device user is using for login is same or different devices are being used.Use below queries to check logs. SigninLogs //put the source IP address between"" | where * has "" 6. Check for user account status in AD. Connect with onshore team to get the user account detials from AD. 7. If there are any successfull events, please verify if there was any change prior to that. Please check with Username in SNOW for checking any change request or any request ticket raised for/by the user 8. If no suspicious activity is observed alert can be treated as BP. 9. If user activity seems suspicious please engage onshore team to confirm the activity with user.
User agent search for log4j exploitation attempt	54		1 Check IP location and reputation in Abusedb/Cisco Talos Reputation Center to check if IP is flagged as malicious. (https://www.abuseipdb.com) 2 Check the Azure Diagnostics (sentinel logs) by running KQL query selecting the "Time range" matching with alert timeline, to find out outcome of the malicious web requests made by the IP flagged in the alert. AzureDiagnostics | search "IP" | summarize count()by TimeGenerated, Message, requestUri_s, httpMethod_s, httpStatus_d, client_ip_s, host_s, ResourceGroup, WAFMode_s, serverStatus_s, action_s, details_message_s, originalHost_s 3 Check targeted resource groups, requested uri, web request methods (Put,Post,Get,Delete) used and header to see if any malicious activity has been observed or not, if observed Notify the team to take necessary actions.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			4 Check the Http status codes for the requests in the logs. If the http status codes are 300s or 400s or 500s, then the confidured WAF has detected/matched/blocked the web requests coming out of that IP. If the requests were blocked close the alert as True positive (If IP is malicious) or False Positive (If IP is not malicous). 5 If the Http status codes is 200 success codes, then need to investigate further about which host is affected, if any sign-ins, inbound/outbound traffic is seen coming out of that malicious IP and for how long. 6 If activity is determined malicious, escalate to L2/L3 Security Analyst. Get the IP blocked by adding them in NSG and update malicousIPWatchlist by adding the malicous IP flagged in the alert.
Shared digital certificates (file extensions)	53		1. Check for the file which has been shared and with whom the file has been shared. 2. If the file is shared internally please verify with user if the user is expected to share the file or not. Please engage onshore team to check with end user to verify the same. 3. If the file is shared with external domain, please verify the status of the domain and if blacklisted, please engage onshore team to block the url/domain. please use the tools provided for checking the blacklist status of domain/url. URL/Domain checking tools: https://mxtoolbox.com/ https://www.virustotal.com/gui/home/url https://urlscan.io/ https://www.urlvoid.com/ 4. Check for any other communication to/from the domain to which file has been shared. 5. Check for cretificate which was being sent, if the certificate is extecpected to be shared treat the alert as BP. 6. If not please check with user to confirm the activity. Please engage onshore team to check with end user to verify the same.
Rare and potentially high-risk Office operations	51		1 Check the Azure Active Directory (AAD) audit logs around time of activity to check details about the office operations performed by the user. 2 Look for the operation name, user's role, IP reputation and sign-in location with conditional access policy status to understand if this is legitimate behavior done by expected user like Administrator. 3 If the performed activities have been identified as expected BAU behavior and no other suspicious activity seen, then close the alert as Benign Positive. 4 If user or its activity looks suspicious, then confirm with the user about it and if they are not aware of it then escalate it to team to block the account, take necessary actions and close the ticket as True positive.
Anomalous behavior of discovered IP addresses	48	OfficeActivity | where Operation == "FileDownloaded" or Operation == "FileUploaded" //use the username between "" | where * has ""	1. Collect the Source/Destination IP address in the alert and check for all the activities performed with the IP address. 2. Check for any unusual large amounts of uploaded data/downloaded compared to other IP addresses, large app transactions compared to the IP address's history.(Please check the description of the alert to see the amount of data uploaded as compared to previously uploaded). Treat the data uploaded provided in the alert description as baseline to check the amount of data uploaded/downloaded. Use below query to get the uploaded/downloaded logs. OfficeActivity | where Operation == "FileDownloaded" or Operation == "FileUploaded" //use the username between "" | where * has "" 3. Check for any Destination IP addresses or URL captured for data being uploaded. If yes please verify the blacklist status of of IP/URL. For IP blacklist checking: https://www.virustotal.com/gui/home/search https://mxtoolbox.com/ https://www.abuseipdb.com/ https://www.ipvoid.com/ip-blacklist-check/

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			URL/Domain checking tools: https://mxtoolbox.com/ https://www.virustotal.com/gui/home/url https://urlscan.io/ https://www.urlvoid.com/ 4. Check in Snow for any such related activity for any change or request being made. If found the activity treat it as BP. If not, Please check with user for confirming the activity. 5. If the IP/url is blacklisted please engage onshore team to block the IP/Url and if there is snow ticket raised for the same, please assign the ticket to EPD-secops team , if there is no business justification from user for the activity.
Authentication Attempts Against Disabled Accounts in AzureAD	44		1.Check audit logs in AAD to check timestamp when the account was disabled, and any significant account changes happened after that. 2.Check sign in logs in AAD for the user to observe which malicious activity was performed after the account was terminated, see details about type of user account (VIP/Normal/Service Account) IP/Location/Conditional Access Policy Status/Device used 3.Validate IP geo-location and reputation in Abuseipdb to check if IP is suspicious and from which country. (https://www.abuseipdb.com) 4.If IP reputation is non-suspicious and user is signing in from expected location using registered/compliant device, check with user/or their manager to see if the user's contract has got extended/recently completed or any other valid reason. If that's the case close the alert has benign positive 5.If the IP is suspicious and there is no valid reason for terminated user account activity, then close the incident as true positive and raise the request to offboard the MDM registered device from the user account. 6.If no suspicious activity, close ticket with comments 'Investigated via AAD. Failed login against disabled account. No suspicious activity. Closing ticket as Benign Positive'
Rare application consent	41		1. Check the events captured due to which offense is triggered. 2. Verify if necessary conditions for offense are matched. 3. Check for any pre-notification received or any ticket raised for usage of this account. a) In such case this activity should be consider as authorized activity. b) If no usage notification is found, you will need to raise a ticket for the same offense 4. Check for which application consent was granted. It can be found in the modified properties field in event payload. 5. Mention all the details regarding application which are present in the modified field. It contains consent type, granted on behalf of and other details. 6. Check which user has granted consent to the application. 7. Attempt to gather relevant information by engaging onshore team about the subject user: • Role of employee or partners involved (Executive, etc.) • Search Active Directory Users and Computers: a.) Get employee or service account owner's full name b.) Group membership, account history, notes c.) Lookup contact information, review role 8. Check if user was authorized to grant consent to the application.Engage onshore team to verify the user assignment groups, RBAC role and permissions of the user to check if user is authorized to perform the activity. 9. Identify source IP related to this activity, check for signin logs with username and check for the blacklist status using below tools: https://www.virustotal.com/gui/home/search https://mxtoolbox.com/ https://www.abuseipdb.com/ https://www.ipvoid.com/ip-blacklist-check/ KQL query: SigninLogs //put the username between "" | where * has "" a. Check the activities performed from the same source IP in last 24 hours. 10. If above mentioned activities are unauthorised, kindly ask to roll back the changes done by the user. Deactivate the user account in AD, Limit the roles assigned to the user. Please engage onshore team to perform the activity. 11. Engage onshore to check with end user for activities performed.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps

Communication with suspicious domain identified by threat intelligence	39	list of tools:
		URL/Domains:
		
		https://mxtoolbox.com/
		https://www.virustotal.com/gui/home/url
		https://urlscan.io/
		https://www.urlvoid.com/
			1. Capture the Domain detials, check for the Domain status, check if there is any redirection from the mentioned domain to another url/domain.
			
			URL/Domain checking tools:
			https://mxtoolbox.com/
			https://www.virustotal.com/gui/home/url
			https://urlscan.io/
			https://www.urlvoid.com/
			
			2. Check for the host if any suspicious activity is observed. Use below queries to get the logs for host machine.
			
			SecurityEvent
			//put the hostname between""
			| where * has ""
			
			DeviceEvents
			//put the hostname between""
			| where * has ""
			
			DeviceProcessEvents
			//put the hostname between""
			| where * has ""
			
			3. Check using KQL queries for any other communication to and from the mentioned domain or with the domain/url which the reported domain is redirecting.
			
			Step 1.
			//replace xyz.com with the url/domain found in alert or while checking the upload/download logs
			search "xyz.com"
			| distinct $table
			
			With all the table available go through different table where the URL is captured using the table name
			
			Step 2
			
			//Replace the table name with the table name found in step 1. Repeat for all the tables found in step 1
			TableName
			//use the url between ""
			| where * has ""
			
			3. Engage Onshore team tp check for further details in Defender
			4. If the domain is clean and no suspicious activity is observed, treat the alert as BP.
			5. If not please escalate for blocking of the domain on perimeter level.
			
			Note: Please do not click on the URL related to domains and defang the url before providing the URL for any further investigations.

Anomalous behavior in discovered users	34	OfficeActivity
		| where Operation == "FileDownloaded" or Operation == "FileUploaded"
		//use the username between ""
		| where * has ""
			1. Collect the user details in the alert and check for all the activities performed by the user during the time alert was triggered.
			
			Step 1.
			//replace xyz with the username found in alert.
			search "xyz"
			| distinct $table
			
			With all the table available go through different table where the username is captured using the table name
			
			Step 2
			
			//Replace the table name with the table name found in step 1. Repeat for all the tables found in step 1
			TableName
			//use the username between ""
			| where * has ""
			
			2. Check for any unusual large amounts of uploaded data compared to other users, large app transactions compared to the user's activity in past.(Please check the description of the alert to see the amount of data uploaded as compared to previously uploaded). Treat the data uploaded provided in the alert description as baseline to check the amount of data uploaded/downloaded. Use below query to get the uploaded/downloaded logs.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			OfficeActivity | where Operation == "FileDownloaded" or Operation == "FileUploaded" //use the username between "" | where * has "" 3. Check for any Destination IP addresses or URL captured for data being uploaded. If yes please verify the blacklist status of of IP/URL. For IP blacklist checking: https://www.virustotal.com/gui/home/search https://mxtoolbox.com/ https://www.abuseipdb.com/ https://www.ipvoid.com/ip-blacklist-check/ URL/Domain checking tools: https://mxtoolbox.com/ https://www.virustotal.com/gui/home/url https://urlscan.io/ https://www.urlvoid.com/ 4. Check in Snow for any such related activity for any change or request being made. If found the activity treat it as BP. If not, Please check with user for confirming the activity. 5. If the IP/url is blacklisted please engage onshore team block the IP/Url and if there is snow ticket raised for the same, please assign the ticket to EPD-secops team, if there is no business justification from user for the activity.
Failed Login Attempt by Expired account	34		1. Check sign in logs in AAD (Azure Active Directory) around time of event to see activity done by the user and if the session access token or session got expired. 2. Check audit logs in AAD around time of user activity and when the account was expired. 3. Check if IP reputation is suspicious and check ISP location of the IP from the tools listed below : For IP blacklist checking: https://www.virustotal.com/gui/home/search https://mxtoolbox.com/ https://www.abuseipdb.com/ https://www.ipvoid.com/ip-blacklist-check/ 4. If IP location is unexpected(not in expected VPN list0), confirm with user if any suspicious activity seen.
Anomalous Token	33		1. Under AAD in signin logs, check what device user is signing into and if its compliant from "Device Info" tab. 2. Check "Location" tab to see IP address & respective location. 3. Confirm with user if sign-in is legitimate and if user is travelling or VPN used in case of suspicious location. 4. If the answer to 3 is "No", get password of the user account changed.
Azure WAF matching for Log4j vuln(CVE-2021-44228)	33		1 Check IP location and reputation in Abusedb/Cisco Talos Reputation Center to check if IP is flagged as malicious. (https://www.abuseipdb.com) 2 Check the Azure Diagnostics (sentinel logs) by running KQL query selecting the "Time range" matching with alert timeline, to find out outcome of the malicious web requests made by the IP flagged in the alert. AzureDiagnostics | search "IP" | summarize count()by TimeGenerated, Message, requestUri_s, httpMethod_s, httpStatus_d, client_ip_s, host_s, ResourceGroup, WAFMode_s, serverStatus_s, action_s, details_message_s, originalHost_s 3 Check targeted resource groups, requested uri, web request methods (Put,Post,Get,Delete) used and header to see if any malicious activity has been observed or not, if observed Notify the team to take necessary actions. 4 Check the Http status codes for the requests in the logs. If the http status codes are 300s or 400s or 500s, then the confidured WAF has detected/matched/blocked the web requests coming out of that IP. If the requests were blocked close the alert as True positive (If IP is malicious) or False Positive (If IP is not malicous). 5 If the Http status codes is 200 success codes, then need to investigate further about which host is affected, if any sign-ins, inbound/outbound traffic is seen coming out of that malicious IP and for how long.
Okta policy change occurred	32		1. Capture details like who initiated the change(actor), what change was made & on which account, changes were made(target). 2. Check if the actor is authorized to make such changes. Check in SNOW with the username, check the user details. verify user is part of the organisation or not. Engage Onshore team to verify the groups, roles and access detials of user on AD. 3. Check if there is any service request raised for it. If yes, close the incident as Benign positive.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			4. Confirm with the actor if the activity is legitimate or not. Engage onshore team to connect with end user for the update. 5. If answer to 2 is 'No', ask the actor for reason behind the activity. 6. Check sign logs & audit logs of the user for suspicious activities. use below queries to get the required logs: SigninLogs //put the Actor/target between "" | where * has "" AuditLogs //put the Actor/target between "" | where * has "" 7. Verify the IP address of the actor using below tools and if blacklisted please engage onshore team to block the IP and if there is snow ticket raised for the same, please assign the ticket to EPD-secops team for blocking the IP address.For IP blacklist checking: https://www.virustotal.com/gui/home/search https://mxtoolbox.com/ https://www.abuseipdb.com/ https://www.ipvoid.com/ip-blacklist-check/

Okta admin role assigned	23		1. Check user details like who is the actor.
			2. Check client details like device type, OS, browser involved, agent details.use below steps to capture logs
			
			Step 1.
			//replace xyz with the username found in alert.
			search "xyz"
			| distinct $table
			
			With all the table available go through different table where the username is captured using the table name
			
			Step 2
			
			//Replace the table name with the table name found in step 1. Repeat for all the tables found in step 1
			TableName
			//use the username between ""
			| where * has ""
			
			3. Check IP details like IP address involved, country & city.and verify the IP address of the actor using below tools and if blacklisted please engage onshore team to block the IP and if there is snow ticket raised for the same, please assign the ticket to EPD-secops team for blocking the IP address.
			
			For IP blacklist checking:
			https://www.virustotal.com/gui/home/search
			https://mxtoolbox.com/
			https://www.abuseipdb.com/
			https://www.ipvoid.com/ip-blacklist-check/
			
			4. Check what priviledges have been provided. Use below query to get the logs
			
			AuditLogs
			//put the Actor/target between ""
			| where * has ""
			
			5. Check if the actor is authorized to assign such roles.Check in SNOW with the username, check the user details. verify user is part of the organisation or not. Engage Onshore team to verify the groups, roles and access detials of user on AD to check if user has authorisation to perform the activity.
			6. Check with the actor if the activity is legitimate or not. Engage onshore team to connect with end user to verify the activity.
			7. If the browser involved is ""Unapproved"", ask the user for reason behind using unapproved software.Engage onshore team to check with enduser for the reason of using an unapproved browser.
			
			8. Check sign logs & audit logs of the user for suspicious activities.
			
			use below queries to get the required logs:
			
			SigninLogs
			//put the Actor/target between ""
			| where * has ""
			
			AuditLogs

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			//put the Actor/target between "" | where * has "" 9. If the activities are suspicious please engage onshore team to deactivate the user account.

External user added (Teams)	17		1. Check user details who performed the activity.
			2. Check Defender for Cloud Apps for further details. Please engage onshore team to check details of user activity in Defender.
			3. Check details of the user added : Name, domain.
			4. Check if communication with the domain involved is allowed or not. Check blacklist status of the domain use below tools
			
			URL/Domain checking tools:
			https://mxtoolbox.com/
			https://www.virustotal.com/gui/home/url
			https://urlscan.io/
			https://www.urlvoid.com/
			
			5. Check user activity who has been added using below queries. If user activities are suspicious please engage onshore team and if confirmed suspicious, plese ask onshore team block the user access.
			
			Step 1.
			//replace xyz with the username found in alert.
			search "xyz"
			| distinct $table
			
			With all the table available go through different table where the username is captured using the table name
			
			Step 2
			
			//Replace the table name with the table name found in step 1. Repeat for all the tables found in step 1
			TableName
			//use the username between ""
			| where * has ""
			
			6. Check with the user if the activity is legitimate or not. Please engage onshore team to connect with enduser to confirm the same.
			7. If answer to 4 is ""Yes"", add the domain to exception list in Defender for Cloud Apps. Please engage onshore team to add the domain in exception list.

Investigation priority score increase	17		1. Check the user for whom alert is triggered. 2. In the Microsoft 365 Defender portal, under Assets, select Identities. 3. Hover over the user. Select the three dots to the right of the user, and choose View User page. 4. Review the information in the User page to get an overview of the user and see if there are points at which the user performed activities that were unusual for that user or were performed at an unusual time. 5. Check with the user if the activities are legitimate. 6. Check sign logs & audit logs of the user for suspicious activities. 7. If the alert is Benign Positive, reset investigation priority score for the user.
New high upload volume app	14		1. Check the app for which alert is triggered. 2. Check volume & type of data uploaded. please use below query to check the logs. OfficeActivity | where Operation == "FileUploaded" //use the username between "" | where * has "" 3. Check users associated with the alert such as the users who are uploading the file & with whom files are being shared. Use below query to check for the logs: OfficeActivity | where Operation == "FileDownloaded" or Operation == "FileUploaded" //use the username between "" | where * has "" 4. If the domain with which files are being shared is external, check if file sharing is allowed or not. Please engage onshore team to verify the external sharing of file in Defender for Cloud Apps. 5. Check with user if the activity is legitimate and reason behind uploading the

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			files. Engage onshore team to check with end user for the legitimacy of the activity.
Anomalous IP with failed sign in attempts	14	list of tools: For IP blacklist checking: https://www.virustotal.com/gui/home/search https://mxtoolbox.com/ https://www.abuseipdb.com/ https://www.ipvoid.com/ip-blacklist-check/	1. Check the user for whom alert is triggered. 2. Check IP details such as IP address, location mapped with IP address and verify the IP address of the actor using below tools and if blacklisted please engage onshore team to block the IP and if there is snow ticket raised for the same, please assign the ticket to EPD-secops team for blocking the IP address. For IP blacklist checking: https://www.virustotal.com/gui/home/search https://mxtoolbox.com/ https://www.abuseipdb.com/ https://www.ipvoid.com/ip-blacklist-check/ 3. Check signin logs of the user and look for the IP address under Signin Logs. 4. Check IP reputation & risk score. Use the tools mentioned in step 2. 5. Check audit logs of the user to look for suspicious factors such as device used for login. use below queries to get the required logs: SigninLogs //put the Actor/target between "" | where * has "" AuditLogs //put the Actor/target between "" | where * has "" 6. If the device used is domain joined & compliant, use the output from Step 5 SigninLogs to verify the detials. Enagage onshore to check with the user if activity is legitimate or not.

Mass delete	13	list of tools:
		
		For IP blacklist checking:
		https://www.virustotal.com/gui/home/search
		https://mxtoolbox.com/
		https://www.abuseipdb.com/
		https://www.ipvoid.com/ip-blacklist-check/
			1. Check the user for whom alert is triggered.
			2. Check volume & type of data deleted.
			
			OfficeActivity
			| where Operation == "HardDelete" or Operation == "FileDeleted" or Operation == "FileDeletedFirstStageRecycleBin"
			//use the username between ""
			| where * has ""
			3. Check other details such as Timeline, IP address involved, user location. use below queries to capture the detials from signin logs. For checking the timeline please engage onshore team to check the Device Timeline in Defender for endpoint for the time duration mentioned the incident occured or delete happened.
			
			SigninLogs
			//put the username between ""
			| where * has ""
			
			4. Check IP reputation & risk score.
			
			For IP blacklist checking:
			https://www.virustotal.com/gui/home/search
			https://mxtoolbox.com/
			https://www.abuseipdb.com/
			https://www.ipvoid.com/ip-blacklist-check/
			
			5. Check audit logs of the user to look for suspicious factors such as device used for login.
			use below queries to get the required logs:
			
			SigninLogs
			//put the Actor/target between ""
			| where * has ""
			
			AuditLogs
			//put the Actor/target between ""
			| where * has ""
			
			6. If the device used is domain joined & compliant, use the output from Step 5 SigninLogs to verify the detials. Enagage onshore to check with the user if activity is legitimate or not.

Impossible travel activity	10	list of tools: For IP blacklist checking: https://www.virustotal.com/gui/home/search https://mxtoolbox.com/	1. Check the user for whom alert is triggered. 2. Check the IP addresses associated and locations mapped with IP addresses. For IP blacklist checking: https://www.virustotal.com/gui/home/search

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
		https://www.abuseipdb.com/ https://www.ipvoid.com/ip-blacklist-check/ KQL Qyery SigninLogs //Please use Username between "" | where * has ""	https://mxtoolbox.com/ https://www.abuseipdb.com/ https://www.ipvoid.com/ip-blacklist-check/ 3. Check if any of these IP addresses are used by the organization for VPN connections, If yes whitelist them. 4. If answer to 3 is ""No"", check IP reputation & risk score. Use the tools provided in step 2. 5. Check audit logs of the user to look for suspicious factors such as device used for login. use below queries to get the required logs: SigninLogs //put the Actor/target between "" | where * has "" AuditLogs //put the Actor/target between "" | where * has "" 6. If the device used is domain joined & compliant, use the output from Step 5 SigninLogs to verify the detials in Device details column. Enagage onshore to check with the user if activity is legitimate or not.
Application Gateway WAF - SQLi Detection	9		1. Capture details : client IP, Uri, action. 2. Over OSINT, check IP reputation. For IP blacklist checking: https://www.virustotal.com/gui/home/search https://mxtoolbox.com/ https://www.abuseipdb.com/ https://www.ipvoid.com/ip-blacklist-check/ 3. Contact Onshore Team to get the Uri captured from incident logs for SQL vulnerabilities. 4. If the action captured from Incident logs is not blocked, get the IP address blocked with the help of Onshore Team.

Activities from suspicious user agents	8	list of tools:
		URL/Domains:
		
		https://mxtoolbox.com/
		https://www.virustotal.com/gui/home/url
		https://urlscan.io/
		https://www.urlvoid.com/
			1. Check user details like who is the actor.
			2. Check client details like device type, OS, browser involved, agent details. Use below queries to get the logs to extrat the required data:
			
			OfficeActivity
			//use the username between ""
			| where * has ""
			
			SigninLogs
			//put the username between ""
			| where * has ""
			
			AuditLogs
			//put the username between ""
			| where * has ""
			
			3. Check activity involved around agent like file sharing. Use the output from step 2.
			
			4. Check sign logs & audit logs of the user for suspicious activities. Use output from step 2.
			
			5. Check domain or users with whom the activity is performed and if communication with them is allowed or not. For domains please use the opensource tools to verify the blacklist status of the domain and if blacklisted treat it as TP and engage onshore team to block the domain and assign the snow ticket to EPD-secops team.
			
			URL/Domain checking tools:
			https://mxtoolbox.com/
			https://www.virustotal.com/gui/home/url
			https://urlscan.io/
			https://www.urlvoid.com/
			
			5. Engage onshore team to check with user if the activity is legitimate and reason behind the activity.

Suspicious Creation of User in AzureAD to perform Privileged Activities	0		1. Check which account created the user and in AAD under assigned roles, check if role of the account is Administrator. 2. Review audit log of account activity by checking the time of the alert in AAD to see if activity is legit or suspicious and if any reason behind the action is provided (Generally Servicenow ticket/Reason for PIM activation is mentioned). 3. Also match this activity timestamp with the AAD sign-in logs for the account to check IP used and sign-in status of the user. 4. Check which user account is created & what all priviledges have been assigned to the account. Also, check if there are any other user accounts created by the source account. and what priviledges have been provided to them

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			5. If the activity looks suspicious validate with the user, get all the accounts blocked & deleted.
Internal Network Port Scan Detected	0		1. Capture details : Source IP, Destination IP, Destination Ports. 2. Under signin logs from AAD, check which user is logged in from that IP. 3. Under "Device Info" tab, check the device status - whether it is compliant or not, domain joined or not. 4. Check if there is any request raised for the activity in ServiceNow. 5. If answer to 4 is No, ask the user to confirm legitimacy of the activity and ask him to share approval for it.
Suspicious High Number of SSO Account Lockouts	0		1. Capture details : accounts impacted. 2. In AAD under signin logs, check what is the IP address behind the login attempts. - check with Onshore team if the IP is internal or external. 3. Under "Device info" check the device details - whether it is compliant or not, domain joined or not. 4. In Signin logs, check which application was the account trying to log into. 5. In ServiceNow, check who is owner of that device. 6. In AAD, under "Users" Tab, search for the account impacted and check if the applications captured in step 4 are listed under "Applications" blade or not. 7. If not check with the user to confirm legitimacy of the actvity.
Workspace deletion attempt from an infected device	0		1. Capture details : Account Impacted, Ip address, file associated, Command line used. 2. Check with Onshore team, if the IP is internal or external. 3. From ServiceNow, fetch the device now associated with the IP address. 4. Ask Onshore team to perform a detailed Scan on the device and to get the impacted file deleted. 5. Check with user whether the activity is legitimate or not. 6. If answer to 5 is No , get the password for User's account reset.
Possible Web Exploit / Webshell Deployment Attempt	0		1. Capture details from incident logs : client IP address, request uri, original host 2. Over OSINT, check reputation ofclient IP. For IP blacklist checking: https://www.virustotal.com/gui/home/search https://mxtoolbox.com/ https://www.abuseipdb.com/ https://www.ipvoid.com/ip-blacklist-check/ 3. Contact Onshore team to get original host scanned for the existence of Webshell vulnerability and ask them to get the client ip blocked.
Credential Dumping Tools - Service Installation	0		1. Capture details : HostName, ServiceName, ServicePath, Account Name. 2. Check device timeline for other suspicious activities using "DeviceEvents" table. Look for the user account logged in near the activity timeline. 3. Check "DeviceNetworkEvents" to look for suspicious inbound & outbound network connections. 4. Check with user to confirm legitimacy of the activity. 5. Contact Onshore team and ask them to run a deep scan on the impacted machine & to get the service uninstalled. 6. Get suspicious domains observed in Step 3 (if any) blocked by Onshore team.
IP address of Windows host encoded in web request - Zscalar	0		1. Capture details : HostIP, Request URL, Remote IP 2. Over OSINT, check reputation of Remote IP. For IP blacklist checking: https://www.virustotal.com/gui/home/search https://mxtoolbox.com/ https://www.abuseipdb.com/ https://www.ipvoid.com/ip-blacklist-check/ 3. Over OSINT, check URL reputation. URL/Domain checking tools: https://mxtoolbox.com/ https://www.virustotal.com/gui/home/url https://urlscan.io/ https://www.urlvoid.com/ 4. Contact Onshore team to get the machine behind client IP deep scanned for presence of malware if any. 5. Using "DeviceEvents" or "DeviceNetworkEvents", check machine timeline for suspicious activities. 6. If IP & domain are blacklisted, get them blocked with the help of Onshore team.
More than 5 applications connections got deleted within Okta	0		1. Capture details : actor, client agent, client geographical country. 2. In AAD, check sign in logs of the user/account and under "Device Info" see if the signins are from compliant or non compliant device. Capture IP addresses involved. 4. Check against EPA's Internal IP range if IP addresses belongs to EPA or not(There should be a list of IP address provided to SOC Team). If Yes, check with the user if it was a legitimate activity. 5. If answer to 4 is "No", discuss with Onshore team and get the password for that user/account changed and OKTA sessions for the user cleared by performig the steps listed at https://support.okta.com/help/s/article/Killing-an-End-User-Session?language=en_US
Okta API token created	0		1. Capture details : actor, securitycontext_isp. 2. In AAD, check sign in logs of the user/account and under "Device Info" see if the signins are from compliant or non compliant device. Capture IP addresses involved. 4. Check against EPA's Internal IP range if IP addresses belongs to EPA or not(There should be a list of IP address provided to SOC Team). If Yes, check with the user if it was a legitimate activity. 5. If answer to 4 is "No", discuss with Onshore team and get the password for that user/account changed and OKTA sessions for the user cleared by performig the steps listed at https://support.okta.com/help/s/article/Killing-an-End-User-Session?language=en_US

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
UC-CC-1497 - Connection to DGA Domain	0		1. Capture details : DGA Domain, SourceIP. 2. Over OSINT, check Domain reputation. URL/Domain checking tools: https://mxtoolbox.com/ https://www.virustotal.com/gui/home/url https://urlscan.io/ https://www.urlvoid.com/ 3. From "DeviceNetworkEvents" table, identify the source machine using IP address captured and identify the account logged in at that time. Also, check if there any any suspicious inbound connections. 4. From "DeviceEvents" table, check machine timeline for suspicious activities if any. 5. Contact Onshore Team and get the host deep scanned for presence of malware if any. Also, ask them to check legitimacy of the connection with the user. 6. Get the domain blocked with the help of Onshore Team
Advanced Multistage Attack Detection	0		1. Capture details : DeviceName, AccountName, Entities involved such as file, domain, process, commandline. 2. Using "DeviceEvents" check machine timeline for suspicious activities. Also, check the command line used if any. 3. Using "DeviceFileEvents" or "DeviceProcessEvents" or "DeviceRegistryEvents" or "DeviceNetworkEvents", check the existence of suspicious activities if any. 4. Contact Onshore Team and get the impacted host deep scanned. Also, ask them to contact the user to confirm legitimacy of the activities. 5. Get the remote URL, Remote IP blocked if found blacklisted. For IP blacklist checking: https://www.virustotal.com/gui/home/search https://mxtoolbox.com/ https://www.abuseipdb.com/ https://www.ipvoid.com/ip-blacklist-check/ . URL/Domain checking tools: https://mxtoolbox.com/ https://www.virustotal.com/gui/home/url https://urlscan.io/ https://www.urlvoid.com/ 6. Get the host isolated with the help of Onshore team if found to be compromised.
Possible API/Application/Session Level Manipulation - Access Application with non-existing sessionCookie	0		1. Capture details from incident logs : IP Address & location, user raw agent. 2. In AAD, under Signin Logs, check the logs against IP address fetched from Step 1 and capture user account associtaed with it. Also, check device details under "Device Info" Tab such as If the device is compliant or not, domain joined or not. 3. In Incident list, check if their are any more incidents for the impacted user account or for the IP address captured. 4. In ServiceNow, check if there is any ticket related to the activity. 5. Check with user to confirm legitimacy of the activity. 6. Contact Onshore Team and ask them to perform steps mentioned at https://support.okta.com/help/s/article/Killing-an-End-User-Session?language=en_US
Possible API/Application/Session Level Manipulation - AuthSession Upgrade with Bad authCookie	0		1. Capture details from incident logs : IP Address & location, user raw agent. 2. In AAD, under Signin Logs, check the logs against IP address fetched from Step 1 and capture user account associtaed with it. Also, check device details under "Device Info" Tab such as If the device is compliant or not, domain joined or not. 3. In Incident list, check if their are any more incidents for the impacted user account or for the IP address captured. 4. In ServiceNow, check if there is any ticket related to the activity. 5. Check with user to confirm legitimacy of the activity. 6. Contact Onshore Team and ask them to perform steps mentioned at https://support.okta.com/help/s/article/Killing-an-End-User-Session?language=en_US
Possible API/Application/Session Level Manipulation - SSO Session Integrity Failure	0		1. Capture details from incident logs : IP Address & location, user raw agent. 2. In AAD, under Signin Logs, check the logs against IP address fetched from Step 1 and capture user account associtaed with it. Also, check device details under "Device Info" Tab such as If the device is compliant or not, domain joined or not. 3. In Incident list, check if their are any more incidents for the impacted user account or for the IP address captured. 4. In ServiceNow, check if there is any ticket related to the activity. 5. Check with user to confirm legitimacy of the activity. 6. Contact Onshore Team and ask them to perform steps mentioned at https://support.okta.com/help/s/article/Killing-an-End-User-Session?language=en_US

Okta Administrator logs in during non-business hours	0		1. Check user details like who is the actor.
			2. Check client details like device type, OS, browser involved, agent details. use below steps to capture logs
			
			Step 1.
			//replace xyz with the username found in alert.
			search "xyz"
			| distinct $table
			
			With all the table available go through different table where the username is captured using the table name
			
			Step 2
			
			//Replace the table name with the table name found in step 1. Repeat for all the tables found in step 1
			TableName

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps

			//use the username between ""
			| where * has ""
			
			3. Check IP details like IP address involved, country & city and verify the IP address of the actor using below tools and if blacklisted please engage onshore team to block the IP and if there is snow ticket raised for the same, please assign the ticket to EPD-secops team for blocking the IP address.
			
			For IP blacklist checking:
			https://www.virustotal.com/gui/home/search
			https://mxtoolbox.com/
			https://www.abuseipdb.com/
			https://www.ipvoid.com/ip-blacklist-check/
			
			4. Check with the actor if the activity is legitimate or not.
			5. Check if the browser used is other than "Microsoft Edge" or "Google Chrome". If Yes, engage them to check with enduser to confirm legitimacy of the activity and the reason of using an unapproved browser.
			6. Check sign logs & audit logs of the user for suspicious activities.
			
			use below queries to get the required logs:
			
			SigninLogs
			//put the Actor/target between ""
			| where * has ""
			
			AuditLogs
			//put the Actor/target between ""
			| where * has ""
			
			7. If the activities are suspicious please engage onshore team to deactivate the user account.

UC-EX.PE.PR-990 - Windows - Scheduled task created	253		1. Get information about name and content of the scheduled task from the events over sentinel and check if it is related to any well-known malicious service. 2. Search Host/IP details in CMDB on which new scheduled task was detected. - Identify Host type is it a workstation, Laptop or any critical asset like server. - Identify domain to which Host belongs. 3. What type of data is contained on the device where new task was detected? - Devices containing sensitive data are a higher priority for remediation. - Does it belong to VIP users? 4. Search past 12 hr logs for the host on which scheduled task was observed. - Check for the related events such as 4698, 4699, 4700, 4701 and 4702. - If event 4698 is followed by 4699 with same user and task name in short time, then there is possibility that task was created for short lifetime and might use to execute something and then was removed from task scheduler itself. - Also check for any other suspicious activities on system in past 12 hrs. 5. Check details of the user in CMDB, who created this task. Also check if user logged in with admin privileges. 6. Search past 12 hr windows logs for this user and check, - if any other suspicious activities have been done by user in past 12 hrs. - check for successful logins with logon type 2 or 10 to check whether task was created remotely. 7. If the task is legitimate close it as Benign positive or If the task is not legitimate then escalate to L2/L3 security member for further investigation and close as True Positive if activity was found malicious after investigation.
UC-EX-2116-Process Execution Frequency Anomaly	140		1.When SOC team observes a 'UC-EX-2116-Process Execution Frequency Anomaly' alert in Sentinel, it means anomalous spike in frequency of executions of sensitive processes. 2.Determine which sensitive processes have experienced anomalous spikes in execution frequency based on the alert details. 3.Examine the properties of the identified processes, such as process names and associated users or accounts. 4.Analyse the users or accounts associated with the anomalous process executions and look for any unusual or unauthorized user activity, including logins from unfamiliar locations or at abnormal times. 5.Analyse system logs, such as event logs and security logs, for any suspicious activities related to the identified processes. 6.check network logs for unusual communication patterns or connections associated with the sensitive processes. 7.Verify that the anomaly is not caused by any misconfigurations or legitimate changes in system behavior, such as recent software updates or system changes. 8.If malicious activities are confirmed, take immediate containment measures to prevent further damage. 9.If the Activity is malicious then escalate to L2/L3 security member for further investigation and close as True Positive if activity was found malicious after investigation ask them to Isolate affected systems from the network, terminate suspicious processes, and revoke credentials of compromised accounts.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
UC-IM-1803 - Windows - Massive file deletion on Mainstream Server	113		1. Check the events captured over sentinel due to which the alert is triggered for collecting ip detials and etc... 2. Verify the activity and if necessary take appropriate conditions for this alert are matched. 3. Check for any pre-notification received or any ticket raised for file deletion activity. - In such case this activity should be consider as authorized activity. - If no usage notification is found, you will need to raise a ticket and ask for details required for the investigation to proceed. 4. Check event payload and identify No. of files which are deleted also try to get details about destination IP, username, file name, file path and file size. 5. Check for all details of destination IP/hostname in CMDB and mention same in the ticket. Search for past 24 hours activity based on destination host/IP. - Identify total No. of files which are deleted in past 24 hr. - Concentrate on event ID 4660 and check for how long file deletion was observed. - Does deleted files includes any sensitive information. - Identify user who was logged in to destination host around time of this activity. - Check if user have accessed any sensitive data and if that data has been copied or uploaded before file deletion. - Check if any other suspicious activity detected from same destination IP such as connection towards malicious hosts etc. 6. Also check for AV status of destination Host to see if any risk has been detected on this host in past few days. 7. If any user found associated with this activity mention all the CMDB details of user account in the ticket. Also check if user account is normal/privileged/service account. 8. Check past 24 hours activity based on user account and check if any other suspicious activity is detected from same user such as brute force attempt or account lockout in past few days.
UC-IM-2113 - TI Map IP Entity to Zscaler	94		1. The initial step is reviewing the TI feed for any flagged IP addresses that seem suspicious. This could be based on multiple factors such as previous malicious activity, geolocation, or other threat intelligence indicators. 2. Review Zscaler logs for any activity linked to the flagged IP addresses. Look for suspicious patterns like multiple blocked requests, attempts to access forbidden websites or services, or unusual amounts of data transfer. 3. If any activities linked to the flagged IPs are found, investigate the user accounts involved. Check for any unusual behaviors like attempting to bypass security controls or accessing inappropriate content. 4. Analyze your network traffic logs to see if the flagged IP addresses are sending or receiving an abnormal volume of data, or if there are connections to unusual ports or services. 5. Review the Zscaler security policies to ensure they are appropriately configured to block potentially malicious activities. Check if any policy violations have been detected from the flagged IPs. 6. If the above steps reveal abnormal behaviors or signs of compromise, it is necessary to confirm the incident,then escalate to L2/L3 security member for further investigation and close as True Positive.
UC-IM-2112-TI Map IP Entity to Syslog	93		1. The initial step is reviewing the TI feed for any flagged IP addresses that seem suspicious. This could be based on multiple factors such as previous malicious activity, geolocation, or other threat intelligence indicators. 2. Syslog is a standard for message logging, and it can provide valuable information about network activities. Review the Syslog for any activity related to the flagged IP addresses. Look for any unusual patterns such as failed login attempts, suspicious network connections, or unexpected system changes. 3. If any activities related to the flagged IP addresses are found, investigate the user accounts and devices involved. Look for any signs of unusual activity, unauthorized access attempts, or security policy violations. 4. Check the network traffic logs to see if the flagged IP addresses are associated with an unusual volume of data transfer or are connecting to unexpected ports. 5. Check whether any devices have connected from the flagged IPs. If possible, review those devices for any suspicious software installations, unusual process activities, or evidence of lateral movement within your network. 6. Review the logs of services and applications that the flagged IP has interacted with. Unusual activities, errors, or security events can provide further insights. 7. If the above steps reveal abnormal behaviors or signs of compromise, it is necessary to confirm the incident then escalate to L2/L3 security member for further investigation and close as True Positive.
UC-CO-469 - O365 - O365_SharePoint_Unusual Multiple File Download activity	53		1. Identify the attack methodology: • Attack vector: -Multiple files downloaded with different file names. -Files downloaded by same username. 2. Identify the Source Host Name(s) and IP Address: If the source is external, gather relevant information about the source IP from open online sources: • Source IP: • Source Port(s):

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			• Blacklisted Status: • ISP: • Domain Name: • Location of the IP: 3. If the source is internal, gather the below details: • What type of data is contained on that device? -Devices containing sensitive data (i.e., PII) are a higher priority for remediation. -Does it belong to VIP users? 4. Identify the Destination Host Type: • Workstation or Server (Enterprise, Production, Development) -Are critical services being impacted? • Which Domain does the host belong to? • What is the MAC address? DHCP enabled? 5. Identify the Destination Host Name(s) and IP Address: • What type of data is contained on that device? -Devices containing sensitive data (i.e., PII) are a higher priority for remediation. -Does it belong to VIP users? 6. Identify the Destination Host Type: • Workstation or Server (Enterprise, Production, Development) -Are critical services being impacted? • Which Domain does the host belong to? • What is the MAC address? DHCP enabled? 7. Check the kind of files downloaded from the destination IP/host by looking at the request URL. Look if the file extensions are suspicious. Check the total number of files downloaded to know the possibility of an infection/attack. 8. Check the user agent used for downloading the files, device action, response code, request URL and its reputation, etc. to gain more information about the attack. 8. Search for the past 24-hour activities based on the source IP and see the following: • Were any suspicious destinations communicated by the same source? • Other signatures/traffic detected from the IP and the device action for them. • Check if any IPS/FW communication traffic is observed from the IP towards any internal asset: -Check the IPS Signatures detected and the device action for the same. -Check the FW traffic is accepted/dropped under the rule name. 9. Search for the past 24-hour Windows logs based on the source IP and see the following: • Event ID 4624 to know the user connected to the source machine and could be responsible for this activity. • (If the Analyst have access to AD) Collect the below information about the user account involved in the unusual download activity: Search Active Directory Users and Computers: -Role of employee -Get employee or service account owner's full name. -Group membership, account history, notes -Lookup contact information, review role. 10. Search for the past 5–15-day activities based on the user observed and see the following: • Was any brute force pattern observed towards the user? • Look for any suspicious event IDs to know if the account has been compromised or not. 11. Check if the antivirus definition for the host is updated or not. Also check if the host was infected with any malware risk. 12. Based on the above information, if the activity seems to be suspicious then escalate to L2/L3 security member for further investigation and close as True Positive.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
UC-CC-527 - O365 - New executable via Office FileUploaded Operation	40		1. Check the source IP involved in the activity. 2. If the source is external, gather relevant information about the source IP from open online sources: • Source IP: • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: 3. Check for past 7 days' logs for any suspicious activity performed from the same Source IP. 4. Check the username (UserId), who performed this action. 5. Check if any user was privileged or not. If yes, increase the severity. 6. Search for the past 7 days for any other suspicious activity from the same username. Have the credentials of the user been compromised, or the user has gone rouge? 7. Check the file that has been uploaded. 8. Check the extension of the file. 9. Check the reputation of the file on websites like "virustotal.com". 10. With the help of sandboxing techniques, the behavior of that executable can be studied. The analysis will provide us what the file was intended to do. 11. After the file was uploaded, check if any user has downloaded it,if downloaded file seems suspicious then escalate to L2/L3 security member for further investigation and ask them If any user has downloaded it remove the file from their system and perform a full AV scan, close as True Positive.
UC-EX-575 - Proxy - Suspicious URL Pattern	34		1. Identify the User Account, who was trying to access the suspicious URL(s). Check the privileges assigned to the user. Admin or non-Admin account. Did this account attempt to login on other systems? 2. Identify all the Source Host Name(s) & IP Address •What type of data is contained on that device? oDevices containing sensitive data (i.e. PII) are a higher priority for remediation oDoes it belong to VIP users? 3. Identify the Host Type •Workstation or Server (Enterprise, Production, Development) oAre critical services being impacted? •Which Domain does the host belong to? 4. Check the past 20 days logs based on the source User and check all the activities done by the user during this period. •Did the user access any other suspicious URL? if yes please check the details. 5. Check the past 20 days logs based on the source host/IP and check all the activity done by the host. •Any other suspicious activity had been done from the host. •Is this host connected towards the same destination or multiple destination? •Is there any pattern of traffic and how frequent traffic was? •Check the requested method and response code (was there any redirection of request) •Check the device action. •Check the reputation of observed requested URL on multiple online tools. •Check the URL category on online tools. •If possible check the user agent used in this activity. 6. Check if any other detection were observed for the same source host in the past 20 days. If yes, then please try to correlate (if possible). 7. If possible check the AV (computer status and risk report) of the system if not possible then escalate to L2/L3 security member for further investigation If not please suggest to AV team. 8. If the task is legitimate close it as Benign positive or If the task is not legitimate then escalate to L2/L3 security member for further investigation and close as True Positive if activity was found malicious after investigation.
Suspicious Cloud Resource Deployment	31		1. When SOC team observes a 'Suspicious Resource deployment' alert in Sentinel, it means that there is a resource deployed a previously unseen Caller. 2. Check for any received pre notification or any raised ticket for activities that could lead to such an alert. In this case, this activity should be considered as an authorized activity and hence be closed. 3. Identify User Principal name, Host name, association between the source, destination and the user (workstation, servers and the role definition). 4. Check if the User is active on Azure AD if yes close it as Benign positive, if not then escalate to L2/L3 security member for further investigation
UC-DE-863 - Windows - Event Auditing disabled	24		1. Identify the attacker that audit logs are disabled. o Investigate the attacker (or) source username. o Investigate the user has performed any malicious activity. o Identify the activity based on source host (or) source ip address. 2. Identify the Host Name(s) & Internal Source IP Address • What type of data is contained on that device? o Devices containing sensitive data (i.e. PII) are a higher priority for remediation o Does it belong to any high critical application? 3. Identify the Host Type • Workstation or Server (Enterprise, Production, Development) o Are critical services being impacted?

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			• Which Domain does the host belong to? • What is the Mac address? If it is a windows workstation DHCP enabled? 4. Examine the Windows event logs on the affected system to identify when the auditing was disabled and if there are any other related events that might indicate the cause of the incident. 5. Investigate if there have been any unauthorized access or login attempts on the affected system. Look for any signs of credential misuse. 6. Confirm the time of the audit logs disabled. The time SIEM tool received the event may not be the time the activity occurred. • Investigate the alert and base logs to check for the additional information related to the event. • Check for the event ids (4624,1102 and 1100 in past 24HRS) 7. Check the AV status of the Host (if available). 8. Research in SIEM for that user in the 7 hours prior to the login events to look for other anomalous activity. · Search for all activity with username in last 15 days 9. Develop historical context associated with the machine. For example, does this machine have a history of malware infections, has the machine generated alerts that were not sent to SIEM, etc. 10.If anything seems malicious then escalate to L2/L3 security member for further investigation and ask them to Enable event auditing immediately on the affected system(s) to start capturing critical security events. and Verify whether this is related to testing activity if yes Recommended to inform to the SOC, before performing any such kind of activities.
Suspicious granting of permissions to an account	19		1. When SOC team observes a 'Suspicious granting of permissions to an account' alert in Sentinel, it means an unauthorized account initiated the granting of permission to an account in Azure Environment. Hence this incident needs to be investigated on priority basis. 2. Check for any prior notification received or any ticket raised or any ongoing change taking place related to this operation in Azure Environment: 3. In such case this activity should be considered as legitimate activity. 4. If not, raise a ticket for the offense and ask for details required for the investigation to proceed. 5. Try to capture the information about the Source IP, Role Assignor, Role Assignee, permission granted. 6. Search for past 24 hours' activities based on the Source IP: 7. Check the reputation of the External IP using online platforms like abuseipdb.com.,virus total,mxtoolbox.com 8. Verify if external IP is allowed to perform such activities. If no, increase the severity. 9. Identify if that source has tried communicating to our environment before which may linked to Command and Control communications. 10. Check for communications in the last 7 days. 11. Check for any other suspicious activity and report in the security incident. 12. Identify the User/subscription role assignor associated with this activity and search for various activities performed by the User/account. For Example: * Check all details of this user from Active Directory. * Check the privileges assigned to the account. 13. Identify if the user/account has granted permission to any critical data/resource, Audit policy information or any other activities. Also check the result type (start,success etc) . 14. Check if the account had any failed login attempts which could indicate a brute force followed by a compromise of the account. 15. Search for the various activities being performed by the user towards same/multiple destination host. Identify if there is any history of suspicious connections from any external IPs. 16. If any other suspicious activity found, report in the security incident. Check the logs based on the User/subscription role assignee around the time of the alert generation: 17. Check the details of user mapped with the Object ID found from Active Directory. Check the privileges assigned to the account. 18. Check the activities based on the user, try to identify the subscription ID/ permissions granted (such as reader, owner etc.) towards one/multiple resources and its respective domains. 19. Identify if any suspicious activity has been performed by the assignee after granting permissions and its impact. Confirm the time of activity. The time Log Analytics Workspace received the event may not be the time the activity occurred. Raise a ticket with respective resolver group/ escalate to l3 if needed to check with user for activities performed.
UC-PE-881 - Windows - Local User Creation	18		1. Start collecting the information about newly created user account, such as their, username:account type:any group memberships:user's email ID:user account privileges from events. 2. Check if this local user creation is legitimate activity or not(based on user details Example :if user belongs to internal Capgemini team or EPA team). Check for the permissions or approvals for creating this account.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			3. If this creation of local user is malicious activity, investigate on the details of user account that has been used to perform this action and fetch the details like their username, user account privileges, email ID, Account type etc., 4. Determine the source system of the attempt with attacker's hostname and IP address. 5.if any ip address is found, kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 6. Check for signs of persistence, such as suspiciously modified registry keys, scheduled tasks, or services. Investigate whether the newly created user account is part of any suspicious groups or has elevated privileges. 7. Check for any other accounts or systems that may have been compromised because of the user creation. Attackers might use this new user account to pivot and escalate their privileges. 8. Check relevant event logs on the affected system, especially the Security event log, for any events related to user creation or modification. 9. Look for Event IDs such as 4720 (A user account was created), 4722 (A user account was enabled), or 4724 (An attempt was made to reset an account's password). 10. Review the permissions of existing user accounts and correlate them with the newly created user account. Investigate for any elevated privileges has been given which grants access to restricted areas of the system or network. 11. If the activity seems as suspicious then escalate it to l3 team or respective resolver group.
UC-CC-209 - DNS - Rare high NXDomain count	14		1) Understand the specifics of the alert • Identify the affected client IP address mentioned in the alert. • Note any associated DNS domain names mentioned in the alert. 2) Check if the client IP is internal or external. 3) Check for Recent Changes: • Identify if there have been recent changes to DNS records or configurations. • Determine if changes align with the increase in NXDomain count. 4) Cross-reference the client IP with any known assets or systems in the organization. 5) Analyze TTL Values: • Check the Time-to-Live (TTL) values of DNS records to ensure they are set appropriately. • Incorrect TTL values might contribute to higher NXDomain counts. 6) Gather relevant data for investigation: • Collect DNS logs for the specified client IP. • Collect network traffic logs if available. • Retrieve historical DNS data for the past 10 days. 7) Correlate the findings with other available data: • Check for any unusual network communication from the client IP. • Look for patterns of communication to specific domain names. 8) Analyze historical data to understand the pattern • Identify if the client IP has shown similar behavior in the past. • Look for changes or spikes in activity. 9) Check the reputation of the client IP: • Utilize threat intelligence sources to determine if the IP is associated with malicious activity. 10) Search for past 24 hr logs based on source IP and check, • Any other offense or logs from the same source IP? • Any other user tried to login using the same source IP? Possibility of brute force attack. 9) Check the AV reports (computer status and risk report) of the target host. If not, please suggest to the AV team. 10) Based on the above information, if the activity seems to be suspicious then escalate to L2/L3 security member or respective resolvergroup for further investigation and close as True Positive.
UC-PR-1152 - AD - Windows Privileged Escalation from a user account	9		1. Identify the attack methodology. • Attack vector: o Identify the user/account responsible for this activity. o Check the privileges assigned to the account. o Check the events based on the account before and after time of activity. 2. Check the token elevation type in the event details or the payload of the events due to which offense is triggered. 3. Identify the User Account(s) for which the privilege got assigned. • Was this account Local account? • Did this account attempt to login on other systems? o Time periods? 4. Identify the Host Type • Workstation or Server (Enterprise, Production, Development)

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			• Does the assert is critical or normal? • Which Domain does the host belong to? • What type of data is contained on that device? o Devices containing sensitive data (i.e., PII) are a higher priority for remediation. 5. Check if any other suspicious activities were performed from the same IP address in 24 hours and also kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ F. Create a focused channel based on the host for about 12-24hrs/last30 days. • Search for Windows/AD logs for the event ID 4624, 4672 to find the details about the user logged in, privileges assigned around the time of alert. • Check all the activities/event Id's based on the host by same/other accounts. • Check for other suspicious activities and report it in the security incident. 6. Attempt to gather relevant information about the subject user: • Role of employee (Executive, Manager etc.) • Is this user having 'privileged' access (ADMIN) • Search Active Directory Users and Computers: a. Get employee full name, Work Location b. Group membership, account history c. Lookup contact information, review role 7. Create a focused channel based on the account for past 24 hrs. • Check the privileges assigned to the user/account. • Check the activities performed by the user towards other hosts. • Identify if the user has granted any access to critical data, and if any changes being done. • Find it any other suspicious activity performed by the User report it in the security incident. 8. Confirm the time of activity. The time SIEM tool received the event may not be the time the activity occurred. 10. Develop historical context associated with the host. For example, does this machine have a history of assigning privileges and performed any activities before that were not sent to SIEM, etc. 11. Check with concerned team or l2/l3 whether If it is authorized behavior or not. 12. If not, kindly investigate the user to know the reason behind performing such activity. 13. If the activity was not legitimate, kindly disable the user who performed this activity temporarily and change the password immediately. Revoke the privileges taken by the account to perform this activity.
UC-PR-1619-PIM Elevation Request Rejected	4		1. Identify source IP associated with this activity. • Check if the IP is internal/external. In case of External IP, check for reputation of the IP on online databases: Check the reputation for all the Client IPs: https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ and if the result is bad reputation, increase the severity of the alert. • In case of internal IP, check if there has been any activity happening from this IP in past 30 days/60 days. 2. Check the User/Account related to this activity. • Check if any user was privileged or not. If yes, increase the severity. • Check if the timestamp for successful login was seen after the failed attempts only and not in between. If yes, increase the severity. 3. Check with respective team for AV reports of source system (in case of internal IP) and check if any risk was detected on system in past 30 days. 4. Search for past 24 hrs/30 days logs based on source IP and check, • If any other suspicious activity is detected from same source IP 5. Search for past 24 hr logs based on User/Account and check, • If this user has tried to login from multiple locations. • If this user has had a high number of failed logins in the recent past with no successful logins. • If this user committed any activity after the triggering of this alert that is suspicious or critical. 6. Develop historical context associated with the machine. For example, does this machine have a history of lockouts or malware infections, has the machine generated alerts that were not sent to SIEM tool.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			7. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team.
UC-PR-112 - Azure - Azure DevOps Administrator Group Monitoring	3		1. Check for any prior notification received or any ticket raised or any ongoing change taking place to this operation in Azure Environment. • In such case this activity should be considered as legitimate activity. • If not, raise a ticket for the offense and ask for details required for the investigation to proceed. 2. Try to capture information about the Source IP, Role Assignor, Role Assignee, permission granted. 3. Review Audit Logs: Check the audit logs in Azure DevOps to see if there are any records of changes made to the Administrator group. Look for any unexpected or unauthorized modifications. 4. Trace System Access: If you suspect a security breach, investigate further by reviewing system logs and tracing user access. Identify any unusual patterns or access from unauthorized sources. 5. Identify the Source Host Name(s) and IP Address: If the source is external, gather relevant information about the source IP from open online sources:Virustotal.com,abuseipdb.com, ipvoid.com • Source IP: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ If the source is internal, gather the below details: • What type of data is contained on that device? - Devices containing sensitive data (i.e., PII) are a higher priority for remediation. - Does it belong to VIP users? Identify the Destination Host Type: • Workstation or Server (Enterprise, Production, Development) - Are critical services being impacted? • Which Domain does the host belong to? • What is the MAC address? DHCP enabled? 6. Check details of the user who created this task. • If the account is a privilege account, increase the severity. • Search past last 24hrs Azure logs for this user and check, if any other suspicious activities have been done by user in past 24hrs 7. Search for the past 24-hour activities based on the source IP/host and see the trend: • Check for any suspicious activities like connections to known malicious internet hosts, etc. • Check or ask respective team to check AV status for the system where scheduled task was created to confirm if there is any malware or some other infection present in system. 8. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team.
Successful Authentication From Known Suspicious/Malicious IP Addresses	2		1.Check entity details by checking events over sentinel to see what type of traffic is observed using which IP. 2.Examine authentication logs and records to understand which accounts were successfully authenticated and from which IP addresses. 3.Determine why certain IP addresses are labeled as known suspicious or malicious. This could involve checking threat intelligence feeds, security databases, or internal records of past incidents. 4.Evaluate the effectiveness of your current security measures. If successful authentications are occurring from known suspicious IP addresses, it may indicate a weakness in the security controls. 5.Check for reputation of the IP on online databases and if the result is bad reputation, increase the severity of the alert. If the source is external, gather relevant information about the source IP from open online sources:Virustotal.com,abuseipdb.com, ipvoid.com • Source IP: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 6.check signin logs for last 30 days for captured Ip using below kql query: Signin logs | where ip address conatins " x.x.x.x" 7.check any other activities are observed in last 30 days ref: Kql query: Security incident | where ip addess conatins "x.x.x.x" 8.check all necessary tables fro both ip & user by using below kql query for more investigation: serch "Ip address" | distinct $table 9.collect & check data from necessary tables and Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them as a.Please check if this is an authorized activity. b.In case this is an authorized activity, please confirm to find a whitelisting solution. c.In case any vulnerability has been exploited, kindly fix it by a patch. d.If the host/account seems compromised, increase severity. e.If external IP is found to be malicious, block it across perimeter level. • Check if any vulnerabilities associated with the host. If found, fix it with a patch. • Run a full scan with updated AV.

Anomalous login followed by Teams action	2		1.Check user details who performed the activity.
			2.Identify the source of the alert that indicates an anomalous login.
			3.Verify the details, including the user account affected, time of login, and any associated metadata.
			4.Gather initial information about the anomalous login, including user roles, permissions, and recent activities.
			5.Review any contextual information provided by the security monitoring system.
			6.Validate the legitimacy of the anomalous login by comparing it with the user's historical login patterns.
			7.Check for any changes in the user's credentials or access rights.
			8.Initiate an investigation into the user's activity within Microsoft Teams.
			9.Review messages, file transfers, meetings, and any other actions taken within Teams.
			10.Look for signs of unauthorized access, data exfiltration, or other suspicious behavior.
			11.Review Teams audit logs for any unusual configuration changes or permissions modifications.
			12.If the source is external, gather relevant information about the source IP from open online sources:Virustotal.com,abuseipdb.com, ipvoid.com
			• Source IPIf:
			• Source Port(s):
			• Blacklisted Status:
			• ISP:
			• Domain Name:
			• Location of the IP:
			kindly check the reputation of IP using online platforms like :
			https://www.ipvoid.com/ip-blacklist-check/
			https://scamalytics.com/ip
			https://db-ip.com/
			https://mxtoolbox.com/blacklists.aspx
			https://www.virustotal.com/gui/home/search
			https://exchange.xforce.ibmcloud.com/
			https://www.talosintelligence.com/
			https://www.abuseipdb.com/
			https://www.talosintelligence.com/
			13.Check user activity who has been added using below queries:
			Check sign logs & audit logs of the user for suspicious activities.
			SigninLogs
			//put the Actor/target between ""
			| where * has ""
			AuditLogs
			//put the Actor/target between ""
			| where * has ""
			14.check below neccessary tables for more investigation to trace out about suspicious activity:
			Step 1.
			//replace xyz with the username found in alert.
			search "xyz"
			| distinct $table
			With all the table available go through different table where the username is captured using the table name
			Step 2

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps

			//Replace the table name with the table name found in step 1. Repeat for all the tables found in step 1
			TableName
			//use the username between ""
			| where * has ""
			15.Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them as: a.Confirm with the actor who performed this activity to check if this is legitimate
			b.If not, please ask the user to reset the password immediately as we suspect this to be a suspicious attempt.
			c.revoke unauthorized access
			d.Kindly update the ticket accordingly.
			e.if user not responded kindly contact to user's manager.

UC-CA-124 - Azure - Mass secret retrieval from Azure Key Vault	1		1. When SOC team observes a 'UC-CA-124 - Azure – Mass secret Retrieval from Azure Key Vault' alert in Sentinel, it means a user/group/application performed many operations related to get secrets or get key or get vaults in Key vault. 2. Check for any prior notification received or any ticket raised or any ongoing change taking place related to this operation in Azure Environment: • In such case this activity should be considered as legitimate activity. • If not, raise a ticket for this alert and ask for details required for the investigation to proceed. 3. Try to capture the information about the Identity, Key Vaults accessed, count of distinct keys or secrets accessed. 4. Identify the identity associated with this activity and check whether it is authorized to do so. For Example: • The identity can be a user/group/application. The identity id coming in the logs will match with the object IDs of user/group/application. • The identity id should be shared with the client to get information from them on whether this identity is allowed to do so. • Identify if the user/account has any other privileges. • Check if the account had any failed login attempts which could indicate a brute force followed by a compromise of the account. • If any other suspicious activity found, report in the security incident. 5. Check from the logs related to this identity which key vault and what secrets/keys were accessed and if any certificate was also downloaded. 6. Search for past 24 hours' activities based on the Source IP: • Check the reputation of the External IP using online platforms like abuseipdb.com,virustotal.com/mxtoolbox.com • Verify if external IP is allowed to perform such activities. If no, increase the severity. • Identify if that source has tried communicating to our environment before which may linked to Command and Control communications. • Check for communications in the last 7 days. • Check for any other suspicious activity and report in the security incident. 7. Confirm the time of activity. The time Log Analytics Workspace received the event may not be the time the activity occurred. Raise a ticket with concern team to check with user for activities performed.
UC-CA-2202 - UEBA - Anomalous Failed SignIns to Azure Resources	1		1. Check for any prior notification received or any ticket raised or any ongoing change taking place to this operation in Azure Environment. • In such case this activity should be considered as legitimate activity. • If not, raise a ticket for the offense and ask for details required for the investigation to proceed. 2. Try to capture information about the Source IP, Role Assignor, Role Assignee, permission granted. 3. Check Sign-In Patterns: Review the sign-in patterns of the affected accounts. Look for any irregular behavior, such as sign-ins from unfamiliar locations or at unusual times. 4. Account Lockout: Determine if the affected accounts were locked out due to repeated failed sign-in attempts. If so, investigate why these attempts were made. 5. Password Reset: If the failed sign-ins are due to incorrect passwords, consider whether unauthorized individuals are attempting to gain access. Encourage affected users to reset their passwords. 6. Identify the Source Host Name(s) and IP Address: If the source is external, gather relevant information about the source IP from open online sources:abuseipdb.com,virustotal.com/mxtoolbox.com • Source IP: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: If the source is internal, gather the below details: • What type of data is contained on that device? - Devices containing sensitive data (i.e., PII) are a higher priority for remediation. - Does it belong to VIP users? Identify the Destination Host Type: • Workstation or Server (Enterprise, Production, Development) - Are critical services being impacted?

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			• Which Domain does the host belong to? • What is the MAC address? DHCP enabled? 7. Identify the Destination Host Name(s) and IP Address: • What type of data is contained on that device? - Devices containing sensitive data (i.e., PII) are a higher priority for remediation. - Does it belong to VIP users? Identify the Destination Host Type: • Workstation or Server (Enterprise, Production, Development) - Are critical services being impacted? • Which Domain does the host belong to? • What is the MAC address? DHCP enabled? 8. Check details of the user who created this task. • If the account is a privilege account, increase the severity. • Search past 24 hrs/48Hrs. Azure logs for this user and check, if any other suspicious activities have been done by user in past 24hrs/last 48Hrs. 9. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team.
UC-PR-2200 - UEBA - Anomalous Application Management task performed by user	1		1.Check the events captured due to which the incident is triggered. 2.Verify, if necessary, conditions are matched. 3.Check the user, host associated with the Source IP as well as the user location. 4.Check whether the Source IP and location are suspicious using online platforms like abuseipdb.com,virustotal.com/mxtoolbox.com 5.Check the activities performed from the user in last 24 hours. 6.Check for any pre notification received or any ticket raised for activity that could raise this incident. In such case this activity should be consider as an authorized activity and hence can be closed. 7.If no such notification is found, you will need to raise a ticket, to ask for which reasons the user was granted owner access to a Subscription role and ask for details required for the investigation to proceed. 8.Raise a ticket with client to check with user for activities performed.

Excessive Office Delete Operations By a User	1		1.Check the events captured due to which offense is triggered.
			2.Verify if necessary conditions for offense are matched.
			3.Check for any pre-notification received or any ticket raised for this activity.
			4.In such case this activity should be consider as authorized activity.
			5.If no usage notification is found, you will need to raise a ticket for the same offense
			6.Check the username (UserId), who performed this action.
			7.Check if any user was privileged or not. If yes, increase the severity.
			8.Search for the past 30 days for any other suspicious activity from the same username.
			9.check below neccessary tables for more investigation to trace out about suspicious activity:
			Step 1.
			//replace xyz with the username found in alert.
			search "xyz"
			| distinct $table
			With all the table available go through different table where the username is captured using the table name
			Step 2
			//Replace the table name with the table name found in step 1. Repeat for all the tables found in step 1
			TableName
			//use the username between ""
			| where * has ""
			example:
			Officeactivity
			| where username contains "x.x.x.x"
			10.check necessary fields like "authFailureTypes" from the logs and this field indicates exact operation performed by captured user.
			for ex:
			authFailureTypes: "TeamDeleted","ChannelDeleted","DeleteAllOganizationApps"
			11.Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them as: a.Confirm with the actor who performed this activity to check if this is legitimate
			b.If not, please ask the user to reset the password immediately as we suspect this to be a suspicious attempt.
			c.revoke unauthorized access
			d.Kindly update the ticket accordingly.
			e.if user not responded kindly contact to user's manager.

Possible Password Spray Attack	0		1.Check audit logs in AAD to check timestamp when the account was disabled, and any significant account changes happened after that. 2.Check sign in logs in AAD for the user to observe which malicious activity was performed after the account was terminated, see details about type of user account (VIP/Normal/Service Account) IP/Location/Conditional Access Policy Status/Device used.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			3.Validate IP geo-location and reputation of ip address using online platforms like Abuseipdb to check if IP is suspicious and from which country. (https://www.abuseipdb.com),https://www.virustotal.com/https://mxtoolbox.com/ 4.If IP reputation is non-suspicious and user is signing in from expected location using registered/compliant device, check with user/or their manager to see if the user's contract has got extended/recently completed or any other valid reason. If that's the case close the alert has benign positive. 5.If the IP is suspicious and there is no valid reason for terminated user account activity, then close the incident as true positive and raise the request to offboard the MDM registered device from the user account. 6.If no suspicious activity, close ticket with comments 'Investigated via AAD. Failed login against disabled account. No suspicious activity. Closing ticket as Benign Positive'
Suspicious Executable/Script Uploaded via FileUploaded Operation	0		1.Check entity details by checking events over sentinel to see which user uploaded what kind of executable/script using which IP. 2.See incident timeline events to check the azure logs for further details about the user (and its role), IP, File upload operation. 3.Check IP address reputation and location using online platforms like Abuseipdb to check if IP is suspicious and from which country. (https://www.abuseipdb.com),https://www.virustotal.com/https://mxtoolbox.com/ and scan File hash using VirusTotal (https://www.virustotal.com). 4.If the Executable/script looks suspicious validate with the user to understand if its expected script or malicious. 5.If the script is legitimate with valid reason, close the alert as Benign positive 6.If the user denies of running that script or script looks malicious, escalate to L2/L3 for further investigation or escalate it to concern team.
Correlate Unfamiliar sign-in properties and atypical travel alerts	0		1.Go to abuseipdb website and check the IP & location where the performed sign in activities came from online platforms like https://www.abuseipdb.com),https://www.virustotal.com/https://mxtoolbox.com/ and scan File hash using VirusTotal (https://www.virustotal.com).Also compare it with previous sign-in IP & location. 2.Check in AAD (Azure Active Directory) sign-in logs of the user to see whether activity originated outside of the user's standard login location and how long before a login was noticed from their normal location. 3.Check AAD sign-in logs of the user to observe the sign-in pattern: Device type and its compliance status, Application signing into, Access Conditional Access Policy status (MFA). 4.If the location is unexpected(based on previous user details,past 30 days activity) confirm with the user if they are travelling or using VPN/Jumphost. 5.If the user validates the reason for sign-in from that location, then close the alert as Benign positive. 6.If the user denies of sign-in from that location, then reset password and escalate to L2/L3 security member or concern team for further investigation.Check the reputation for all the Client IPs: https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/
Multiple Password Reset by user	0		1.Check AAD audit logs for user to see details of password reset activity performed, which account did it. 2.Check AAD sign-in logs of the user to see if any suspicious sign-in attempts/successful log-ins. 3.Check OKTA_CL logs of the user to see if any suspicious sign-in attempts/successful log-ins/user activity. 4.Check the source IP reputation and location to see if its suspicious. (https://www.abuseipdb.com/) Check the reputation for all the Client IPs: https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ 5.If suspicious events found, confirm with user if activity was performed by them. If user confirms, close the alert as benign positive. 6.If the user denies of performing password reset, then revoke user sessions, add the malicious IP to Threat Intelligence - (IOC), and escalate to L2/L3 security member for further investigation or Concern team.
Intrusion Attempts Targeting a Sensitive Web Application Detected	0		1.Check IP location and reputation in Abusedb/Cisco Talos Reputation Center to check if IP is flagged as malicious. (https://www.abuseipdb.com) 2.Check the Azure Diagnostics (sentinel logs) by running KQL query selecting the "Time range" matching with alert timeline, to find out outcome of the malicious

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			web requests made by the IP flagged in the alert. AzureDiagnostics | search "IP" | summarize count()by TimeGenerated, Message, requestUri_s, httpMethod_s, httpStatus_d, client_ip_s, host_s, ResourceGroup, WAFMode_s, serverStatus_s, action_s, details_message_s, originalHost_s 3.Check targeted resource groups ("host_s" or "originalHost_s"), requested uri, web request methods (Put,Post,Get,Delete) used and header to see if any malicious activity has been observed or not, if observed Notify the team to take necessary actions. 4.Check the Http status codes for the requests in the logs. If the http status codes are 300s or 400s or 500s, then the confidured WAF has detected/matched/blocked the web requests coming out of that IP. If the requests were blocked close the alert as True positive (If IP is malicious) or False Positive (If IP is not malicous). 5.If the Http status codes is 200 success codes, then need to investigate further about which host is affected, if any sign-ins, inbound/outbound traffic is seen coming out of that malicious IP and for how long. 6.If activity is determined malicious, escalate to L2/L3 Security Analyst. Get the IP blocked by adding them in NSG and update malicousIPWatchlist by adding the malicous IP flagged in the alert.
First access credential added to Application or Service Principal where no credential was present	0		1.Check entity details from events over sentinel to see which user account performed the action on which application. 2.See incident timeline to check the azure logs for further details about the user and if he is having administrator role, application name, IP address using which user added credentials to the application. 3.Check IP address reputation and location (https://www.abuseipdb.com) Check the reputation for all the Client IPs: https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 4.Review audit log of account activity by checking the time of the alert in AAD to see if activity is expected BAU activity or suspicious. 5.If the activity looks suspicious validate with the user. 6.Check for any prior notification received or any ticket raised or any ongoing change taking place related to this operation in Azure Environment: • In such case this activity should be considered as legitimate activity. • If not, raise a ticket for this alert and ask for details required for the investigation to proceed.
Account Created and Deleted in Short Timeframe	0		1.Click on "Events" or go and check under "Incident Timeline" to see the logs related to this incidents and entities involved. 2.Investigate further in AAD audit logs, about account creation & deletion done by which actor and timestamp. For checking the deleted account details, go to AAD-Users-Deleted Users tab. 3.Confirm with the actor who performed this activity to check if this is legitimate 4.If the user confirms of performing this activity or you can search the deleted account name in Servienow portal to see if any such request came for deleted account user. If this is expected activity, close the alert as Benign positive. 5.If the user don't confirm and activity is suspicious , escalate to L2/L3 for futher investigation and close as True Positive if activity was found malicious after investigation.
Okta user changed their MFA method or password from a different country	0		1.Check Overview Blade, Link To La and read KQL logs. 2.Collect the deatils: Check country_of_okta_activation, eventType_s and actor_alternateId_s from events or KQL logs over sentinel. 2.Identify the IP address(s) form which the user have been logged in 3. Check the reputation of the external IP on various online tools. kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ and Also, check the IP belongs to which country. 4.Go to AD Entra look up user. Look in Overview, check Account status and sign in logs. If from approved employee working abroad (investigate approval in ServiceNow by looking up user id and user details), close ticket as Benign Positive. 5.If not approved to work abroad, lodge ticket to temporarily disable account after consulting with L2/L3 Security/respective resolver group.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
UC-IM-122 - Azure - Large Number of Virtual Machines Deleted	0		1. Identify attack methodology, • Attack vector: § Did the machines were in use before it got deleted? § Were the machines infected with a malware before deletion? § Is the source doing this activity compromised? § Is the Microsoft Azure account doing this activity compromised? 2.Check for any prior notification received or any ticket raised or any ongoing change taking place related to these operations in Azure Environment: • In such case this activity should be considered as legitimate activity. • If not, raise a ticket for the offense and ask for details required for the investigation to proceed. 3. Identify all the machines and capture: • What type of data is contained in all the machines? § Why were these machines connected to each other? 4. Identify which Microsoft Azure user has performed this activity. • Is the user who has performed this activity the admin? 5. If the user is non admin, collect the below information about the user accounts who deleted the machine connection: • Role of the user • Get user or service account owner's full name • Group membership, account history, notes • Was this account associated as a service account? 6. Confirm the time of deletion. The time SIEM received the event may not be the time the activity occurred. 7. Search for past 5–15-day/30 days events for the deleted application connection and see the trend: • Check for all the user having admin rights of deleting the connection or not. • Check if any VM was still connected before it got deleted. • Check if any VM got added to this connection recently or not. 8. Based on the above information, if the activity seems to be suspicious, escalate it to the concerned team.
UC-DE-128 - Azure - Network Security Group was Deleted	0		1. Identify the attack methodology • Attack vector: • Did user delete one Network security group? • Did user delete multiple Network security group? • Did multiple user delete network security group? KQL query: AzureActivity |where OperationName == "Microsoft.Network/networkSecurityGroups/delete" | where ActivityStatusValue == "Success" 2. Identify the User Account(s) from events who has performed this action. • Was this account associated as a Service account? • If a service account? Who is the owner of the service account? 3. Identify which Network security group was deleted. 4. Check all the activity done by the source user in past 30 days. a. Attempt to gather relevant information about the subject user: • Role of employee or partners involved (Executive, etc.) • Search Active Directory Users and Computers: a.)Get employee or service account owner's full name b.) Group membership, account history, notes c.) Lookup contact information, review role. b. Mentioned below all the activity done by source user • Any other Network security group was deleted. • Any Network security group was created • Any Network security group was modified like (any SRC, DST were added. Or any action was changed (Allow, Deny)). c. Check if there was spike in traffic after deletion of this group. d. Mentioned if any other suspicious activity was observed. 5. If this activity was legitimate, check there was proper approval or ticket raised for this activity. 6. If this activity was malicious then please raise a ticket with respective resolver Group/L3
UC-PE-1617-Bulk Changes to Privileged Account Permissions	0		1. Identify the Source User Account who did this activity. Using KQL queries: Azure Audit Logs | where * has "useraccount" • Was this account associated as a Service account? If a service account, who is the owner of the service account? 2. Check the past 30 days logs based on the source account and check all the activity done by the account. • Is this only account for which Bulk changes of account permissions had happened? • Is this event has been observed before in the past 20 days logs? • Check for the other suspicious event like account added to privilege group, account removal from privilege group, attempt to change the password etc. • Did this account attempt to login on other systems? 3. Identify the Privileged Account for which Bulk changes of Account permissions happened. • Was this account associated as a Service account?

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			If a service account, who is the owner of the service account? • Check all the activities done by the account after permissions changes. 4. Check the past 30 days logs based on the targeted host. • Note down the list of changes happened to the privilege account. • Investigate on the changes get the details of who performed the activity and whether they do have required permissions to do so. 5. If the analysis gives sufficient proof that the user performing this activity has been compromised or performing not allowed activity or If this activity is not legitimate, then raise ticket with respective resolver group and it should be recommended to disable the account for the time being/During the initial phase of the analysis, if it seems like the activity could be benign but still suspicious, recommend to at least change the password of the account performing this activity.
UC-PR-1620-User Assigned Privileged Role	0		1. Identify the Initiator and try to find out the details of the account, who did this activity using Azure Audit logs table. KQL Query: Auditlogs | where userprinciple name contains "username". • Was this account associated as a Service account? • If a service account? Who is the owner of the service account? 2. Identify in which role destination user was added. 3. Did destination user was added into multiple role? 4. Check all the activity done by the source in past 30 days. 5.Check for any received pre notification or any raised ticket for activities that could lead to such an alert. In this case, this activity should be considered as an authorized activity 6. Identify the Target and try to find out the details of the account. • Was this account associated as a Service account? • If a service account? • Who is the owner of the service account? 7. Check the last 30 days logs based on the destination user. 8.. Check for the date and time when that was added to privilege group. 9. Check all the activity performed by the user after added to privilege group. 10. after further investigation anything seems suspicious then raise a ticket with concern team/L3 and Mention if any other suspicious activity was observed.
UC-CA-1788-Permutations on logon attempts by UserPrincipalNames indicating potential brute force	0		1. Identify source IP associated with this activity. • Check if the IP is internal/external. In case of External IP, check for reputation of the IP on online databases: Check the reputation for all the Client IPs: https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ and if the result is bad reputation, increase the severity of the alert. • In case of internal IP, check if there has been any activity happening from this IP in past 30 days/60 days. 2. Check the User/Account related to this activity. • Check if any user was privileged or not. If yes, increase the severity. • Check if the timestamp for successful login was seen after the failed attempts only and not in between. If yes, increase the severity. 3. Check with respective team for AV reports of source system (in case of internal IP) and check if any risk was detected on system in past 30 days. 4. Search for past 24 hrs/30 days logs based on source IP and check, • If any other suspicious activity is detected from same source IP 5. Search for past 24 hr logs based on User/Account and check, • If this user has tried to login from multiple locations. • If this user has had a high number of failed logins in the recent past with no successful logins. • If this user committed any activity after the triggering of this alert that is suspicious or critical. 6. Develop historical context associated with the machine. For example, does this machine have a history of lockouts or malware infections, has the machine generated alerts that were not sent to SIEM tool. 7. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team.
UC-DE-2105-Creation of expensive computes in Azure	0		1. When SOC team observes a 'UC-DE-2105-Creation of expensive computes in Azure' alert in Sentinel, it means a expensive VM's are been created in azure. Definition: "expensive computes in Azure" is used, it generally refers to the deployment and utilization of high-cost computing resources within Microsoft Azure, a cloud computing platform. Azure offers a variety of virtual machines (VMs) and other computing resources with different specifications and performance levels, and the cost associated with these resources varies accordingly.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			2. Check for any prior notification received or any ticket raised or any ongoing change taking place related to this operation in Azure Environment: • In such case this activity should be considered as legitimate activity. • If not, raise a ticket for this alert and ask for details required for the investigation to proceed. 3. Determine the Azure subscription(s) and resource group(s) where the expensive compute resources were created by checking azure activity Table. 4. Determining the reason for the creation of expensive compute resource. 5. If unauthorized activity is confirmed, take immediate containment measures, such as: • Disabling or deleting the impacted compute resources. • Revoking privileges of unauthorized users. • Resetting compromised credentials. 6. Collaborate with relevant teams to address any misconfigurations or issues leading to the creation of expensive resources. 7. Check for any other suspicious activity and report in the security incident with this caller or caller IP. 8.Kindly check if the user performed similar/related activities in last 30 days over sentinel. 9. Confirm the time of activity. The time Log Analytics Workspace received the event may not be the time the activity occurred. Raise a ticket with client to check with user for activities performed and kindly recommend them to : * Please check if this creation is an authorized activity. * Please check and correct if this creation is happened due to wrong configuration/script. * If any vulnerability seems to be exploited, raise the severity. * If user seems to be involved with this activity. Raise user awareness explaining the consequences of creation of such expensive VM's. * Run complete AV Scan on the source host. * Please update the ticket accordingly.
UC-CA-117 - Azure - Azure Key Vault access TimeSeries anomaly	0		1. When SOC team observes a 'UC-CA-117 - Azure - Azure Key Vault access TimeSeries anomaly' alert in Sentinel, it means a sudden increase in count of Azure Key Vault secret or vault access operations by CallerIPAddress 2. Check for any prior notification received or any ticket raised or any ongoing change taking place related to this operation in Azure Environment: • In such case this activity should be considered as legitimate activity. • If not, raise a ticket for this alert and ask for details required for the investigation to proceed. 3. Note the Operation Name fields to identify any unusual requests or operations. 4. If malicious activity is confirmed, take appropriate containment measures to prevent further damage. This may include resetting credentials, isolating affected systems, or blocking malicious IP addresses. 5. Check the reputation of the External IP using online platforms like : Check the reputation for all the Client IPs: https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ • Verify if external IP is allowed to perform such activities. If no, increase the severity. • Identify if that source has tried communicating to our environment before which may linked to Command and Control communications. • Check for communications in the last 30 days. 6. Check for any other suspicious activity and report in the security incident. 7. Confirm the time of activity. The time Log Analytics Workspace received the event may not be the time the activity occurred. Raise a ticket with concerned team to check with user for activities performed.
UC-IM-139 - Azure - Sensitive Azure Key Vault operations	0		1. When SOC team observes a 'UC-IM-139 - Azure – Sensitive Azure Key Vault operations' alert in Sentinel, it means any operations among the following – 'SecretDelete', 'SecretPurge', 'VaultDelete', 'KeyDelete', 'KeyPurge', 'SecretBackup', 'KeyBackup' has happened in Azure Environment. Hence this incident needs to be investigated on priority basis. 2. Check for any prior notification received or any ticket raised or any ongoing change taking place related to these operations in Azure Environment: • In such case this activity should be considered as legitimate activity. • If not, raise a ticket for the offense and ask for details required for the investigation to proceed. 3. Try to capture the information about the UPN of the account, Operation Name, Source IP, identity ID, Key Vault Name (Resource) from the events over sentinel or use Azure keyvault and Azure diagnostics tables. 4. The key/secret on which the operation was performed can be found out checking the id_s column in the event related to the alert. The last value in the field will give the name of the key/secret on which the action was performed. 5. The operation name values that have triggered the alert should be identified. This information can be obtained from the event logs related to this alert in the

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			column OperationNameList. 6. Identify the User/identityID associated with this activity and search for various activities performed by the User. For Example: a. Check all details of this user from Azure Active Directory. b. Check the privileges assigned to the account. c. Check if the account had any failed login attempts which could indicate a brute force followed by a compromise of the account. d. Search for the various activities being performed by the user towards same key vault resource. e. If any other suspicious activity found, report in the security incident. 7. Search for past 30 days activities based on the Source IP: a. If the source IP is not internal, check the reputation using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ b. Verify if the IP is allowed to perform such activities. If no, increase the severity. c. In case of External IP, check if it has tried communicating to our environment before which may be linked to Command and Control communications. d. Check for communications in the last 30 days. e. Check for any other suspicious activity and report in the security incident. 8. Confirm the time of activity. The time Log Analytics Workspace received the event may not be the time the activity occurred. Raise a ticket with concerned team to check with user for activities performed
UC-CC.EF-382 - Proxy - Large Outbound Transfer High Rate of Transfer	0		1. Check the events captured from events part over sentinel due to which the incident is triggered. 2. Check for any pre-notification received or any ticket raised for transfer of data. - In such case this activity should be consider as authorized activity. - If no usage notification is found, you will need to raise a ticket and ask for details required for the investigation to proceed. 3. Check event payload and identify source IP, destination IP, destination port, rate of data transfer and check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 4. Check source IP from which data transfer was initiated and identify internal host associated with this IP. - Check if source host is a workstation or server - What type of data is present on this device 5. Search for past 30 days activity based on destination source host/IP. - Check if source host contains any sensitive information - Analyze all connection from same source IP to same destination IP in past few days and check if any reverse traffic was observed. - Identify port used for data transfer - From how long data transfer is going on - Identify user who was logged in to source host around time of this activity - Check if user have accessed any sensitive data and if that data has been copied or uploaded or transferred. - If any other suspicious activity is detected on same host in past few days 6. Also check for AV status of source Host to see if any risk has been detected on this host in past 30 days. 7. Identify destination IP towards which data transfer is observed and get all details of this IP from online sources. Also check for reputation of destination IP address from mentioned online platforms 10. Check past 30 days activity based on destination IP and check if any other suspicious activity is detected from same IP address. 11. Raise a ticket with respective group to check with user for activities performed.
UC-EF-1994 - Proxy - Large Inbound Transfer High Rate of Transfer	0		1.Check the events captured from events part over sentinel due to which the incident is triggered. 2. Verify, if necessary, conditions for alerts are matched. 3. Check for any pre-notification received or any ticket raised for transfer of data. • In such case this activity should be consider as authorized activity. • If no usage notification is found, you will need to raise a ticket and ask for details required for the investigation to proceed.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			4. Check event payload and identify source IP, destination IP, destination port, rate of data transfer and check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 5. Check source IP from which data transfer was initiated and identify internal host associated with this IP. • Check if source host is a workstation or server • What type of data is present on this device 6. Search for past 30 days activity based on destination source host/IP. 7. Check if host contains any sensitive information 8. Analyze all connection from same source IP to same destination IP in past few days and also check if any reverse traffic was observed. • Identify port used for data transfer • From how long data transfer is going on • Identify user who was logged in to host around time of this activity 9. If any other suspicious activity is detected on same source in past 30 days 10. Also check for AV status of destination Host to see if any risk has been detected on this host in past 30 days. 11. Identify destination IP towards which data received is observed and get all details of this IP Using KQL queries(): Proxy logs. 12. Check past 30 days activity based on destination IP and check if any other suspicious activity is detected from same IP address. 13. Refer to the CMDB information, such as the function of the servers and the location where they are hosted and determine the severity based on urgency and impact 15. Raise a ticket with concerned team to check with user for activities performed.
UC-IM-2106 - TI Map IP Entity to KeyVault	0		1. Identify the attack methodology: • Search for past 24hrs activity based on the external source IP and check: - The Critical ports that have been targeted. - Type of traffic observed from this particular source and frequency of the connections and if those are accepted or dropped. - Any reverse connection observed towards this source and if its accepted or dropped. Kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 2. Identify the targeted Service(s): • What type of data is contained on that application? - Devices containing sensitive data (i.e. PII) are a higher priority for remediation 3. Check for any received pre notification or any raised ticket for activities that could lead to such an alert. In this case,It will be helpful for further investigation. 4. If user found, then Attempt to gather relevant information about the subject user. Like • Role of employee or partners involved (Executive, etc.) • Search Active Directory Users and Computers: a.Get employee or service account owner's full name b.Group membership, account history, notes c.Lookup contact information, review role 5. Analyze the access logs of the KeyVaults to determine who has accessed or modified the IP entities. Ensure that access is limited to authorized personnel only. 6. Check for any unusual patterns or anomalies in the access logs that might indicate unauthorized access attempts or suspicious activities. 7. Evaluate the configurations of the KeyVaults associated with the IP entities. Check if the access controls, encryption settings, and auditing mechanisms are correctly implemented according to the organization's security standards. 8. Cross-check the IP-to-KeyVault mapping records against the actual configuration of KeyVaults and the IPs themselves. Ensure there are no discrepancies or errors in the mapping. 9. Verify whether the mapping process complies with the organization's security policies, data protection regulations, and industry best practices 10. Based on the above information, if the activity seems to be suspicious, create a ticket/security incident and assign it to the concerned team.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
UC-CC-2107-TI Map IP Entity to Azure WAF	0		1. When SOC team observes a “UC-CC-2107-TI Map IP Entity to Azure WAF” alert in Sentinel, it should be treated on priority because it plays a crucial step in identifying unusual and suspicious behaviors within the network that can lead to exploitation. 2. Check for any pre-notification received or any ticket raised that could trigger this alert. a. In such case this activity should be consider as authorized activity. b. If no notification is found, you will need to raise a ticket for the same alert 3. Check the events captured due to which alert is triggered. 4. Verify if necessary, conditions for alert is matched. 5. Check the details and reputation of the external source IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the source IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 6. Take a detailed look at the IPs in the alert trigger. This can help you understand the behaviour and help analyses if it is suspicious or not. https://ipinfo.info/html/tcp-ip-ports.php 7. Search for past Last 30 Days activity based on the external source IP and check: • The Critical ports that have been targeted. • Type of traffic observed from this particular source and frequency of the connections and if those are accepted or dropped. • Any reverse connection observed towards this source and if its accepted or dropped. 8. Gather the targeted host(s) details from the database: • What kind of data is contained on that device? • Is there any sensitive data (i.e. PII)? • Check the host details (like host is a server, desktop or laptop). And also collect other information (like domain, location, assigned to, etc) 9. Search for past 30 Days activity based on the targeted IP(s) and check the activities done by it and if those seems suspicious or not. 10. Check for other suspicious activities observed around the time of the alert. 11. Confirm the time of activity. The time SIEM tool received the event may not be the time the activity occurred. 12. Based on the above information, if the activity seems to be suspicious then escalate to respective resolver groups for further investigation and close as True Positive.
UC-CA-2108-TI Map IP Entity to Dynamics 365	0		1. When SOC team observes a “UC-CA-2108-TI Map IP Entity to Dynamics 365” alert in Sentinel, it should be treated on priority because it plays a crucial step in identifying unusual and suspicious behaviors within the network that can lead to exploitation. 2. Check for any pre-notification received or any ticket raised that could trigger this alert. a. In such case this activity should be consider as authorized activity. b. If no notification is found, you will need to raise a ticket for the same alert 3. Check the events captured due to which alert is triggered. 4. Verify, if necessary, conditions for alert is matched. 5. Check the details and reputation of the external source IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the source IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 6. Take a detailed look at the IPs in the alert trigger. This can help you understand the behaviour and help analyses if it is suspicious or not. https://ipinfo.info/html/tcp-ip-ports.php 7. Search for past last 30 days activity based on the external source IP and check: • The Critical ports that have been targeted. • Type of traffic observed from this particular source and frequency of the connections and if those are accepted or dropped. • Any reverse connection observed towards this source and if its accepted or dropped. 8. Gather the targeted host(s) details from the database: • What kind of data is contained on that device? • Is there any sensitive data (i.e. PII)? • Check the host details (like host is a server, desktop or laptop). And also collect other information (like domain, location, assigned to, etc) 9. Search for past last 30days activity based on the targeted IP(s) and check the activities done by it and if those seems suspicious or not. 10. Check for other suspicious activities observed around the time of the alert. 11. Confirm the time of activity. The time SIEM tool received the event may not be the time the activity occurred.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			12. Based on the above information, if the activity seems to be suspicious then escalate to respective resolver groups for further investigation and close as True Positive.
UC-IM-2109-TI Map IP Entity to Office Activity	0		1.The initial step is reviewing the TI feed for any flagged IP addresses that seem suspicious. This could be based on multiple factors such as previous malicious activity, geolocation, or other threat intelligence indicators. 2.Check the details and reputation of the external source IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the source IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 3.Review Okta system logs for any activity linked to the flagged IP addresses. Look for irregular patterns like multiple failed logins, suspicious user creation or privilege escalation, or abnormal usage patterns. 4.If any activities linked to the flagged IPs are found, investigate the user accounts involved. Check for any unusual behavior like suspicious access to sensitive resources or abnormal user behaviors and also check If the involved user account exists in AD/AAD then kindly raise ticket and ask them to check about user activity/reason behind this activity 5.Review session logs from the suspicious IP for last 30 days. This can include timing, duration, accessed applications, and authentication methods used. 6.If the above steps reveal abnormal behaviors or signs of compromise, it is necessary to confirm the incident, then escalate to respective resolver Group/L3 for further investigation and close as True PositiveIf the above steps reveal any abnormal behavior or signs of compromise, confirm the incident, assess the impact, and determine the scope of the compromise. 7.Mention in recommendations Depending on the impact, you might need to isolate affected systems, deactivate or reset compromised accounts, or initiate other recovery procedures.
UC-CA-2110-TI Map IP Entity to Okta	0		1.The initial step is reviewing the TI feed for any flagged IP addresses that seem suspicious. This could be based on multiple factors such as previous malicious activity, geolocation, or other threat intelligence indicators. 2.Check the details and reputation of the external source IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the source IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 3.Review Okta system logs for any activity linked to the flagged IP addresses. Look for irregular patterns like multiple failed logins, suspicious user creation or privilege escalation, or abnormal usage patterns. 4.If any activities linked to the flagged IPs are found, investigate the user accounts involved. Check for any unusual behavior like suspicious access to sensitive resources or abnormal user behaviors and also check If the involved user account exists in AD/AAD then kindly raise ticket and ask them to check about user activity/reason behind this activity 5.Review session logs from the suspicious IP for last 30 days. This can include timing, duration, accessed applications, and authentication methods used. 6.If the above steps reveal abnormal behaviors or signs of compromise, it is necessary to confirm the incident, then escalate to respective resolver Group/L3 for further investigation and close as True PositiveIf the above steps reveal any abnormal behavior or signs of compromise, confirm the incident, assess the impact, and determine the scope of the compromise. 7.Mention in recommendations Depending on the impact, you might need to isolate affected systems, deactivate or reset compromised accounts, or initiate other recovery procedures.
UC-CA-2111-TI Map IP Entity to Windows Events	0		1. The initial step is reviewing the TI feed for any flagged IP addresses that seem suspicious. This could be based on multiple factors such as previous malicious activity, geolocation, or other threat intelligence indicators. 2. Review the Windows event logs for any activity linked to the flagged IP addresses. we need to pay special attention to Security, System, and Application event logs. Look for any unusual or suspicious patterns such as repeated failed logins, access attempts to sensitive resources, or software installation attempts. 3.Check the details and reputation of the external source IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the source IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 4.If any activities linked to the flagged IPs are found, investigate the user or system accounts involved. Check for any unusual activities such as sudden changes in privileges or unusual account behavior and also check If the involved

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			user account exists in AD/AAD then kindly raise ticket and ask them to check about user activity/reason behind this activity 5. Look at your network traffic logs for last 30 days to see if the flagged IP addresses are associated with an unusual volume of data transfer, are connecting on unexpected ports, or are involved in any other suspicious network behavior. 6. Check the process and system events associated with the flagged IP addresses. Look for signs of malicious process execution, suspicious software installations, or unusual system changes. 7. If the above steps reveal abnormal behaviors or signs of compromise, it is necessary to confirm the incident, then escalate to respective resolver Group/L3 for further investigation and close as True Positive
UC-IM-2114 - TI Map Domain Entity to Zscaler	0		1.The initial step is reviewing the TI feed for any flagged IP addresses that seem suspicious. This could be based on multiple factors such as previous malicious activity, geolocation, or other threat intelligence indicators. 2.Review Zscaler logs for last 30 Days to know any activity linked to the flagged domains. Look for patterns like users accessing the flagged domains, repeated blocked requests, or large amounts of data transfer to/from the domains. 3.Check the details and reputation of the external source IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the source IP address and domain reputation on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 4.If any activities linked to the flagged domains are found, investigate the user accounts involved. Check for unusual behaviors like attempted security bypass or repeated access to flagged domains and also check If the involved user account exists in AD/AAD then kindly raise ticket and ask them to check about user activity/reason behind this activity 5.Analyze your network traffic logs for alst 30 Days to see if the flagged domains are sending or receiving an abnormal volume of data, or if there are connections to unusual ports or services. 6.Review your Zscaler security policies to ensure they are properly configured to block potentially malicious activities. Check if any policy violations have been detected from the flagged domains. 7. If the above steps reveal abnormal behaviors or signs of compromise, it is necessary to confirm the incident, then escalate to respective resolver Group/L3 for further investigation and close as True Positive
UC-CO.EF-521 - O365 - Mail redirect via ExO transport rule	0		1. Check the source IP/IPs involved in the activity. a. If the source is external, gather relevant information about the source IP from open online sources: • Source IP: • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: 2. Check the details and reputation of the external source IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the source IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 3. Check for past 30days' logs for any suspicious activity performed from the same Source IP. 4. Check the username (UserId), who performed this action and also check If the involved user account exists in AD/AAD then kindly raise ticket and ask them to check about user activity/reason behind this activity a. Check if any user was privileged or not. If yes, increase the severity. b. Search for the past 30 days logs for any other suspicious activity from the same username. 5. Check the payload for the parameter "BlindCopyTo" OR "RedirectMessageTo" to get the details of the recipient/recipients. 6. Check the Originating Server Name and IP address. 7. Check the payload based on the logs to get some more relevant information. 8. Check if any emails are forwarded to that address or not. a. If yes, does that email contains any sensitive information or not. b. If yes, increase the severity. 9. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team.
UC-PE.DE-522 - O365 - Malicious Inbox Rule	0		1.Check the source IP involved in the activity. 2.If the source is external, gather relevant information about the source IP from open online sources:Virustotal.com,abuseipdb.com, ipvoid.com • Source IP: • Source Port(s): • Blacklisted Status:

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			• ISP: • Domain Name: • Location of the IP: kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 3.Check for past 30 days logs for any suspicious activity performed from the same Source IP. 4.Check the username (UserId), who performed this action. a. Check if any user was privileged or not. If yes, increase the severity. b. Search for the past 30 days for any other suspicious activity from the same username using kql query: security incident | where username contains "abcde " 5.Check the Originating Server Name and IP address. 6.Check the keyword specified in any of “SubjectContainsWords”,” BodyContainsWords”, “SubjectOrBodyContainsWords” field in the payload . 7.Check if the specified keywords/ phrase contain any of (helpdesk, alert, suspicious, fake, malicious, phishing, spam, do not click, do not open, hijacked, fatal etc.) 8.Check the payload to get more information on any other parameter specified like “ForwardTO”, “MoveToFolder”, “StopProcessingRules” etc. 9.Check if any incident of phishing or spam mails are observed in the organization before this rule got triggered, this could indicate intrusion of attacker in the organization. 10.Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them : a. Check with the client if this was an authorized activity or not. b. Check with the client the user who performed this activity is authorized to do that or not. c. If yes, check with that user if he has performed that action or not. d. If yes, then close the ticket with no risk. e. Else, ask the user to change its account credential as account might be compromised. f. Else, delete those inbox rule ASAP and ask SOC team to do the further investigation. g. If source IP if external and malicious, ask the client to block that IP. h. Please update the ticket accordingly.
UC-PE-1138 - O365 - O365_SharePoint anti-virus engine detects malware in a file	0		1.Identify source IP associated with this activity. 2.Check if the IP is internal/external. In case of External IP, check for reputation of the IP on online databases and if the result is bad reputation, increase the severity of the alert. 3.Check the details and reputation of the external source IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the source IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 4.In case of internal IP, check if there has been any activity happening from this IP in last 30 days 5.Find out if the given infected file has been downloaded by any user. Although, Sharepoint won’t allow to download such a file as soon as it is tagged as an infected file. 6.Check the User/Account related to this activity. a.Was this account associated as a Service account? If a service account,check who is the owner of the service account with L2/L3. 7.The given link has more info on procedure followed by Virus engine before and after scanning the file: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection-for-spo-odfb-teams-about?view=o365-worldwide 8.The file should be removed soon from sharepoint and it should be found out as to what were the origins of such file. 9.Develop historical context associated with the machine. For example, does this machine have a history of lockouts or malware infections, has the machine generated alerts that were not sent to SIEM tool. 10.Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
UC-IA-1429 - Office 365 - User Added as Site Admin to Multiple Sites	0		1.Identify the user who performed the action from the events over sentinel. • Check whether this user should be able to perform such operations ie. Does he/she have the rights on policies? • Check with the user if the operation was done deliberately. 2.If he/She user should not have been able to perform the operation or the user mentioned that it was not done by him/her, check on the SIEM for privilege escalation related offenses/events. • Check users added to which sites and list out the multiple sites. 3.Check for any pre-notification received or any ticket raised that could trigger this alert. a. In such case this activity should be consider as authorized activity. b. If no notification is found, you will need to raise a ticket for the same alert 4..Identify the IP address (source IP) used in this process. • Check the details and reputation of the external source IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the source IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 5.Check other users who are linked to this IP address using the SIEM log search for last 30 days. 6.Check the Audit policy which was deleted/changed/cleared in the logs - • Identify the significance of the Audit policy or try to understand what it does as the policies are named like that. Try to understand using the naming convention of the policies. • Check last 30 adys logs if the user has performed other actions which resulted in any additional offenses. 7.Search for past 30days logs based on source IP and check, • Any other offense or logs from the same source IP? • Any other user tried to login using the same source IP? Possibility of brute force attack. 8.Develop historical context associated with the machine. For example, does this user have a history of lockouts or suspicious activities? The user done actions for which logs were not sent to SIEM tool. 9. Based on the above information, if the activity is suspicious, create a ticket using the ticketing tool and assign it to the concerned team.
UC-DE-416 - Linux - Clear command history detected	0		1.Here are the procedures an Analyst should follow to determine root cause of this activity: A. Identify the attack methodology: • Attack vector: - Command history cleared. - Activities performed by the source host - Account used to clear the command history B. Identify the Source Host Name(s) and IP Address from the events part over sentinel. If the source is external, gather relevant information about the source IP from open online sources: • Source IP: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP and Check the source IP address reputation on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ If the source is internal, gather the below details: • What type of data is contained on that device? - Devices containing sensitive data (i.e. PII) are a higher priority for remediation - Does it belong to VIP users?(VIP Users: A list of user accounts/employees that have high impact value in the organization.) C. Identify the Destination Host Name(s) and IP Address: • What type of data is contained on that device? - Devices containing sensitive data (i.e. PII) are a higher priority for remediation - Does it belong to VIP users? Identify the Destination Host Type: • Workstation or Server (Enterprise, Production, Development) - Are critical services being impacted? • Which Domain does the host belong to? D. (If the Analyst have access to User DB) Collect the below information about the user who cleared the command history: • Search below details about the user: - Role of employee - Get employee or service account owner's full name - Group membership, account history, notes

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			- Lookup contact information, review role If Not kindly raise a ticket with respective Group and ask them to check on these details. E. Confirm the time when the command history was cleared. The time SIEM received the event may not be the time the activity occurred. F. Search for the last 30 days activities based on the source IP and see the trend: - Check if the source host has history of suspicious activity like connection to known malicious hosts, etc. - Check if any suspicious traffic was observed to and from the source host which could compromise the host. G. Search for the past 30 days activities based on the source user who cleared the command history and see the following: - Check if the user has history of suspicious activity like connection to known malicious hosts, etc. - Check if the account has any activities that could lead to compromise the account. - If possible, check what commands were cleared and try to identify if it can affect something. H. Also check if the source (if internal) and destination hosts are updated with AV or not and check if it has had any infection history. I. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team.
UC-CA-437 - Linux - Multiple Login Failures One Source - Multiple Destinations - Root Account	0		1. When SOC team observes a 'UC-CA-437 – Linux -Multiple Login Failures One Source – Multiple Destinations – Root Account' alert in Sentinel, it means Multiple login failures have been observed for any number of user accounts from one source IP towards any number of destinations. 2. Check the events captured due to which the alert is triggered. 3. Verify if necessary conditions is matched. 4. Identify the Source IP Address from the events part over sentinel. If the source is external, gather relevant information about the source IP from open online sources: • Source IP: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP and Check the source IP address reputation on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 5. Gather the Source IP/host details from the database: What kind of data is contained on that device? - Is there any sensitive data (i.e. PII)? - And also collect other information (like domain, location, assigned to, etc.) 6. Search for past 30days activity based on the destination user(s) and see the following: - If we observed the "authentication failure", the failed authentication can happen on the device host name from the destination host name (or) destination address. 7. check with the device process name to check what type of connection was registered. - If we observed the "failed password", the failed authentication can happen on the destination host name (or) address from the source host name (or) source address. - Check, since when these login failures are happening? - Is there any successful login observed? 8. Search for past 30Days. activity based on the source host/IP and check the activities done by it and if those seems suspicious or not. 9. Also identify the user connected to the source machine and check for the past 30days activity by the user and if its suspicious or not. 10. Ask for details required for the investigation to proceed. 11. Check for other suspicious activities observed around the time of the alert
UC-DE-1038 - Linux - Log Deletion Attempt	0		A. Identify the user who performed the action. • Check whether this user should be able to perform such operations i.e. Does he/she have the rights on that resource configurations? • Check with the user if the operation was done deliberately. B. If the user should not have been able to perform the operation or the user mentioned that it was not done by him/her, check on the SIEM for privilege escalation related offenses/events. C. Identify the IP address (source IP) used in this process. • Check the role of IP if it is internal. • Check he reputation of the IP address for malicious behaviour or other suspicious activities, if it is external. D. Identify the destination IP address. • Check the role of IP if it is internal.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			• Check the reputation of the IP address for malicious behaviour or other suspicious activities, if it is external. If the source IP is external, gather relevant information about the source IP from open online sources: • Source IP: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP and Check the source IP address reputation on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ E. Check other users who are linked to this IP address using the SIEM log search. F. Check the complete details of the configuration changes using CloudTrail logs - • Identify the significance of the configuration change and what impact does it make to the resource/environment. • Based on the impact/significance of the change, identify the severity of the operation. • Check if the user has performed other actions which resulted in any additional offenses. G. Search for past 30 days logs based on source IP and check, • Any other offense or logs from the same source IP? • Any other user tried to login using the same source IP? Possibility of brute force attack. H. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team.
UC-CA-1034 - Linux - Excessive Failed Logins for one user	0		1. When SOC team observes a 'UC-CA-1034 - Linux - Excessive Failed Logins for one user' an alert is triggered in Sentinel, it means Multiple login failures have been observed for single user. 2. Check the events captured due to which the alert is triggered. 3. Verify if necessary conditions are matched. 4. collect the details about Ip address which is used by user for performing login activity from events. 5. If the IP is external, gather relevant information about the IP from open online sources: • Source IP: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP and Check the source IP address reputation on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 6. Search past 30 days activities of the user and check : - What kind of failed authentications are being observed. - From how long failed authentications are generated - Authentication failures are happening from same system/IP or multiple systems/IPs. 7. Check for any other suspicious activities from the user. 8. Check if any successful login events are there in past 30 days. If you find for the same Time both failure and Succeed connection for the same account on the same server then we can consider as no risk. 9. check the AV status for the system from which user is trying to login. 10. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them : a. Verify why these authentication failures are happening. b. Please check and correct if these failure authentications are happening due to wrong configuration/ script. c. (If user or host details are not available in cmdb) Kindly update the source host details in CMDB. d. If the account seems compromised, disable the account/ reset the password.
UC-IA.PR-2002 - Linux - New Root Equivalent User Created	0		1. When SOC team observes a 'UC-IA.PR-2002-Linux - New Root Equivalent User Created' offense in Sentinel, it should be treated on priority because it plays a crucial step in identifying unusual and suspicious behaviors within the network that can lead to exploitation. 2. Check for any pre-notification received or any ticket raised that could trigger this offense. • In such case this activity should be consider as authorized activity. • If no notification is found, you will need to raise a ticket for the same offense

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			3. Check the events captured due to which offense is triggered. 4. Identify the user who performed the action. • Check whether this user should be able to perform such Activity • Check past 30 days activity for user if the operation was done deliberately. 5. If the user should not have been able to perform the operation or the user mentioned that it was not done by him/her, check on the SIEM for privilege escalation related offenses/events. 6. Check if newly created username performing root equivalent activity in the network, example if user is scheduling task or running root privilege, we will be observing privilege escalation success or failed attempt. 7. Observe specifically the privilege escalation failed or success events from the user 8. Check newly created account trying to clear audit logs or trying to create new users or changing credential in the security group. 9. Check the details and reputation of the external source IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the source IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 10. Search for past 30days activity based on the external source IP/host and check: • The Critical ports that have been targeted. • Type of traffic observed from this particular source and frequency of the connections and if those are accepted or dropped. • Any reverse connection observed towards this source and if its accepted or dropped. 11. Gather the targeted host(s) details from the database: • What kind of data is contained on that device? • Is there any sensitive data (i.e. PII)? • Check the host details (like host is a server, desktop or laptop). And also collect other information (like domain, location, assigned to, etc) 12. Search for past 30days logs, based on the targeted host(s) and check the activities done by it and if those seems suspicious or not. 13. Check the activity performed by the created user. 14. Check for other suspicious activities observed around the time of the alert. 15. Confirm the time of activity. The time SIEM tool received the event may not be the time the activity occurred. 16. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them
UC-DE-27 - AD - Interactive Logon with Service Accounts	0		1. When SOC team observes a 'UC-DE-27 - AD - Interactive Logon with Service Accounts' incident in Sentinel, it means successful interactive logon was made to the service account . 2. Check the events captured due to which the incident is triggered. 3. Identify the attack methodology: • Attack vector: o Reason for interactive logon of service accounts. o What kind of privileges are assigned to the service accounts? 4. Check the event IDs 4624 and 4625 for the service account and source IP for past 30days logs. 5. Check for the type of logon being used by the user,collect information about specific logon type. 6. Check for any failed login attempts before the successful logon from the same source IP or service account. 7. Also try to fetch details about service account that is being used for interactive logon (Privileges and general usage). 8. Service account should never logon interactively, hence, increase the severity of the incident . 9. Check the last 30 days' logs for the same source IP and look for any suspicious activities occurring from this source IP. 10. Confirm the time of activities. The time SIEM tool received the event may not be the time the activity occurred. 11. Check the details and reputation of the external source IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the source IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 12. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team.
UC-DE-59 - AD - Windows Firewall Policy Changed	0		1. Check the SIEM alert and Check the events captured due to which offense is triggered. 2. check logs for last 30days logs for host. 3. Check in alert logs policy name and profile change for firewall.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			4. Check for last 24 hrs logs if any user has connected between these timeframe, may be he will be responsible for this activity. 4. If we found user, check whether user is Admin account or local account. 5. If user found, mentioned all details for user. User Details: a. Name: b. Title: c. Location: d. Department: e. Email ID: f. Manager 6. Check Host details: a. HostName: b. OS: c. Owner Group: d. Assigned to: e. Location: f. Function: 7. Check Computer Status and Risk report for the Host in AV. a. Last Scan: b. Virus definition: 8. Check last30 days logs if any other events were observed apart from event id 4950 (A Windows Firewall setting was changed), list those all events . 9. Verify the Event id and check for the Event id details for which Tactic it pertains to .ex(Failed password , bruteforce, Password spray) 10. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them to: 1.If user is Admin account, check if he is authorized to change policy. 2. If user is local account, increase severity. 3. If system is infected, please isolate the host from the network. 4. Run a full scan with updated AV on the impacted host for any signs of malware. 5. If account seems compromised, disable the account(In case no business dependency)
UC-DE-60 - AD - Windows Firewall Stopped	0		1. Check the SIEM alert and check logs for last 12 hours for host. 2. Check in 12hrs/24 Hr logs, if we have observed shutdown and reboot activity during same time frame, if so, then ignore this alert. 3. Else investigate this alert. 4. Check in 12hrs logs if any user has connected between this timeframe, maybe he will be responsible for this activity. 5. If user found, mentioned all details for user. User Details: a. Name: b. Title: c. Location: d. Department: e. Email ID: f. Manager: 6. Check Host details: a . HostName: b. OS: c. Owner Group: d. Assigned to: e. Location: f. Function: 7. Check Computer Status and Risk report for the Host in AV. a. Last Scan: b. Virus definition: 8. Check past 30days logs if any other events were observed apart from event id 5025 (The Windows Firewall service was stopped), list those all events in the ticket. 9. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team for further Investigation and recommend them to: 1. Check with host owner, reason for stopping firewall and if this is an authorized activity or not? 2. Please run a full AV scan to confirm for any trace of infection. 3. Check for any vulnerabilities associated with the host and if found fix it with a patch (if available). 4. Check if the hosts OS, applications, and security software's are updated with the latest patch or not?
UC-DE-864 - Windows - Event or Audit Log Cleared	0		1. Examine the Windows event logs on the affected system to identify when the Event or Audit Log Cleared and if there are any other related events that might indicate the cause of the incident for lat 30 days 2. Conduct a thorough analysis of the affected systems and logs. Determine the extent of log tampering and time when they occurred. 3. Investigate the source of the activity and block the IOC's if they are external and malicious.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			4. If the source of activity is from internal user with privileged access, determine whether the activity is legitimate, or it has occurred by compromising the privileges. 5. Investigate if there have been any unauthorized access or login attempts on the affected system. Look for any signs of credential misuse. 6. Confirm the time of the logs got cleared. The time SIEM tool received the event may not be the time the activity occurred. • Investigate the alert and base logs to check for the additional information related to the event. • Check for the event ids (1102,517 and 104 in past 24HRS) 7. Investigate whether there were other activities or security incidents before or after the log clearing that might be related. 8. Check if this incident led to any potential data breach or compromise of sensitive information and check the AV status of the Host. 9. Research in SIEM for that user in the last 30 days prior to the login events to look for other anomalous activity. · Search for all activity with username in last 15 days 10.Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them to: a. Verify if this action is legitimate or not. b. Evaluate the organization's access control policies and practices to identify any weaknesses or gaps that may have allowed the incident to occur. c. Recommended to run thorough scans using up-to-date antivirus and anti-malware tools. d. Verify whether this is related to testing activity. Recommended to inform to the SOC, before performing any such kind of activities e. Change all passwords associated with the compromised system and review the privileges granted to users to prevent unauthorized access. f. Contact SOC if any additional details required.
UC-DE.IM-2115-Potential re-named sdelete usage	0		1. Investigate the logs and identify any suspicious activities related to the potential misuse of "sdelete" or any other commands. 2. Examine file system metadata and changes to understand when and how the "sdelete" utility was potentially renamed or utilized. 3. Investigate who might be responsible for the unauthorized access or attack and gather the information about the actor who performed. 4. Block the IOC's and make sure that only authorized users have access to critical utilities and commands, including "sdelete." 5. Investigate whether any sensitive data was deleted or exfiltrated using "sdelete". 6. Estimate the loss due to deleted information and take necessary actions. 7. Isolate the system from the network to prevent further damage or data exfiltration. 8. If the source of activity is from internal user with privileged access, determine whether the activity is legitimate, or it has occurred by compromising the privileges. 9. Investigate if there have been any unauthorized access or login attempts on the affected system. Look for any signs of credential misuse. 10. Identify Renamed Files or Utilities and look for any indications of "sdelete" being potentially renamed. 11. Investigate whether there were other activities or security incidents before or after the usage and renaming of sdelete that might be related. 12. check the AV status of the Host. 13. Research in SIEM for that user in the last 30 days prior to the login events to look for other anomalous activity. · Search for all activity with username in last 30 days 14. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them to: a. Implement Multi-factor authentication if it's not yet enabled. b. Ensure that all software and systems are up to date with the latest security patches to prevent exploitation of known vulnerabilities. c. Implement principle of least privilege. d. Ensure that only authorized users have access to critical utilities and commands, including sdelete. e. Recommended to run thorough scans using up-to-date antivirus and anti-malware tools. f. Change all passwords associated with the compromised system and review the privileges granted to users to prevent unauthorized access. g. Recommended to have regular security assessments. h. Contact SOC if any additional details required.
UC-EX-2117-Scheduled Task Hide	0		1.Check for last 30 days windowslogs for suspicious scheduled tasks. 2.Get information about name and content of the scheduled task observed from online sources and check if it is related to any well-known malicious service. 3.If possible Using system forensics tools, identify any unusual or suspicious tasks, especially those that may not appear in a regular schtasks /query or Task Scheduler view. You'll need to look for tasks with unusual names, tasks set to run at odd times or intervals, or tasks associated with uncommon or suspicious programs.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			4.If you find a suspicious task, analyze the associated program or script for signs of malicious activity. This might include downloading additional malicious software, contacting command-and-control servers, or modifying system settings. 5.Review the activity logs of any user accounts that may have been involved in creating or modifying the suspicious tasks. Look for signs of unusual behavior such as logging in at odd times, running unusual commands, or accessing sensitive resources. 6.Analyze your network traffic logs for any signs of communication with known malicious IP addresses or domains, particularly those that correspond to the timing of the suspicious tasks. 7.Search past last30days windows logs for this user and check, - if any other suspicious activities have been done by user in past 30 days. 8.If the above steps reveal abnormal behaviors or signs of compromise, it is necessary to confirm the incident, assess the impact, and determine the scope of the compromise. 9.Depending on the impact of the incident, you may need to disable or delete the suspicious tasks, remove any associated malware, reset compromised account credentials, or even rebuild affected systems and kindly raise a ticket with below recommendation steps. Recommended Actions a.Use advanced threat detection tools that can detect suspicious registry changes or abnormal scheduled task activities. b.Regularly monitor your registry for changes, especially in the areas related to scheduled tasks. This can help detect attempts to hide tasks. c.Audit your scheduled tasks regularly, not only through the Task Scheduler but also by using tools that can uncover hidden tasks. d.Use tools that provide user behavior analytics to detect anomalous behavior, such as a user unexpectedly modifying tasks or registry entries. e.Depending on the impact, you may need to isolate affected systems, change passwords, or even reset compromised accounts. f.In case any vulnerability has been exploited, kindly fix it by a patch. g.Please update the ticket accordingly.
UC-CA-113 - Azure - Azure DevOps Personal Access Token (PAT) misuse	0		1. When SOC team observes a 'UC-EX.IM-113 - Azure – DevOps Personal Access Token (PAT) misuse' alert in Sentinel, it means a possible PAT authentication through browser or abnormal use of PAT took place. 2. Check for any prior notification received or any ticket raised or any ongoing change taking place related to this operation in Azure Environment: • In such case this activity should be considered as legitimate activity. • There is a possibility that PAT may have been used for a sensitive operation which has been allowed for this event. • If not, raise a ticket for the offense and ask for details required for the investigation to proceed. 3. Try to capture the information about the Username, Source IP, Project Name, Operation Name, Details from logs. 4. The exact scenario for which the alert was generated should be found out – whether PAT was used for authentication with browser or used for an abnormal activity. 5. Identify the Username associated with this activity. Other information to be retrieved from the logs is - a. Find out the Project Name from the logs. b. The details column from the log should be added to the ticket to give more information behind the event. 6. The exact operation name in case of abnormal activity should be added to the ticket. This will help the client in deciding if this was indeed allowed or not. 7. Confirm the time of activity. The time Log Analytics Workspace received the event may not be the time the activity occurred. Raise a ticket with client to check with user for activities performed with below recommendations: • Please check if this activity was legitimate or malicious. • If this activity was legitimate, check there was proper approval or ticket raised for this activity. • If this activity was malicious then please disable/delete this user. • In case of PAT being used to authenticate through browser, the user password should be changed and PAT should be revoked. • In case of PAT being used for abnormal activity, the operation name should tell us if the activity should be allowed or not. It is not advised to use PAT for such sensitive operations. The client should be asked to abstain from using PAT for such operations. Also the client should make sure that the user associated with this alert performed this activity or not? If not, change the password and revoke PAT. • Roll back the changes, if this activity was malicious. • Update ticket accordingly.
UC-CC-1497 - Connection to DGA Domain	0		DGA stands for "Domain Generation Algorithm." It is a technique used by malware or malicious software to create a large number of unique domain names dynamically. The purpose of using a DGA is to evade detection by security measures, such as domain blacklisting, and to establish communication with command and control (C&C) servers. 1.Identify source IP associated with this activity. 2.Check if the IP is internal/external. In case of External IP: Check the details and reputation of the external source IP from the online tools to know if the IP

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			has been reported recently for any suspicious activity. Check the source IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ a.In case of internal IP, check if there has been any suspicious activity happening from this IP in last 30 days. 3.Search for past 30days logs based on source IP and check, a.Frequency of the connections towards destination IP address b.Request type for all these connections c.If any other suspicious activity is detected from same source IP 4.Check from the logs which domain names have been generated by the algorithm to setup the communication. 5.Check this domain is associated with any known malware family and analyze and its associated IP addresses for indicators of compromise (IOCs). 6.If you suspect the system is infected with malware, conduct analysis, and identify its capabilities. 7.Check for any patterns ,security alerts and anomalies in the network traffic that may indicate malicious activity. 8.Investigate the activities performed on the system after the connection was made. 9.Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them to: Recommendations: • If you suspect a compromise, Isolate the system from the network. • Recommended to conduct a malware analysis. • The IP on which the DGA is operating should be scanned and cleaned of malwares. • If Source IP is highly malicious, kindly block the IP. • Blacklist the DGA domain and update the DNS configuration. • Please update the ticket accordingly.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
UC-CC-1277 - DNS - High NULL Records Requests Rate	0		DNS NULL record request refers to a query for a resource record of type NULL in the Domain Name System (DNS) and DNS requests with a record type set to "Null". This is not common DNS traffic and is indicative of DNS tunneling. Blocking these packets will usually block the tunnel. 1.Check the events captured due to which incident is triggered. 2.Verify, if necessary, conditions for incident are matched. 3.Check for any pre-notification received or any ticket raised for usage of this account. a.In such case this activity should be consider as authorized activity. b.If no usage notification is found, you will need to raise a ticket for the incident. 4.Identify the user account who has performed this activity. •Check the activities performed from the same user account in last 30 days. •Analyze the pattern and frequency of NULL records requests. Look for any discernible trends, sources, or destinations. 5.Identify the source IP related to this activity. Check the activities performed from the same source IP in last 30 days. 6.Review DNS logs for the identified timeframe to identify the nature and volume of NULL record requests. Look for patterns, excessive requests from the same source IP, or any other abnormal behavior. 7.Look for last 30 days DNS events and check if any other suspicious behavior is observed. 8.Determine the source of the high NULL record request rate. Analyze the source IP address and investigate whether it corresponds to a legitimate user or an external entity. 9.Determine the protocols or services associated with the NULL records requests. Are they related to a specific application, communication channel, or system component. 10.Evaluate the potential impact of the NULL records requests on the affected systems or network. Are there signs of service disruption, performance degradation, or data leakage. 11. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them to: Recommendations: • Please check if this is legitimate or authorized activity. • If it is legitimate and approved activity, kindly check is this one time or repeated activity. If it is repeated activity, please confirm whether it can be whitelisted. • If it is not legitimate or approved activity, please check the root cause for this whether it is due to user activity or due to any other process/application on the system that is triggering it. • If external IP is found to be malicious, block it across perimeter level. • Check if any vulnerabilities associated with the host. If found, fix it with a patch. • Run a full scan with updated AV. • Kindly update the ticket accordingly.
UC-DI.CA-2001- Web Servers - Inbound web requests with IP instead of domains	0		1.Check the events captured due to which alert is triggered. 2.Analyze DNS traffic logs to identify any suspicious activity that may be related to the threats identified in the TI map. This can include looking for unusual domain name resolutions, queries to known malicious domain names, and other anomalies. 3.Identify the IP address (source IP) used in this process. •Check the role of IP if it is internal. •Check he reputation of the IP address for malicious behavior or other suspicious activities, if it is external. 4.Identify the destination IP address. •Check the role of IP if it is internal. •Check the reputation of the IP address for malicious behavior or other suspicious activities, if it is external. 5.Gather the targeted host details from the database: •What kind of data is contained on that device? •Is there any sensitive data (i.e. PII)? •Check the host details (like host is a server, desktop or laptop). And also collect other information (like domain, location, assigned to, etc.) 6.Search for past last 30 days activity based on the target host and check. 7.Investigate any IP that are associated with the suspicious DNS activity. This can include looking up the domain in threat intelligence databases and analyzing any associated indicators of compromise. 8.If malware is suspected, analyze any associated malware samples to identify its behavior, capabilities, and potential impact on the organization. 9.Review web server logs for the identified timeframe to identify inbound web requests with IP addresses instead of domains. Look for patterns, multiple requests from the same source IP, or any other abnormal behavior. 10.Raise a ticket using ticketing tool and ask for details required for the investigation to proceed and recommend them to: Recommendations: a. Based on the analysis of W3CIISLog, any identified malicious IP and associated IP addresses should be blocked at the firewall or DNS level to prevent further communication with these entities.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			b. Any systems that are found to be compromised should be immediately isolated and remediated to prevent further damage. c. Review and update security controls, including firewalls, intrusion detection and prevention systems, and antivirus software, to ensure that they are configured to detect and block the identified threats. d. Investigate the web server configurations and any potential vulnerabilities that may have allowed such requests. e. Perform a complete AV scan of the target machine with the updated AV. f. Kindly update the ticket accordingly.
UC-PR-2088-Dynamics Encryption Settings Changed	0		1.If you see encryption settings changes in dynamics 365 • Firstly, look for the changes that had newly implemented and investigate on them. • Understand the impact of those changes on the organization. 2.Verify the current encryption settings and compare them to the previous settings. 3.Check the permissions of users who have access to the Dynamics 365 and investigate whether any unauthorized access has been happened. 4.Identify the IP address (source IP). o Check the role of IP if it is internal. o Check the reputation of the IP address for malicious behaviour or other suspicious activities if it is external. Check the details and reputation of the external source IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the source IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 5.If the changes had taken place by authorized users, investigate under what conditions the changes had happened and also check whether they do have permissions to perform. 6.Identify the root cause of the changes. This could be an intentional action by an insider or an external attacker, or it could be the result of a misconfiguration or other technical issue. 7.Check other users who are linked to this IP address using the SIEM log search. 8. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team. and recommend them to: Recommended Actions a.Please check and confirm if this action was legitimate or malicious. b.If you suspect that account has been compromised, change all your passwords immediately. c.Implement Multi-Factor Authentication. d.Recommended only authorized users have access to encryption settings. e.Regularly review access controls and user permissions f.Immediately block the identified IOC's. g.Sometimes authorized setting changes may lead to issue like compatibility and performance issues, so it is recommended to test before deploying the changes. h.Please update the ticket accordingly.
UC-EF-2093-Dynamics 365 - User Bulk Retrieval Outside Normal Activity	0		1.Check for any prior notification received or any ticket raised or any ongoing change taking place to this operation in Azure Environment. • In such case this activity should be considered as legitimate activity. • If not, raise a ticket for the offense and ask for details required for the investigation to proceed. 2.Try to capture information about the Source IP, Role Assignor, Role Assignee, permission granted from events 3.Analyze Access Patterns: Compare the bulk retrieval activity with normal user access patterns. Look for deviations in the timing, frequency, or volume of data accessed. 4.Identify the Source Host Name(s) and IP Address: If the source is external, gather relevant information about the source IP from open online sources: • Source IP: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: Check the details and reputation of the external source IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the source IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ If the source is internal, gather the below details: • What type of data is contained on that device? - Devices containing sensitive data (i.e., PII) are a higher priority for remediation.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			- Does it belong to VIP users? Identify the Destination Host Type: • Workstation or Server (Enterprise, Production, Development) - Are critical services being impacted? • Which Domain does the host belong to? • What is the MAC address? DHCP enabled? 5.Identify the Destination Host Name(s) and IP Address: • What type of data is contained on that device? - Devices containing sensitive data (i.e., PII) are a higher priority for remediation. - Does it belong to VIP users? 6.Identify the Destination Host Type: • Workstation or Server (Enterprise, Production, Development) - Are critical services being impacted? • Which Domain does the host belong to? • What is the MAC address? DHCP enabled? 7.Review User Access: Examine the users involved in the bulk retrieval activity. Verify whether these users have appropriate permissions to access the retrieved data. 8.Check Export Options: Investigate the methods used for bulk retrieval. Determine if the data was exported using built-in export functionalities, APIs, or other methods. 9.Verify Intent: Assess the purpose behind the bulk retrieval. Determine if it aligns with legitimate business needs or if there are indications of unauthorized data extraction. 10.Review Third-Party Integrations: If third-party integrations are involved, investigate their role in the bulk data retrieval. Ensure that any integrations are legitimate and properly configured. 11.Check details of the user who created this task. • If the account is a privilege account, increase the severity. • Search past 30days. Azure logs for this user and check, if any other suspicious activities have been done by user in past 12hrs 12.Search for the past last 30 days activities based on the source IP/host and see the trend: • Check for any suspicious activities like connections to known malicious internet hosts, etc. • Check or ask respective team to check AV status for the system where scheduled task was created to confirm if there is any malware or some other infection present in system. 13.Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team. Recommended Actions a.Disable or limit the account during the investigation and response. b.Identify the possible impact of the incident and prioritize; accordingly, the following actions can help you gain context: •Identify the account role in the cloud environment. •Assess the criticality of affected services and servers. •Work with your IT team to identify and minimize the impact on users. •Identify if the attacker is moving laterally and compromising other accounts, servers, or services. •Identify any regulatory or legal ramifications related to this activity. c.Containment and Mitigation: If unauthorized access is confirmed, take steps to contain the breach, revoke unauthorized access, and mitigate the impact on affected data. d.Check if unauthorized new users were created, remove unauthorized new accounts, and request password resets for other users. e.Enhance Monitoring: Implement additional monitoring and alerts for bulk retrieval activities. Set up notifications for unusual data access patterns. f.Implement Data Loss Prevention (DLP): Consider implementing DLP policies to prevent unauthorized data exports and transfers. This can help prevent similar incidents in the future. g.Consider enabling multi-factor authentication for users. h.Determine the initial vector abused by the attacker and take action to prevent reinfection via the same vector.
UC-PR-2203 - UEBA - Anomalous administrative task performed on Azure	0		1.Check for any prior notification received or any ticket raised or any ongoing change taking place to this operation in Azure Environment. • In such case this activity should be considered as legitimate activity. • If not, raise a ticket for the offense and ask for details required for the investigation to proceed. 2.Try to capture information about the Source IP, Role Assignor, Role Assignee, permission granted. 3.Identify the Source Host Name(s) and IP Address: If the source is external, gather relevant information about the source IP from open online sources: • Source IP: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: If the source is internal, gather the below details: • What type of data is contained on that device?

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			- Devices containing sensitive data (i.e., PII) are a higher priority for remediation. - Does it belong to VIP users? Identify the Destination Host Type: • Workstation or Server (Enterprise, Production, Development) - Are critical services being impacted? • Which Domain does the host belong to? • What is the MAC address? DHCP enabled? 4.Identify the Destination Host Name(s) and IP Address: • What type of data is contained on that device? - Devices containing sensitive data (i.e., PII) are a higher priority for remediation. - Does it belong to VIP users? Identify the Destination Host Type: • Workstation or Server (Enterprise, Production, Development) - Are critical services being impacted? • Which Domain does the host belong to? • What is the MAC address? DHCP enabled? 5.Check details of the user who created this task. • If the account is a privilege account, increase the severity. • Search past 30 days. Azure logs for this user and check, if any other suspicious activities have been done by user in past 30 days 6.Search for the past 30 days activities based on the source IP/host and see the trend: • Check for any suspicious activities like connections to known malicious internet hosts, etc. • Check or ask respective team to check AV status for the system where scheduled task was created to confirm if there is any malware or some other infection present in system. 7.Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team with below Recommended Actions: a.Disable or limit the account during the investigation and response. b.Identify the possible impact of the incident and prioritize; accordingly, the following actions can help you gain context: • Identify the account role in the cloud environment. • Assess the criticality of affected services and servers. • Work with your IT team to identify and minimize the impact on users. • Identify if the attacker is moving laterally and compromising other accounts, servers, or services. • Identify any regulatory or legal ramifications related to this activity. c.Investigate credential exposure on systems compromised or used by the attacker to ensure all compromised accounts are identified. Reset passwords or delete API keys as needed to revoke the attacker's access to the environment. Work with your IT teams to minimize the impact on business operations during these actions. d.Check if unauthorized new users were created, remove unauthorized new accounts, and request password resets for other users. e.Consider enabling multi-factor authentication for users. f.Determine the initial vector abused by the attacker and take action to prevent reinfection via the same vector.
UC-CA-2204 - UEBA - Anomalous activity on SecurityEvent	0		1.Identify the attack methodology: • Attack vector: § Identify anomalies that may indicate the compromise of an asset or credentials. § Identify Source Details, User account trying to request handle to an object in AD, etc. § Identify all the suspicious activities occurred from the same source IP. 2.Identify the user who performed the action. • Check whether this user should be able to perform such operations ie. Does he/she have the rights on that resource configurations? • Check with the user if the operation was done deliberately. 3.If the user should not have been able to perform the operation or the user mentioned that it was not done by him/her, check on the SIEM for privilege escalation related offenses/events. 4.Identify the IP address (source IP) used in this process. • Check the role of IP if it is internal. • Check he reputation of the IP address for malicious behaviour or other suspicious activities if it is external. 5.Identify the destination IP address. • Check the role of IP if it is internal. • Check the reputation of the IP address for malicious behaviour or other suspicious activities if it is external. Check the details and reputation of the external source IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the source IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 6.Check other users who are linked to this IP address using the SIEM log search. 7.Check the logs captured due to which the offense is triggered.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			8.Search for past 30days logs based on source IP and check, • Any other offense or logs from the same source IP? • Any other user tried to login using the same source IP? Possibility of brute force attack. 9.Check any other suspicious activities observed on the system/host. 10.Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team with below mentioned Recommended Actions a.If successful logon has occurred, check for which user it has happened and for how long the user was logged in. Check with the user if it was a legitimate activity or not. If not, then disable the user temporarily and change the password immediately. b.If successful logon has not occurred, check if any other malicious/suspicious activities are performed from the same source. If yes, then ask the client to block the source IP if it does not have any impact on the business continuity. c.Reset the changes if the activity was illegitimate. d.Revoke unnecessary access to such resources for users and groups. e.Run AV scans on the host using the source IP. f.If the user account was compromised, ask the user to reset the password and use strong authentication methods like MFA. g.If additional suspicious activities are seen from the same source IP, block the IP. h.Please update the ticket accordingly.
UC-DE-2118-Too many NSG Denies from a Single IP	0		1.Identify the attack methodology: • Attack vector: § What ports have been accessed by the source. § Threat actors may often try to gain the advantage of unpatched vulnerabilities. 2.Identify the IP address(s) form which the too many NSG denies have been observed. • Check the details and reputation of the external source IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the source IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ §Also, check the IP belongs to which country. •Check the associated port with the connections and mention brief detail of the port. •Are there any accepted connections from same IP on any other port? §If yes, then please mention all those port numbers. •Check how many accepted and dropped connections are there. 3. Identify all the Host Name(s) & Internal Source IP Address • What type of data is contained on that device? § Devices containing sensitive data (i.e. PII) are a higher priority for remediation § Does it belong to VIP users? § Please check is there any suspicious process is running into the host. 4. Identify the Host Type • Workstation or Server (Enterprise, Production, Development) § Are critical services being impacted? • Which Domain does the host belong to? 5. Attempt to gather relevant information about the subject user: • Role of employee or partners involved (Executive, etc.) • Search Active Directory Users and Computers: § Get employee or service account owner's full name. § Group membership, account history, notes § Lookup contact information, review role. 6. Based on source IP check IPS/IDS has triggered any signature or not in past lasst 30 days. 7. Check the AV status of the Host. • If analyst have the access of respective AV solution, then observe the following: § Version: § Last scan performed: § Risk: • If analyst don't have the access of AV portal, then ask the concern team to check the same. 8. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team with below mentioned Recommended Actions a.Please check if this is an authorized activity. b.In case this is an authorized activity, please confirm to find a whitelisting solution. c.In case any vulnerability has been exploited, kindly fix it by a patch. d.If the host/account seems compromised, increase severity. e.Please block the IP at NSG, if required. f.Check any file has been downloaded in the host or not. g.If ports are not in use, then close it. h.Run complete AV Scan on the source host (if internal).

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
Suspicious application consent similar to O365 Attack Toolkit	0		1.Check the events captured due to which offense is triggered. 2.Verify if necessary conditions for offense are matched. 3.Check for any pre-notification received or any ticket raised for this activity. 4.In such case this activity should be consider as authorized activity. 5.If no usage notification is found, you will need to raise a ticket for the same offense 6.Check for which application consent was granted. It can be found in the modified properties field in event payload. 7.Mention all the details regarding application which are present in the modified field. It contains consent type, granted on behalf of and other details. 8.Check which user has granted consent to the application. 9.Attempt to gather relevant information about the subject user: 10.Role of employee or partners involved (Executive, etc.) 11.Search Active Directory Users and Computers: a.)Get employee or service account owner's full name b.)Group membership, account history, notes c.)Lookup contact information, review role 12.Check if user was authorized to grant consent to the application. 13.Identify source IP related to this activity. 14.Check the activities performed from the same source IP in last 30 days. 15.If above mentioned activities are unauthorised, kindly ask to roll back the changes done by the user. Remove the user from the reference set SOC-REF-0271 AD Active users if he is added to it after when the offense is generated. 16.Raise a ticket with client to check with user for activities performed and recommemd as: a.For illegitimate activity, revoke the consent from the application. b.Review the other existing permissions of the application. c.Review the permissions and roles assigned to the user who initiated the action. d.Remove the user from the reference set AD Active users if he is added to it after when the offense is generated e.Allow consents for applications from verified publishers only and specific types of permissions classified as low impact.
Possible Covering Track Attempt - Exchange Auditlog Disabled	0		1.Check the events captured due to which offense is triggered. a.Covering Track Attempt: An attempt by an unauthorized user to hide their activities by disabling or manipulating audit logs. b.Exchange Audit Logs: Identifies when the exchange audit logging has been disabled which may be an adversary attempt to evade detection or avoid other defenses and Logs generated by the Microsoft Exchange Server to record activities such as logins, message tracking, and configuration changes. 2.Review system logs, network logs, and any available security information to trace the activities leading up to the disabling of audit logs. Look for signs of unauthorized access or suspicious behavior. 3. Check the source IP involved in the activity from the events. a. If the source is external, gather relevant information about the source IP from open online sources: • Source IP: • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: #Gather relevant information about the source IP from open online sources:Virustotal.com,abuseipdb.com, ipvoid.com • Source IPIf: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 3.Check for past 30days' logs for any suspicious activity performed from the Source IP. 4.Check for past 30days' logs for any suspicious activity performed from user. 5.Check all necessary tables for more investigation using below kql query: Search "Username or Ip address" | distinct $table 6.Check the username (UserId), who performed this action. a.Check if any user was privileged or not. If yes, increase the severity. b.Search for the past 30 days for any other suspicious activity from the same username. 7.Check "Set-AdminAuditLogConfig" operation from office activity logs and also cehck is this activity is done by Admin user.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			Officeactivity | where Ipaddress or userprinicipal name contains "x.x.x.x" 8.Check for any pre-notification received or any ticket raised for this activity. 9.In such case this activity should be consider as authorized activity. 10.If no usage notification is found, you will need to raise a ticket for the same offense 11.Based on the above information, if the activity is suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them: a.Please check if the activity was authorized or not. b.If activity is not legitimate, check for all the actions performed towards alerted machines. c.Disable compromised accounts or reset passwords. d.isolate the affected system or server from the network to prevent potential further compromise or data exfiltration. e.Implement Multi-Factor Authentication (MFA) f.If change is not correlated with an approved internal events - subject to corporate change management policy, reverse the change in Windows. g.Review activity logs in Office365 via Azure Sentinel console and identify any abnormal activities to within the time when the change was done. h.Update ticket accordingly.
Anonymous Link Created for a Sensitive Office365 Folder / File	0		1.Check the events captured due to which offense is triggered. a.Anonymous Link: A shareable link that allows access to a folder or file without requiring authentication. b.Sensitive Information: Information that, if disclosed, could have a significant impact on the organization's security, privacy, or compliance. 2.Check the source IP involved in the activity from the events. a. If the source is external, gather relevant information about the source IP from open online sources: • Source IP: • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: #Gather relevant information about the source IP from open online sources:Virustotal.com,abuseipdb.com, ipvoid.com • Source IPIf: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 3.Check for past 30days' logs for any suspicious activity performed from the Source IP. 4.Check for past 30days' logs for any suspicious activity performed from Ananymous link. 5.Check all necessary tables for more investigation using below kql query: Search "Username or Ip address" | distinct $table 6.Check the username (UserId), who performed this action. a.Check if any user was privileged or not. If yes, increase the severity. b.Search for the past 30 days for any other suspicious activity from the same username. 7.Check Office activity table for identifying, responding to, and preventing the creation of anonymous links for sensitive Office 365 folders/files in the organization using below kql query: Officeactivity | where Ipaddress or userprinicipal name contains "x.x.x.x" 8.Check and collect details about "AnonymousLinkCreated" activity done by user from officeactivity table 9.Analyst kindly check Anonymous link reputation using below threat intel online tools: https://www.urlvoid.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ 10.Investigate how the anonymous link was created from the logs Review audit logs, access history, and permissions to identify the user account responsible for generating the link. 11.Based on the above information, if the activity is suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			them: a.Please check if the activity was authorized or not. b.If activity is not legitimate, check for all the actions performed towards alerted machines. c.Perform complete scan on system with updated AV and make sure system is clean in the scanned report. If, not work on mitigating the threat as per report. d.If any user is associated with an activity, please check with user for purpose behind such activity, if necessary, raise user awareness. e.Disable compromised accounts or reset passwords. f.If created Anonymous link is considered as suspicious,Disable or revoke the anonymous link immediately to prevent further unauthorized access. This can typically be done through the Office 365 admin console or SharePoint settings. g.Implement Multi-Factor Authentication (MFA) h.Update ticket accordingly.
Suspicious External Mail Forwarding	0		1.Check the events captured due to which offense is triggered. 2.Check the source IP involved in the activity. a. If the source is external, gather relevant information about the source IP from open online sources: • Source IP: • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: #Gather relevant information about the source IP from open online sources:Virustotal.com,abuseipdb.com, ipvoid.com • Source IPIf: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 3.Check for past 30days' logs for any suspicious activity performed from the same Source IP. 4.Check the username (UserId), who performed this action. a.Check if any user was privileged or not. If yes, increase the severity. b.Search for the past 30 days for any other suspicious activity from the same username. 5.Check the Originating Server Name and IP address. 6.Check the keyword specified in any of "SubjectContainsWords"," BodyContainsWords", "SubjectOrBodyContainsWords" field in the payload. a.Check if the specified keywords/ phrase contain any of (helpdesk, alert, suspicious, fake, malicious, phishing, spam, do not click, do not open, hijacked, fatal etc.) 7.Check the payload to get more information on any other parameter specified like "ForwardTO", "MoveToFolder", "StopProcessingRules" etc. 8.Check if any incident of phishing or spam mails are observed in the organization before this rule got triggered, this could indicate intrusion of attacker in the organization. 9.Check all necessary tables for more investigation using below kql query: Search "Username or Ip address" | distinct $table 10.Check and collect user details using below kql query: Identityinfo | where * has "Username" 11.Check office activity for last 30 days to know exact operation performed by captured user Ref: Office actiivty | where * has "username" 12.Check reptation of email received domain using online resources like: https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search 13.Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them: a. Check with the user who performed this activity is authorized to do that or not. b.Ask to block the source IP if external and malicious. c.Check with the client whether the forwarding SMTP address is internal and legit to their environment or not. d.If not, then modify the settings not to forward the mail to that particular address.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			e.Disable and delete the inbox forwarding rule. f.For the Inbox Rule forwarding type, reset the user's account credentials. g. Block the external mail address. h. Disable compromised accounts or reset passwords. i. Remove unauthorized forwarding rules. j.Communicate with affected parties and provide guidance on securing their accounts. k. Please update the ticket accordingly
Possible Data Exfiltration - Excessive SharePointFileOperation from a Previously Unseen IP	0		1.This rule detects events that allows huge chunk of data to go out from systems. The analyst shall confirm whether necessary conditions were met for the UC to get triggered, to do so, identify the number of bytes that are traced under potential exfiltration & confirm the alert. 2.Analyst should check what type of SharePointFileOperations are performed: Any operation related to files within SharePoint, including uploads, downloads, modifications, and deletions. 3.Kindly check any unauthorized transfer of sensitive or confidential data outside the organization that might be cause to Data Exfiltration. 4.Identify all the Host Name & Source IP (Internet Protocol) Addresses a.What type of data is contained on the sharepoint opearion from unseen ip? b.Device containing sensitive data (i.e. PII) are a higher priority for remediation 5.Check the source IP involved in the activity. a. If the source is external, gather relevant information about the source IP from open online sources: • Source IP: • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: #Gather relevant information about the source IP from open online sources:Virustotal.com,abuseipdb.com, ipvoid.com • Source IPIf: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 6.Check for past 30days' logs for any suspicious activity performed from the same Source IP. 7.Check all necessary tables for more investigation using below kql query: Search "Username or Ip address" | distinct $table 8.Check the username (UserId), who performed this action. a.Check if any user was privileged or not. If yes, increase the severity. b.Search for the past 30 days for any other suspicious activity from the same username. 9.Identify the Type of data shared oversharepoint & Check whether any business-related documents attached. 10. Identify if the source user is associated with activity and check, a.Was this a 'privileged' account? b.Was this account associated as a Service account? If a service account, who is the owner of the service account? 11.Check officeactivity for both captured user and unseen IP for last 30 days using below kql query: Officeactivity | where Ipaddress or userprinicipal name contains "x.x.x.x" 12.check and collect all necessary details about sharepoint opearions like how many files uploaded,downloaded,file modified on single session using unseen ip. 13.Analyst kindly check url reputation using below threat intel online tools: https://www.urlvoid.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ Based on the above information, if the activity is suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them: a.Please check if the activity was authorized by checking if the system data is leaked or not. If yes, isolate the system from the network and try to remediate b.If a security breach occurs, it is vital to be prepared and frequently back up all data so it's available for quick restoration. Failing to regularly back up data can lead to significant loss, should the worst happen. Data backup is a cybersecurity standard requirement.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			c.If activity is not legitimate, check for all the actions performed towards alerted machines. d.Perform complete scan on system with updated AV and make sure system is clean in the scanned report. If, not work on mitigating the threat as per report. e.If any user is associated with an activity, please check with user for purpose behind such activity, if necessary, raise user awareness. f.Block the external source ip address if its an malicious. g. Disable compromised accounts or reset passwords. h.Update ticket accordingly.
Multi-Factor Authentication Disabled for a User	0		1.Check if any prior notification was provided for this activity. If the activity was intended, mark it as legitimate and the alert can be closed. 2.Identify target user for which MFA is disabled. The target user is mentioned in the log field "targetResources":"userPrincipalName". Check all details of this user from the Azure AD and find if user has admin privileges. 3.Search on the time interval from alert detection to investigation for all activities based on target user and check, •Is there any successful login attempts detected from same user after disabling MFA. •Frequency of login towards destination host. •If any suspicious activity is done by this account after MFA was disabled. 4.Check the user who initiated the activity. It can be found in the log field "initiatedBy":"userPrincipalName". Check if this user is part of other alerts within past 30 days of alert detection and also after detection. 5.Identify IP address from where this activity was performed and check if it was from a suspicious IP address (Suspicious location,malicious IP,etc). 6.Search past 30 days activity based on source user and check, •If any other alerts are detected by SIEM tool from same source user. •If MFA was disabled for any other user apart from user detected in alert. Following artefacts should be collected from the logs • Source User • Source IP • Target User (user affected) • Time and date of alert 7.If the source is external, gather relevant information about the source IP from open online sources:Virustotal.com,abuseipdb.com, ipvoid.com • Source IP: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 8.Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them : a.Please check and confirm if this action was legitimate or malicious. b.If the analysis gives sufficient proof that the user performing this activity has been compromised or performing not allowed activity, it should be recommended to disable the account for the time being. c.During the initial phase of the analysis, if it seems like the activity could be benign but still suspicious, recommend to at least change the password of the account performing this activity. d.If the outcome of the analysis states that the activity is not legitimate, then recommend to re-enable the MFA for destination user and also to change the password of the account. e.Perform the investigation to find out if there is any successful login event from the destination user after MFA has been disabled for him/her. Also capture the activities that are performed by the user after the MFA disablement. MFA Registration Policy Disabled a.Check if any prior notification was provided for this activity. If the activity was intended, mark it as legitimate and the alert can be closed. b.Check the user who initiated the activity. It can be found in the log field "initiatedBy":"userPrincipalName". Check if this user is part of other alerts within past 30 days of alert detection and also after detection. c.Identify IP address from where this activity was performed and check if it was from a suspicious IP address (Suspicious location,malicious IP,etc). d.Search past 24 hr activity based on source user and check if any other alerts are detected by SIEM tool from same source user. e.Also search after the generation of alert for any other alerts related to the same user.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
Failed Logins from Unknown or Invalid User	0		1.Identify the attack methodology • Attack vector: o Logins with same usernames from different IP address o Excessive failed logins from the same IP address 2.Identify the User Account(s) for which • Did this account attempt to login on other systems? o Time periods? • Check the logon types, error code and event IDs (4776, 4625) in past 24hrs/30 days logs. • Check the time of account expiry and observe the activity after that for any suspicious behavior. 3.Identify all the Host Name(s) & Internal Source IP Address • What type of data is contained on that device? o Devices containing sensitive data (i.e. PII) are a higher priority for remediation o Does it belong to VIP users? If the source is external, gather relevant information about the source IP from open online sources:Virustotal.com,abuseipdb.com, ipvoid.com • Source IP: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 4.Identify the Host Type • Workstation or Server (Enterprise, Production, Development) o Are critical services being impacted? • Which Domain does the host belong to? 5.Attempt to gather relevant information about the subject user: • Role of employee or partners involved (Executive, etc.) • Search Active Directory Users and Computers: a.) Get employee or service account owner's full name b.) Group membership, account history, notes c.) Lookup contact information, review role 6.Confirm the time of the failed login. The time SIEM tool received the event may not be the time the activity occurred. 7.Check the AV status of the Host. • If analyst have the access of respective AV solution, then observe the following: o Version: o Last scan performed: o Risk: • If analyst don't have the access of AV portal, then ask the concern team to check the same. 8.Note that this rule triggers only when failed login attempts were observed from an expired account. 9.Research in past 30 days' logs for any malicious or suspicious activity of the account. 10..Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them : a. Delete the account from AD, if the account is not in use. b. Check and confirm it was an authorized activity or not. c. Perform the compete scan of the host with updated antivirus and share the report with SOC. d. Please update the ticket accordingly.
Multiple users email forwarded to same destination	0		1. Check the source IP/IPs involved in the activity. 2. If the source is external, gather relevant information about the source IP from open online sources: · Source IP: · Blacklisted Status: · ISP: · Domain Name: · Location of the IP: 3.Check the source IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			• AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 4. Check for past 30 days' logs for any suspicious activity performed from the same Source IP. 5. Check the username (UserId), who performed this action. 6. Check if any user was privileged or not. If yes, increase the severity. 7. Search for the past 30 days for any other suspicious activity from the same username. 8. Check the target user (ObjectID) and can also check the complete address in the payload e.g. {"Name":"ForwardingSmtpAddress","Value":"smtp:payroll@xyz.com"}. 9. Check the Originating Server Name and IP address. 10. Check the number of users sending mails to the Forwarding SMTP address. 11. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them: a. Check with the user who performed this activity is authorized to do that or not. b.Ask to block the source IP if external and malicious. c.Check with the client whether the forwarding SMTP address is internal and legit to their environment or not. d.If not, then modify the settings not to forward the mail to that particular address. e. Block the external mail address. f. Disable compromised accounts or reset passwords. g. Remove unauthorized forwarding rules. h.Communicate with affected parties and provide guidance on securing their accounts. i. Please update the ticket accordingly
New internet-exposed SSH endpoints	0		1.Identify source IP associated with this activity. 2.Check for reputation of the IP on online databases and if the result is bad reputation, increase the severity of the alert. If the source is external, gather relevant information about the source IP from open online sources:Virustotal.com,abuseipdb.com, ipvoid.com • Source IP: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 3.Check the Source Host related to this activity. 4.Check if the source host is a critical server or not. If yes, increase the severity. 5.Check if there has been any alert for compromise on this host in any of your AV service or Security subscriptions like Defender. 6.Search for past 24 hr/lat 30 days logs based on source IP and check, · All successful login from the same IP. · Any got successful for MFA authentication? · If any other suspicious activity is detected from same source IP 7. Search for past 24 hr/last 30 days logs based on User/Account and check, · If this user has tried to login from multiple locations. · If this user has had a high number of failed logins in the recent past with no successful logins. · If this user committed any activity after the triggering of this alert that is suspicious or critical. · Check if the user if he/she has tried to login from a different IP or service provider or location which may explain the use of public IP address. 8. Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them as :

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			a. Please check if system (in case of internal IP) is infected or not, if yes isolate system from the network and try to remediate. b. If Source IP is highly malicious, kindly block the IP. c. Make appropriate changes to the settings if you don't want public IP addresses to access this endpoint. d. If any privileged activity or critical activity has been seen from this user, recommend to block the user until the issue is resolved. e. Please update the ticket accordingly
SSH - Potential Brute Force	0		1.Identify source IP(s) associated with this activity from the events over sentinel. 2.Check the External/malicious IP (towards/from which connections are detected) in multiple online Reputation tools and find, All details of this IP: Source IP: · Blacklisted Status: · ISP: · Domain Name: · Location of the IP: 2.Check the source IP address reputation on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 3.Check the User(s)/Accounts related to this activity. 4.Check if any successful login was seen for the User/Account from the same source IP. 5.Check the system associated with this activity and check with respective team if any risk was detected on system in past 30 days. 6.check last 30 days logs for knowing: a.From how long these failed authentications were happening; b.Are other IP addresses also generating similar alerts; c.What kind of failed authentications are being observed? 7.Search for successful authentication events from this particular source. 8.Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing and assign it to the concerned team.
Web Reconnaissance/Unauthorised Scanning Activities Detected	0		1.Look into the details of the alert to understand what specific reconnaissance or scanning activities were detected. This may include details about IP addresses, the type of scans, and other relevant information. 2.Identify the Source Host Name(s) and IP Address: If the source is external, gather relevant information about the source IP from open online sources:Virustotal.com,abuseipdb.com, ipvoid.com • Source IP: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 3.check Azure diagnostics logs using below query for last 30 days: Azurediagnostics | where Ip address contains "x.x.x.x" by selecting the "Time range" matching with alert timeline, to find out outcome of the malicious web requests made by the IP flagged in the alert. AzureDiagnostics | search "IP" | summarize count()by TimeGenerated, Message, requestUri_s, httpMethod_s, httpStatus_d, client_ip_s, host_s, ResourceGroup, WAFMode_s, serverStatus_s, action_s, details_message_s, originalHost_s 4.Search for the last 30 days activities based on the source IP and see the trend: - Check if the source host has history of suspicious activity like connection to known malicious hosts, etc. - Check if any suspicious traffic was observed to and from the source host which could compromise the host. 5.Check targeted resource groups, requested uri, web request methods (Put,Post,Get,Delete) used and header to see if any malicious activity has been observed or not, if observed Notify the team to take necessary actions. 6.Check the Http status codes for the requests in the logs. If the http status codes are 300s or 400s or 500s, then the confidured WAF has detected/matched/blocked the web requests coming out of that IP. If the requests were blocked close the alert as True positive (If IP is malicious) or False Positive (If IP is not malicous). 7.If the Http status codes is 200 success codes, then need to investigate further about which host is affected, if any sign-ins, inbound/outbound traffic is seen coming out of that malicious IP and for how long.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			8.If activity is determined malicious, escalate to respective resolver group Get the IP blocked by adding them in NSG and update malicousIPWatchlist by adding the malicous IP flagged in the alert. 9. If IP & domain are blacklisted kindly recommend to : a.get them blocked with the help of Onshore team. b.Check with the actor if the activity is legitimate or not. c.Any systems that are found to be compromised should be immediately isolated and remediated to prevent further damage. d.Perform a complete AV scan of the target machine with the updated AV. e.Kindly update the ticket accordingly.
Anomalous / Unknown Web Requests Detected	0		1.Check entity details by checking events over sentinel to see what type of traffic is observed using which IP. 2. Identify the Source Host Name(s) and IP Address: If the source is external, gather relevant information about the source IP from open online sources:Virustotal.com,abuseipdb.com, ipvoid.com • Source IP: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 3.check Azure diagnostics logs using below query for last 30 days: Azurediagnostics | where Ip address contains "x.x.x.x" 4.Search for the last 30 days activities based on the source IP and see the trend: - Check if the source host has history of suspicious activity like connection to known malicious hosts, etc. - Check if any suspicious traffic was observed to and from the source host which could compromise the host. 5.check & collect details about IP like any uri's are captured for 200(HTTPS success code) using step3 Kql query. Conditions: a.If 200 success code observed for captured uri's for respected time kindly escalate it to respected resolver group b.If there is no 200 success code for captured uri's and captured ip reputtaion is good,consider it as Benign positive 6.Ensure comprehensive logging of web requests, including source and destination IP addresses, URLs, and user agents. 7.Gather additional context, such as user roles, time of day, and historical behavior, to determine the significance of the anomaly. 8.Using "DeviceEvents" or "DeviceNetworkEvents", check machine timeline for suspicious activities. 9. If the above steps reveal abnormal behaviors or signs of compromise, it is necessary to confirm the incident,then escalate to L2/L3 security member for further investigation. 10. If IP & domain are blacklisted kindly recommend to : a.get them blocked with the help of Onshore team. b.Check with the actor if the activity is legitimate or not. c.Any systems that are found to be compromised should be immediately isolated and remediated to prevent further damage. d.Perform a complete AV scan of the target machine with the updated AV. e.Kindly update the ticket accordingly.
TI map IP entity to AzureActivity	0		1.Check the External/malicious IP (towards/from which connections are detected) in multiple online Reputation tools and find, All details of this IP: Source IP: · Blacklisted Status: · ISP: · Domain Name: · Location of the IP: 2.Check the source IP address reputation on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 3.Search past 30 days FW logs from source and Destination IP. 4.check and Collect the details about: a.check Requested connection Type b.Connection observed on which port c.Frequency of those request

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			d.Firewall action(Accept/block) if action is allowed kindly raise it with concerned team. e.No. of return traffic and ports 5.If the connection is http/https, check past 24 hr proxy logs based on source IP and search for requested URL if present. If requested URL is observed, then check its reputation in online tools. 6.Check if there is any reverse traffic detected from malicious IP towards internal IPs in past 30 days. 7.Review the Azure activity logs for any activity linked to the flagged IP addresses. we need to pay special attention to Security, System, and Application event logs. Look for any unusual or suspicious patterns such as repeated failed logins, access attempts to sensitive resources, or software installation attempts. 8.Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team also Check with the respective team for AV status of internal IP/Host reported in the Alert.
Critical or High Severity Detections by User	0		1.This rule detects events from security device – Crowdstrike under High severity detection by User. Identify the threat for which alert triggered and check for risks associated with it. 2.Identify all the Host Name(s) & Source IP Addresses •What type of data is contained on that device? -Devices containing sensitive data (i.e. PII) are a higher priority for remediation If the source is external, gather relevant information about the source IP from open online sources:Virustotal.com,abuseipdb.com, ipvoid.com • Source IP: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 3.Identify the Host Type: •Which Domain does the host belong to? •What is the MAC Address? 4.Search for past 30 days logs based on host IPs and try to identify user who has done this activity. Also Check if any other suspicious activity is detected on same host in past 30 days. 5.Check with respective team for AV reports of hosts and check if any risk was detected on system in past 30 days. 6.Identify if any source user is associated with activity and check, •Was this a 'privileged' account? •Was this account associated as a Service account? If a service account, who is the owner of the service account? 7.Search for the past 30 day activities based on the Severity and see the trend - Check for any suspicious activities . 8.Develop historical context associated with the machine. For example, does this machine have a history of lockouts or malware infections, has the machine generated alerts that were not sent to SIEM tool. 9.check other activities for captured IP,host and account using below kql query for last 30 days: Security incident | where IP or username or host contains "x.x.x.x" 10.Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them as: a.Please check if the activity was authorized by checking if the system is infected or not. If yes, isolate systems from the network and try to remediate b.Please check how these threat detection events were raised on hosts and if any vulnerability is discovered. c.If activity is not legitimate, check for all the actions performed towards alerted hosts. d.Perform complete scan on system with updated AV and make sure system is clean in the scanned report. If not, look upon mitigating the threat as per report. e.If any user is associated with activity, please check with user for purpose behind such activity if necessary raise user awareness. f.Update ticket accordingly.
Critical Severity Detection	0		1.This rule detects events from security device – Crowdstrike under ctitical severity detection. Identify the threat for which alert triggered and check for risks associated with it. 2.Identify all the Host Name(s) & Source IP Addresses •What type of data is contained on that device? -Devices containing sensitive data (i.e. PII) are a higher priority for remediation

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			the source is external, gather relevant information about the source IP from open online sources:Virustotal.com,abuseipdb.com, ipvoid.com • Source IPIf: • Source Port(s): • Blacklisted Status: • ISP: • Domain Name: • Location of the IP: kindly check the reputation of IP using online platforms like : https://www.ipvoid.com/ip-blacklist-check/ https://scamalytics.com/ip https://db-ip.com/ https://mxtoolbox.com/blacklists.aspx https://www.virustotal.com/gui/home/search https://exchange.xforce.ibmcloud.com/ https://www.talosintelligence.com/ https://www.abuseipdb.com/ https://www.talosintelligence.com/ 3.Identify the Host Type: •Which Domain does the host belong to? •What is the MAC Address? 4.Search for past 30 days logs based on host IPs and try to identify user who has done this activity. Also Check if any other suspicious activity is detected on same host in past 30 days. 5.Check with respective team for AV reports of hosts and check if any risk was detected on system in past 30 days. 6.Identify if any source user is associated with activity and check, •Was this a 'privileged' account? •Was this account associated as a Service account? If a service account, who is the owner of the service account? 7.Search for the past 30 day activities based on the Severity and see the trend - Check for any suspicious activities . 8.Develop historical context associated with the machine. For example, does this machine have a history of lockouts or malware infections, has the machine generated alerts that were not sent to SIEM tool. 9.check other activities for captured IP,host and account using below kql query for last 30 days: Security incident | where IP or username or host contains "x.x.x.x" 10.Based on the above information, if the activity seems to be suspicious, create a ticket using the ticketing tool and assign it to the concerned team and recommend them as: a.Please check if the activity was authorized by checking if the system is infected or not. If yes, isolate systems from the network and try to remediate b.Please check how these threat detection events were raised on hosts and if any vulnerability is discovered. c.If activity is not legitimate, check for all the actions performed towards alerted hosts. d.Perform complete scan on system with updated AV and make sure system is clean in the scanned report. If not, look upon mitigating the threat as per report. e.If any user is associated with activity, please check with user for purpose behind such activity if necessary raise user awareness. f.Update ticket accordingly.
D365 - Audit log configuration change	0		1. When SOC team observes a "D365 - Audit log configuration change" alert in Sentinel, it should be treated on priority because it plays a crucial step in identifying change in Security Audit Configuration. 2. Check for any pre-notification received or any ticket raised that could trigger this alert in last 30 days. a. In such case this activity should be consider as authorized activity. b. If no notification is found, you will need to raise a ticket for the same alert 3. Check the events captured due to which alert is triggered. 4. Verify, if necessary, conditions for alert is matched. 5. Check the details and reputation of the Client IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the IP address on open threat websites. Reference websites: • VirusTotal: https://www.virustotal.com • AlienVault OTX: https://otx.alienvault.com/ • IBM XForce: https://exchange.xforce.ibmcloud.com/ • AbuseIPDB: https://www.abuseipdb.com/ 6. Take a detailed look at the IPs in the alert trigger. This can help you understand the behaviour and help analyses if it is suspicious or not. https://ipinfo.info/html/tcp-ip-ports.php 7. Search for past last 30days activity based on the targeted IP(s) and check the activities done by it and if those seems suspicious or not. 8. Check for other suspicious activities observed around the time of the alert. 9.check below neccessary tables for more investigation to trace out about suspicious activity: Step 1. //replace xyz with the username/ip address found in alert. search "xyz"

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps

			| distinct $table
			With all the table available go through different table where the username/ipaddress is captured using the table name
			Step 2
			//Replace the table name with the table name found in step 1. Repeat for all the tables found in step 1
			TableName
			//use the username/ipaddress between ""
			| where * has ""
			10.Kindly use the below mentioned KQl query for further investigation :
			Dynamics365Activity
			| Where * has "username or Ipaddress"
			11.check necessary fields from the above kql query like "TimeGenerated, UserId, AccountName, UPNSuffix, UserType, ClientIP, EntityName, Message, OriginalObjectId, ResultStatus, InstanceUrl, UserAgent, Type, and Fields" from the logs and this field indicates exact operation performed by captured user.
			12. Confirm the time of activity. The time SIEM tool received the event may not be the time the activity occurred.
			13. Based on the above information, if the activity seems to be suspicious then escalate to respective resolver groups for further investigation and recommed to:
			Recommendations:
			a. Kindly Confirm if there was a scheduled change request to modify the audit log settings or not
			b. please confirm with the application owner if this was an approved task or not
			c. Kindly check with the actor if they modified the settings,if not immediately reset the user password and isolate the infected machine.
			d. Regularly review and update audit log configuration based on changes in business requirements, regulatory standards, or system updates.

D365 - Audit log data deletion	0		1. When SOC team observes a "D365 - Audit log data deletion'' alert in Sentinel, it should be treated on priority because it plays a crucial step in identifying audit log data deletion activity in Dynamics 365.
			2. Check for any pre-notification received or any ticket raised that could trigger this alert in last 30 days.
			a. In such case this activity should be consider as authorized activity.
			b. If no notification is found, you will need to raise a ticket for the same alert
			3. Check the events captured due to which alert is triggered.
			4. Verify, if necessary, conditions for alert is matched.
			5. Check the details and reputation of the Client IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the IP address on open threat websites.
			Reference websites:
			• VirusTotal: https://www.virustotal.com
			• AlienVault OTX: https://otx.alienvault.com/
			• IBM XForce: https://exchange.xforce.ibmcloud.com/
			• AbuseIPDB: https://www.abuseipdb.com/
			6. Take a detailed look at the IPs in the alert trigger. This can help you understand the behaviour and help analyses if it is suspicious or not.
			https://ipinfo.info/html/tcp-ip-ports.php
			7. Search for past last 30days activity based on the targeted IP(s) and check the activities done by it and if those seems suspicious or not.
			8. Check for other suspicious activities observed around the time of the alert.
			9.check below necessary tables for more investigation to trace out about suspicious activity:
			Step 1.
			//replace xyz with the username/ip address found in alert.
			search "xyz"
			| distinct $table
			With all the table available go through different table where the username/ipaddress is captured using the table name
			Step 2
			//Replace the table name with the table name found in step 1. Repeat for all the tables found in step 1
			TableName
			//use the username/ipaddress between ""
			| where * has ""
			10.Kindly use the below mentioned KQl query for further investigation :
			Dynamics365Activity
			| Where * has "username or Ipaddress"
			11.Check necessary fields from the above kql query like "TimeGenerated, UserId, AccountName, UPNSuffix, UserType, ClientIP, EntityName, Message, OriginalObjectId, ResultStatus, InstanceUrl, UserAgent, Type, and Fields" from the logs and this field indicates exact operation performed by captured user.
			12. Confirm the time of activity. The time SIEM tool received the event may not be the time the activity occurred.
			13. Based on the above information, if the activity seems to be suspicious then escalate to respective resolver groups for further investigation and recommend to:
			Recommendations:
			a. Kindly Confirm if there was a scheduled change request to delete the audit logs or not.
			b. please confirm with the application owner if this was an approved task or not.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			c. Kindly check with the actor if they deleted the logs, if not immediately reset the user password and isolate the infected machine. d. Configure retention policies within Dynamics 365 or leverage external data management solutions to streamline the deletion process. e. Implement monitoring mechanisms to track compliance with audit log data deletion policies. Monitor the execution of deletion tasks, verify that retention periods are being adhered to, and generate audit reports to demonstrate compliance with regulatory requirements.

D365 - Dormant admin or previously non-admin user conducting admin activity	0		1. When SOC team observes a "D365 - Dormant admin or previously non-admin user conducting admin activity" alert in Sentinel, it should be treated on priority because it plays a crucial step in identifying, Monitors and detects dormant admins or previously non-admin users currently conducting admin activities in Dynamics 365.
			2. Check for any pre-notification received or any ticket raised that could trigger this alert in last 30 days.
			a. In such case this activity should be consider as authorized activity.
			b. If no notification is found, you will need to raise a ticket for the same alert
			
			3. Check the events captured due to which alert is triggered.
			4. Verify, if necessary, conditions for alert is matched.
			5. Search for past last 30days activity based on the targeted user and check the activities done by it and if those seems suspicious or not.
			6.Check for other suspicious activities observed around the time of the alert.
			7.Check the details and reputation of the Client IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the IP address on open threat websites.
			Reference websites:
			• VirusTotal: https://www.virustotal.com
			• AlienVault OTX: https://otx.alienvault.com/
			• IBM XForce: https://exchange.xforce.ibmcloud.com/
			• AbuseIPDB: https://www.abuseipdb.com/
			8.Take a detailed look at the IPs in the alert trigger. This can help you understand the behaviour and help analyses if it is suspicious or not.
			https://ipinfo.info/html/tcp-ip-ports.php
			9.Search for past last 30days activity based on the targeted IP(s) and check the activities done by it and if those seems suspicious or not.
			10.check below neccessary tables for more investigation to trace out about suspicious activity:
			Step 1.
			//replace xyz with the username found in alert.
			search "xyz"
			| distinct $table
			With all the table available go through different table where the username/ipaddress is captured using the table name
			Step 2
			//Replace the table name with the table name found in step 1. Repeat for all the tables found in step 1
			TableName
			//use the username/ipaddress between ""
			| where * has ""
			11.Kindly use the below mentioned KQl query for further investigation :
			Dynamics365Activity
			| Where * has "username/Ipaddress "
			or
			Kindly check Audit logs table to identifying user roles and for any malicious admin activities performed in last 30 days.
			KQL Query:.
			Auditlogs
			| where * has "userprincipal name"
			12.check necessary fields from the above kql query like "timestamp, AccountName,UPNSuffix,UserId.
			13. Confirm the time of activity. The time SIEM tool received the event may not be the time the activity occurred.
			14. Based on the above information, if the activity seems to be suspicious then escalate to respective resolver groups for further investigation and recommend to:
			Recommendations:
			a. Confirm audit logs to confirm PIM role activation
			b. please confirm with the application owner if this was an approved task or not
			c. kindly check with user what is the intention behind configuration changes, if its expected activity kindly provide business justification.
			d. If it's an unauthorized activity, kindly reset the user password and isolate the infected machine.

D365 - Mass deletion of records	0		1. When SOC team observes a "D365 - Mass deletion of records" alert in Sentinel, it should be treated on priority because it plays a crucial step in identifying large scale delete operations where the number of delete entries exceeds a query defined threshold within the last period. The scheduling of bulk delete jobs in Dynamics 365 is also detected. 2. Check for any pre-notification received or any ticket raised that could trigger this alert in last 30 days.

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps

			a. In such case this activity should be consider as authorized activity.
			b. If no notification is found, you will need to raise a ticket for the same alert
			
			3. Check the events captured due to which alert is triggered.
			4. Verify, if necessary, conditions for alert is matched.
			5. Search for past last 30days activity based on the targeted user and check the activities done by it and if those seems suspicious or not.
			6.Check for other suspicious activities observed around the time of the alert.
			7.check below neccessary tables for more investigation to trace out about suspicious activity:
			Step 1.
			//replace xyz with the username found in alert.
			search "xyz"
			| distinct $table
			With all the table available go through different table where the username is captured using the table name
			Step 2
			//Replace the table name with the table name found in step 1. Repeat for all the tables found in step 1
			TableName
			//use the username between ""
			| where * has ""
			8.Kindly use the below mentioned KQl query for further investigation :
			Dynamics365Activity
			| Where * has "username "
			9.check necessary fields from the above kql query like "UserId, Message, EntityName, InstanceUrl, and OriginalObjectId.
			10. Confirm the time of activity. The time SIEM tool received the event may not be the time the activity occurred.
			11. Kindly collect the details about Mass deletion activity using step 8.
			12. Based on the above information, if the activity seems to be suspicious then escalate to respective resolver groups for further investigation and recommmed to:
			Recommendations:
			a. Kindly Confirm if there was a scheduled change request to delete the records or not.
			b. please confirm with the application owner if this was an approved task or not.
			c. Kindly check with the actor if they deleted the records, if not immediately reset the user password and isolate the infected machine.
			d. kindly check reason behind these mass deletion of records, if its expected activity from user kindly provide business justification.

D365 - Mass export of records to Excel	0		1. When SOC team observes a "D365 - Mass export of records to Excel'' alert in Sentinel, it should be treated on priority because it plays a crucial step in identifying if the user exporting a large amount of records from Dynamics 365 to Excel, significantly more records exported than any other recent activity by that user.
			2. Check for any pre-notification received or any ticket raised that could trigger this alert in last 30 days.
			a. In such case this activity should be consider as authorized activity.
			b. If no notification is found, you will need to raise a ticket for the same alert
			3. Check the events captured due to which alert is triggered.
			4. Verify, if necessary, conditions for alert is matched.
			5. Search for past last 30days activity based on the targeted user and check the activities done by it and if those seems suspicious or not.
			6.Check for other suspicious activities observed around the time of the alert.
			7.Check the details and reputation of the Client IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the IP address on open threat websites.
			Reference websites:
			• VirusTotal: https://www.virustotal.com
			• AlienVault OTX: https://otx.alienvault.com/
			• IBM XForce: https://exchange.xforce.ibmcloud.com/
			• AbuseIPDB: https://www.abuseipdb.com/
			8.Take a detailed look at the IPs in the alert trigger. This can help you understand the behaviour and help analyses if it is suspicious or not.
			https://ipinfo.info/html/tcp-ip-ports.php
			9.Search for past last 30days activity based on the targeted IP(s) and check the activities done by it and if those seems suspicious or not.
			10.check below neccessary tables for more investigation to trace out about suspicious activity:
			Step 1.
			//replace xyz with the username found in alert.
			search "xyz"
			| distinct $table
			With all the table available go through different table where the username/ipaddress is captured using the table name
			Step 2
			//Replace the table name with the table name found in step 1. Repeat for all the tables found in step 1
			TableName
			//use the username/ipaddress between ""
			| where * has ""

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			11.Kindly use the below mentioned KQl query for further investigation : Dynamics365Activity | Where * has "username/Ipaddress " 12.check necessary fields from the above kql query like "UserId,CurrentExportRate,Client ip EntityName, InstanceUrl, and OriginalObjectId. 13. Confirm the time of activity. The time SIEM tool received the event may not be the time the activity occurred. 14. Kindly collect the details about Mass deletion activity using step 8. 15. Based on the above information, if the activity seems to be suspicious then escalate to respective resolver groups for further investigation and recommend to: Recommendations: a. Kindly Confirm if there was a scheduled change request to export the records or not b. please confirm with the application owner if this was an approved task or not c. Kindly check with the actor if they exported the records, if not immediately reset the user password and isolate the infected machine. d. kindly check with user intention behind export of records, if its expected activity kindly provide business justification.

D365 - Monitored Security configuration changed	0		1. When SOC team observes a "D365 - Monitored Security configuration changed" alert in Sentinel, it should be treated on priority because it plays a crucial step in identifying security configuration changes in Dynamics 365 based on a watchlist. The watchlist deployed as part of the Dynamics 355 Continuous Threat Monitoring Solution contains common security configuration related changes and can be modified to tune which events generate an alert.
			2. Check for any pre-notification received or any ticket raised that could trigger this alert in last 30 days.
			a. In such case this activity should be consider as authorized activity.
			b. If no notification is found, you will need to raise a ticket for the same alert
			
			3. Check the events captured due to which alert is triggered.
			4. Verify, if necessary, conditions for alert is matched.
			5. Search for past last 30days activity based on the targeted user and check the activities done by it and if those seems suspicious or not.
			6.Check for other suspicious activities observed around the time of the alert.
			7.Check the details and reputation of the Client IP from the online tools to know if the IP has been reported recently for any suspicious activity. Check the IP address on open threat websites.
			Reference websites:
			• VirusTotal: https://www.virustotal.com
			• AlienVault OTX: https://otx.alienvault.com/
			• IBM XForce: https://exchange.xforce.ibmcloud.com/
			• AbuseIPDB: https://www.abuseipdb.com/
			8.Take a detailed look at the IPs in the alert trigger. This can help you understand the behaviour and help analyses if it is suspicious or not.
			https://ipinfo.info/html/tcp-ip-ports.php
			9.Search for past last 30days activity based on the targeted IP(s) and check the activities done by it and if those seems suspicious or not.
			10.check below neccessary tables for more investigation to trace out about suspicious activity:
			Step 1.
			//replace xyz with the username found in alert.
			search "xyz"
			| distinct $table
			With all the table available go through different table where the username/ipaddress is captured using the table name
			Step 2
			//Replace the table name with the table name found in step 1. Repeat for all the tables found in step 1
			TableName
			//use the username/ipaddress between ""
			| where * has ""
			11.Kindly use the below mentioned KQl query for further investigation :
			Dynamics365Activity
			| Where * has "username/Ipaddress "
			or
			Kindly check Audit logs table to identifying user roles in last 30 days.
			KQL Query:.
			Auditlogs
			| where * has "usename"
			12.check necessary fields from the above kql query like "UserId,Client ip, EntityName, InstanceUrl, and OriginalObjectId.
			13. Confirm the time of activity. The time SIEM tool received the event may not be the time the activity occurred.
			14. Based on the above information, if the activity seems to be suspicious then escalate to respective resolver groups for further investigation and recommend to:
			Recommendations:
			a. Kindly Confirm if there was a scheduled change to add or replace privileges.
			b. please confirm with the application owner if this was an approved task or not

UC Name	Total Count (Last 3 month data)	Tools/KQL Queries	Triaging Steps
			c. Kindly check with the actor if they modified the privileges,if not immediately reset the user password and isolate the infected machine. d. kindly check with user what is the intention behind configuration changes, if its expected activity kindly provide business justification.