A picture containing drawing, light

Description automatically generated

Q-P07-W370 SECURITY Incident Remediation  
Playbook

Business technology

Version Number 1.0

1 November 2022

Contents

[Introduction 3](#_Toc124420335)

[Document Overview 3](#_Toc124420336)

[Purpose 3](#_Toc124420337)

[Scope 3](#_Toc124420338)

[1. Incident Remediation Processes – Priority 1 4](#_Toc124420339)

[Ransomware, Malware 4](#_Toc124420340)

[Initial Access - Remote Access - Account Created 5](#_Toc124420341)

[Initial Access - Remote Access - Group Change 5](#_Toc124420342)

[Initial Access - Remote Access - Login Attempt - Interactive Login 6](#_Toc124420343)

[Defence Evasion - System Change - Event Logs Cleared 6](#_Toc124420344)

[2. Incident Remediation Processes – Priority 2 7](#_Toc124420345)

[Initial Access - Remote Access - Login Attempt - Admin Account 7](#_Toc124420346)

[Command and Control - Access Attempt - CnC IP - High Conf 7](#_Toc124420347)

[Command and Control - Network - Access Attempt - CnC Web Domain 8](#_Toc124420348)

[Command and Control - Access Attempt - Malicious IP 8](#_Toc124420349)

[Discovery - Internal - Account Enumeration 9](#_Toc124420350)

[Execution - Internal - User Activity - Web Access - Service Account / Enterprise Admin 10](#_Toc124420351)

[Initial Access - Remote Access - Login Attempt - Different Geos 11](#_Toc124420352)

[Lateral Movement - Internal - User Activity - Abnormal Host 12](#_Toc124420353)

[Persistence - System Change - Domain Policy Changed 12](#_Toc124420354)

[Persistence - System Change - Service Installed 13](#_Toc124420355)

[Privilege Escalation - AD - Account Created - Computer Object 14](#_Toc124420356)

[Lateral Movement - Domain Controller - Login Attempt - Interactive - Service Account 14](#_Toc124420357)

[Credential Access - Internal - User Activity - User of Interest 16](#_Toc124420358)

[3. Incident Remediation Processes – Priority 3 17](#_Toc124420359)

[Privilege Escalation - AD - Group Change - Admin 17](#_Toc124420360)

[Command and Control - Access Attempt - CnC IP – Medium Confidence 17](#_Toc124420361)

[Credential Access - AD - Account Lockout - Admin 18](#_Toc124420362)

[Credential Access - AD - Account Lockout – DOMAIN Admin / Service Account 19](#_Toc124420363)

[Credential Access - O365 - User Activity - Overseas - Account Lockout 20](#_Toc124420364)

[Discovery - Network - Recon Activity - Internal 20](#_Toc124420365)

[Execution - Email - Excessive Outbound 21](#_Toc124420366)

[Exfiltration - Email - Auto Forwarding 21](#_Toc124420367)

[Initial Access – O365 – Login Attempt – Overseas – Success 22](#_Toc124420368)

[Initial Access - Email - Ransomware Campaign – Shipping / Utility 22](#_Toc124420369)

[Initial Access - Email - Spearphishing Campaign 23](#_Toc124420370)

[Initial Access - Remote Access - Login Attempt - Account Enumeration 23](#_Toc124420371)

[Initial Access - Remote Access - Login Attempt - Malicious IP 24](#_Toc124420372)

[Initial Access - Remote Access - Login Attempt – Overseas - Success 24](#_Toc124420373)

[Lateral Movement - Login Attempt - Domain Controller – Interactive - OBH 25](#_Toc124420374)

[Persistence - System Change - New Process Created 26](#_Toc124420375)

[Privilege Escalation - AD - Account Created - OBH 26](#_Toc124420376)

[Initial Access - Email - Phishing Campaign 27](#_Toc124420377)

[4. Incident Remediation Processes – Priority 4 28](#_Toc124420378)

[Discovery - Network - Recon Activity - External 28](#_Toc124420379)

Appendices

**No table of contents entries found.**

Figures

**No table of contents entries found.**

Tables

**No table of contents entries found.**

Introduction

Document Overview

This document provides a high-level overview of incident information and suggested triage and remediation approaches for the most common security incidents detected and reported within Kinetic IT’s environment.

Purpose

The content of this document is intended to aid in investigating and remediating security incidents raised by Business Technology. It is intended to be used as a guide to utilise in conjunction with work instructions and the Information Security Incident Management and Major Incident Management processes.

Scope

In scope

The document will outline the typical security incidents detected and reported within Kinetic IT’s Business Technology and will include the priority classification, cause of the incident, investigation and remediation steps to take if the incident is to occur.

Out of scope

This document will outline the typical incidents which are likely to be encountered by Business Technology. The investigation and remediation information provided is high level and does not cover the intricacies of any particular incident.

# Incident Remediation Processes – Priority 1

The following incidents describe in detail the priority category, what caused the incident and the suggested investigation and remediation required to resolve this incident.

|  |  |
| --- | --- |
| Ransomware, Malware | |
| Priority | Priority 1 |
| Cause | User initiated by clicking on a malicious link or on an endpoint.  Software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system |
| System reported | CrowdStrike alert with the malware code, or unusual user behaviour.  CrowdStrike will automatically stop the process and prevent further proliferation of malware or ransomware. |
| User reported | User has contacted the Business Technology Service Desk advising they have clicked on a link that they feel may be malicious. |
| Investigate | Investigate alerts raised by the monitoring system (CrowdStrike) through platform containing the malware or ransomware.  Network lock within CrowdStrike the device if applicable. [KB0010384]  Evidence is retained within the monitoring systems. |
| Remediate | Contact user/s identified in the alert, request urgent action to disconnect from all networks, do not login again until advised otherwise.  Reset user/s password immediately.  Remove the device account from AD.  Provide swap out device for the user as a work around.  Reimage affected device prior to redeployment from the device pool. |

|  |  |
| --- | --- |
| Initial Access - Remote Access - Account Created | |
| Priority | Priority 1 |
| Cause | An account is created within Active Directory by a user that has accessed the Kinetic IT network remotely. |
| System reported | Alert from SOC |
| Investigate | Check the account is being used by the authorised person.  Confirm the change was authorised. |
| Remediate | If the activity was unauthorised, the accounts can be disabled for further investigation. |

|  |  |
| --- | --- |
| Initial Access - Remote Access - Group Change | |
| Priority | Priority 1 |
| Cause | A successful remote access login followed by any group changes where users have been added/removed from security groups, or groups have been created. |
| System reported | Alert from SOC |
| Investigate | Check the account is being used by the authorised person.  Confirm the change was authorised. |
| Remediate | If the activity was unauthorised the accounts can be disabled for further investigation. |

|  |  |
| --- | --- |
| Initial Access - Remote Access - Login Attempt - Interactive Login | |
| Priority | Priority 1 |
| Cause | Detect instances where a user account has logged into VPN and then initiated an interactive logon to a server. This rule can be extended to check specifically for Admin or Service accounts. |
| System reported | Alert from SOC |
| Investigate | Confirm the account is being used by the authorised person.  Confirm the change was authorised.  If the activity is deemed legitimate, no further action is required. If the activity is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Manually end VPN session.  Disable source user account.  Block the external source IP on the external firewall / VPN appliance. |

|  |  |
| --- | --- |
| Defence Evasion - System Change - Event Logs Cleared | |
| Priority | Priority 1 |
| Cause | The clearing of windows event logs on a host. |
| System reported | Alert from SOC |
| Investigate | Determine the host on which the event logs were cleared and determine which user performed this task. This may involve:   * Follow up with the user to determine if they performed this task. * If the user performed this task, evaluate whether the user is permitted to perform this task and their stated reason for doing so. * Determine if other actions were performed by the user. * If the activity is deemed legitimate, no further action is required. If the activity is deemed suspicious, proceed to remediation.   Request additional information from the SOC as required. |
| Remediate | Lock the account that was used to perform the task.  Check the host for signs of compromise and look for evidence of successful/failed exploit attempts or undesirable changes.  If the host is suspected to be compromised, isolate the host from the network via CrowdStrike, or physically remove from the network and remediate. |

# Incident Remediation Processes – Priority 2

The following incidents describe in detail the priority category, what caused the incident and the suggested investigation and remediation required to resolve this incident.

|  |  |
| --- | --- |
| Initial Access - Remote Access - Login Attempt - Admin Account | |
| Priority | Priority 2 |
| Cause | An account which is part of the defined admin account group(s), logged in successfully via remote access. |
| System reported | Alert from SOC |
| Investigate | Confirm the account is being used by the authorised person.  Confirm the change was authorised.  If the activity is deemed legitimate, no further action is required. If the activity is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Manually end VPN session.  Disable source user account.  Block the external source IP on the external firewall/VPN appliance. |

|  |  |
| --- | --- |
| Command and Control - Access Attempt - CnC IP - High Conf | |
| Priority | Priority 2 |
| Cause | An asset on the Kinetic IT network has contacted a likely Botnet Command & Control server. This is the high confidence rule and the IP address must be listed on 3 out of the 7 bad IP reputation lists. |
| System reported | Alert from SOC. |
| Investigate | Perform malware triage on the identified system [KB0010384].  If the activity is deemed legitimate, no further action is required. If the activity is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident for any remediation details.  Contact the affected user to validate if it is suspicious activity. If yes, block the offending external IP on network perimeter.  If unable to contact the user, consider CrowdStrike network lock [KB0010384] the device.  Isolate the host from the network and investigate for compromise or the presence of hacking tools.  **Workaround**: Issue user with an alternate device from the device pool.  Request user to reset their password as soon as practical. |

|  |  |
| --- | --- |
| Command and Control - Network - Access Attempt - CnC Web Domain | |
| Priority | Priority 2 |
| Cause | Any system within the Kinetic IT network attempting to contact a botnet Command & Control (CnC) server using a known bad web domain. This rule uses web domains rather than IP addresses which have a higher confidence value. |
| System reported | SIEM Incident |
| Investigate | Perform malware triage on the identified system [KB0010384].  Identify any compromised files or accounts.  If the activity is deemed legitimate, no further action is required. If the activity is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident for any remediation details.  Contact the affected user to validate if it is suspicious activity. If yes, block the offending external IP on network perimeter.  If unable to make contact with the user, consider CrowdStrike network lock [KB0010384] the device.  Isolate the host from the network and investigate for compromise or the presence of hacking tools.  **Workaround**: Issue user with an alternate device from the device pool.  Request user to reset their password as soon as practical. |

|  |  |
| --- | --- |
| Command and Control - Access Attempt - Malicious IP | |
| Priority | Priority 2 |
| Cause | Any system within the Kinetic IT network attempting to contact a known malicious IP address. This rule uses a list of malicious IP address from a well-known security vendor and it has a high confidence rating. |
| System reported | SIEM Incident |
| Investigate | Perform malware triage on the identified system.  Identify any compromised files or accounts.  If the activity is deemed legitimate, no further action is required. If the activity is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident for any remediation details.  Contact the affected user to validate if it is suspicious activity. If yes, block the offending external IP on network perimeter.  If unable to make contact with the user, consider CrowdStrike network lock [KB0010384] the device.  Isolate the host from the network and investigate for compromise or the presence of hacking tools.  **Workaround**: Issue user with an alternate device from the device pool.  Request user to reset their password as soon as practical. |

|  |  |
| --- | --- |
| Discovery - Internal - Account Enumeration | |
| Priority | Priority 2 |
| Cause | Multiple failed login attempts for **multiple user accounts** originating from a single source IP. |
| System reported | SIEM Incident |
| Investigate | Verify the legitimacy of the account lockout. This may involve:  Determine the source of the login attempts.  Follow up with the user and determine if the account was locked because of multiple failed logins or some other reason.  Follow up with the user and determine if they were using the device which caused the lockout.  If the activity is deemed legitimate, no further action is required. If the activity is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.  If deemed the source is from **one workstation**, contact the affected user to validate if it is suspicious activity. If yes, block the offending external IP on network perimeter.  If unable to contact the user, consider CrowdStrike network lock [KB0010384] the device.  Isolate the host from the network and investigate for compromise or the presence of hacking tools.  Request user to reset their password as soon as practical.  If deemed the source **other than a workstation**, such as **a server, cloud service, network device, software as a service, engage** Major Incident Management.Isolate the source from the network. |

|  |  |
| --- | --- |
| Execution - Internal - User Activity - Web Access - Service Account / Enterprise Admin | |
| Priority | Priority 2 – UNDISCLOSED INCIDENT |
| Cause | An account which is not expected to access the internet has accessed an external resource. This may be an indicator of account misuse, host misconfiguration or host compromise. |
| System reported | SIEM Incident |
| Investigate | Verify the legitimacy of the web activity. This may involve:  Determine whether the account should be accessing external resources as part of its function.  Determine whether the resources accessed are in line with the accounts expected function / expected use.  If the activity is deemed legitimate, no further action is required. If the activity is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.  Lock the AD account, isolate the host from the network and investigate for compromise or the presence of hacking tools.  Collect evidence as part Information Security Incident Management process. |

|  |  |
| --- | --- |
| Initial Access - Remote Access - Login Attempt - Different Geos | |
| Priority | Priority 2 |
| Cause | Multiple successful remote access login attempts which occur from different geographical locations. |
| System reported | SIEM incident |
| Investigate | Determine whether the user that initiated the login is currently expected to be in either of the locations mentioned in the incident. This may involve:  Contacting the user to determine their current geographical location.  If the activity is deemed legitimate, no further action is required. If the activity is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.  Contact the user to determine if they are in the location mentioned in the incident record. [KB00010021]  End any current remote access sessions. Lock the account, change the password and block the external source IP at the network perimeter.  Check for any recent activity that looks suspicious:   * Recent file uploads/downloads * Sent emails * Viewed documents * SharePoint page views * Network infrastructure / systems changes   If data exfiltration is suspected or undesirable infrastructure / systems changes have occurred, assess the impact to Kinetic IT and remediate. |

|  |  |
| --- | --- |
| Lateral Movement - Internal - User Activity - Abnormal Host | |
| Priority | Priority 2 |
| Cause | An asset within Kinetic IT’s network uses an abnormal host identifier. These hosts are often the default within tools included suites such as Kali. |
| system reported | SIEM Incident |
| Investigate | This rule could identify the presence of an unauthorised asset on the network attempting to authenticate:  Team can track down the asset if provided with source IP or other information.  Asset can be isolated to determine what is attempting the authentication requests. |
| Remediate | Refer to the SOC Incident record for any remediation details.  Block the source IP, control list the host identifier to prevent further compromise. |

|  |  |
| --- | --- |
| Persistence - System Change - Domain Policy Changed | |
| Priority | Priority 2 |
| Cause | Any change to domain policy. |
| system reported | SIEM Incident |
| Investigate | Verify the legitimacy of the policy change. This may involve:  Investigate the specific policy change that was made and evaluate its impact to Kinetic IT.  Determine the privileged account that changed the policy and whether the account is permitted to perform this task.  If the change is deemed legitimate, no further action is required. If the change is deemed suspicious, proceed to remediation.  Request additional information from the Kinetic IT SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.  Lock the account that rolled-out the change.  If the change was not approved, roll back domain policy change and investigate cause of change. |

|  |  |
| --- | --- |
| Persistence - System Change - Service Installed | |
| Priority | Priority 2 |
| Cause | The installation of a service on a host that is not excluded by a watchlist. |
| system reported | SIEM Incident |
| Investigate | Verify the legitimacy of the created service. This may involve:  Perform an online reputation check of the service.  Determine **the account** that installed the service and whether the user is permitted to perform this task.  If the service is deemed legitimate, no further action is required. If the service is deemed suspicious, proceed to remediation.  Request additional information from the Kinetic IT SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.  Lock **the account** that installed the service.  If the service is suspicious or does not have a legitimate purpose, stop the service and investigate host for compromise or misconfiguration. |

|  |  |
| --- | --- |
| Privilege Escalation - AD - Account Created - Computer Object | |
| Priority | Priority 2 |
| Cause | An attempt to create an account has been made by a computer object. |
| system reported | SIEM Incident |
| Investigate | Verify the legitimacy of the account creation. This may involve:  Determine whether this behaviour is expected from the computer object.  If the account creation is deemed legitimate, no further action is required. If the account creation is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.  Locate the computer and investigate for compromise or misconfiguration. Remediate as dictated by [KB0010384]  If the Computer object is not supposed to create the account, lock the computer account and follow re-image process [KB0010275]. |

|  |  |
| --- | --- |
| Lateral Movement - Domain Controller - Login Attempt - Interactive - Service Account | |
| Priority | Priority 2 |
| Cause | An interactive login to a domain controller by a service account |
| system reported | SIEM Incident |
| Investigate | Determine which service account initiated the login and whether the service account is permitted to perform this task. This may involve:  Determine whether the access attempt is in line with the account’s expected function/expected use.  Determine if any changes were made by the service account.  Follow up with the service account user to confirm they performed this action.  Other activity which should be investigated includes:   * user/group changes in Active Directory * changes to other services which may be running on the same server such as DNS, File Services etc.   If the login is deemed legitimate, no further action is required. If the login is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.  Check for Change Records that align to the timing and actions being taken by the service account.  If there aren’t any Change Records:   * Lock the service account * Reverse undesirable changes, document actions being taken * Contact the Service Owner for further information |

|  |  |
| --- | --- |
| Credential Access - Internal - User Activity - User of Interest | |
| Priority | Priority 2 |
| Cause | Activity has been observed involving a nominated user of interest. This may be an indicator of account misuse. |
| system reported | SIEM Incident |
| Investigate | Investigate Verify the legitimacy of the observed activity. This may involve:  Determine whether the activity is expected.  Determine the source of the activity (internal vs. external).  Follow up with the user to ascertain whether the account owner performed the recorded actions.  If the activity is deemed legitimate, no further action is required. If the activity is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.   * lock the account * isolate the host from the network * remediate aligned to the Major Incident Management and Information Security Incident Management Processes |

# Incident Remediation Processes – Priority 3

The following incidents describe in detail the priority category, what caused the incident and the suggested investigation and remediation required to resolve this incident.

|  |  |
| --- | --- |
| Privilege Escalation - AD - Group Change - Admin | |
| Priority | Priority 3 |
| Cause | An account has been removed or added to a specified Admin group or groups (e.g. Domain Admins). |
| system reported | SIEM Incident |
| Investigate | Check the user account is being used by the authorised person.  Determine whether the group change was authorised.  Scrutinise whether the destination user requires elevated privileges via the Business Technology contact list.  If the activity is deemed legitimate then no further action is required, if not, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.   * Lock the source user account and reset the password. * Reverse any unauthorised changes |

|  |  |
| --- | --- |
| Command and Control - Access Attempt - CnC IP – Medium Confidence | |
| Priority | Priority 3 |
| Cause | An asset on the Kinetic IT network has contacted a likely Botnet Command & Control server. This is the medium confidence rule and the IP address must be listed on 2 out of the 5 bad IP reputation lists. |
| system reported | SIEM Incident |
| Investigate | Perform malware triage on the identified system.  If the activity is deemed legitimate, no further action is required. If the activity is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.   * Isolate the host from the network * Investigate for compromise or the presence of hacking tools * Remediate aligned to the Information Security Incident Management Process |

|  |  |
| --- | --- |
| Credential Access - AD - Account Lockout - Admin | |
| Priority | Priority 3 |
| Cause | An account lockout event on a user account that is a member of a domain admin group. This may be an indicator of account misuse, host misconfiguration or host compromise. |
| system reported | SIEM Incident |
| Investigate | Verify the legitimacy of the account lockout. This may involve:  Determine the source of the login attempts.  Follow up with the user and determine if the account was locked because of multiple failed logins or some other reason.  Follow up with the user and determine if they were using the device which caused the lockout.  If the activity is deemed legitimate, no further action is required. If the activity is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.   * Isolate the host from the network * Investigate for compromise or the presence of hacking tools * Remediate aligned to the Information Security Incident Management Process |

|  |  |
| --- | --- |
| Credential Access - AD - Account Lockout – DOMAIN Admin / Service Account | |
| Priority | Priority 3 |
| Cause | An account lockout by an account which is either a service account or an domain admin user. This may be an indicator of account misuse, host misconfiguration or host compromise. |
| system reported | SIEM Incident |
| Investigate | Verify the legitimacy of the account lockout. This may involve:  Determine the source of the login attempts.  Follow up with the user and determine if the account was locked because of multiple failed logins or some other reason.  Follow up with the user and determine if they were using the device which caused the lockout.  If the activity is deemed legitimate, no further action is required. If the activity is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.   * Isolate the host from the network * Investigate for compromise or the presence of hacking tools * Remediate aligned to the Information Security Incident Management Process |

|  |  |
| --- | --- |
| Credential Access - O365 - User Activity - Overseas - Account Lockout | |
| Priority | Priority 3 |
| Cause | Multiple failed login attempts have been detected in Office 365, which has subsequently caused a user account to lockout. |
| system reported | SIEM Incident |
| Investigate | Determine if the login attempts were performed by the user in question. This may involve:  Contacting the user to determine their current geographical location.  Determine legitimacy of the login attempts.  If the activity is deemed legitimate, contact user to determine if they have unlocked their account successfully.  If the activity is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.   * Contact user for them to utilise the password reset tool * Ensure password complexity policy is met, and that the user’s credentials match the specified requirements |

|  |  |
| --- | --- |
| Discovery - Network - Recon Activity - Internal | |
| Priority | Priority 3 |
| Cause | An Internal IP address scanning many unique internal hosts within a short period. |
| system reported | SIEM Incident |
| Investigate | Determine which host the reconnaissance activity originated from. This may involve:  Using the source IP and source host name to locate the device.  Contact the user who is expected to be using the device and ascertain what the device was being used at the time listed in the event.  If the activity is deemed legitimate, no further action is required.  If the activity is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.   * Isolate the host from the network * Investigate for compromise or the presence of hacking tools * Remediate aligned to the Information Security Incident Management Process |

|  |  |
| --- | --- |
| Execution - Email - Excessive Outbound | |
| Priority | Priority 3 |
| Cause | A large volume of outbound emails is sent from a single client mailbox. This is an indicator of a compromised or misused mailbox. |
| system reported | SIEM Incident |
| Investigate | Follow up with the user to determine if the volume and type of email was sent deliberately.  If the activity is deemed legitimate, no further action is required. If the activity is deemed suspicious, proceed to remediation. |
| Remediate | Refer to the SOC Incident record for any remediation details.  Isolate the host from the network and investigate for compromise or the presence of hacking tools.  Triage the assets compromised and perform the appropriate clean-up actions such as a reimage.  Investigate the mailbox configuration for suspicious email rules.  If the mailbox is a single-user mailbox; request the user to reset their password.  If the mailbox is a shared mailbox, all users with access should reset their passwords. |

|  |  |
| --- | --- |
| Exfiltration - Email - Auto Forwarding | |
| Priority | Priority 3 |
| Cause | Potential unauthorised transfer of information out of Kinetic IT using email auto-forwarding. This is a common tactic for exfiltrating data from an organisation. |
| system reported | SIEM Incident |
| Investigate | Follow up with the user to determine if the volume and type of email was sent deliberately and whether they are permitted to perform this task.  If the mail is being forwarded to an external mailbox, assess how this aligns with organisational policy and remediate as directed.  If the activity is deemed legitimate, no further action is required. If the activity is deemed suspicious, proceed to remediation. |
| Remediate | Refer to the SOC Incident record for any remediation details.  Investigate the mailbox configuration for suspicious email rules.  Remediate aligned to the Information Security Incident Management Process and Acceptable Use Guidelines – FAQ’s. [See ISMS for these documents](https://kineticitau.sharepoint.com/sites/ISMS/SitePages/Home.aspx). |

|  |  |
| --- | --- |
| Initial Access – O365 – Login Attempt – Overseas – Success | |
| Priority | Priority 3 |
| Cause | Successful login to Microsoft Office365 from a location outside of Australia. |
| System reported | SIEM Incident |
| Investigate | Determine whether the user that initiated the login is currently expected to be overseas. This may involve:  Contacting the user to determine their current geographical location.  If the activity is deemed legitimate, no further action is required.  If the activity is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.  If suspicious:   * lock the account and change the password * Force all current O365 sessions to expire   Check for any recent activity that looks suspicious:   * Recent file uploads/downloads * Sent emails * Viewed documents * SharePoint page views   If data exfiltration is suspected, assess the impact on Kinetic IT and remediate as aligned to Information Security Incident Management process and Major Incident Management Process. [See ISMS for these documents](https://kineticitau.sharepoint.com/sites/ISMS/SitePages/Home.aspx). |

|  |  |
| --- | --- |
| Initial Access - Email - Ransomware Campaign – Shipping / Utility | |
| Priority | Priority 3 |
| Cause | This alarm is designed to pick up any email log events that would indicate an Australian flavoured ‘Ransomware’ campaign. This is different to the phishing email alarm as it is looking for subject line matches rather than geographically dispersed senders. Common keywords seen in ransomware campaigns include lines such as courier, parcel etc. |
| system reported | SIEM Incident |
| Investigate | Investigate the source IP and the source user to determine if the email is suspicious.  Confirm with the user if they were expecting the email or if they are familiar with the origin user.  Advise the recipient to contact the sender directly (telephone is advisable, do not reply to the original email) and confirm the legitimacy of the request. |
| Remediate | Remove any suspicious emails that are detected upon being discovered by the SOC.  Block sender and source IP address. |

|  |  |
| --- | --- |
| Initial Access - Email - Spearphishing Campaign | |
| Priority | Priority 3 |
| Cause | A suspicious email has been delivered to an individual(s) in Kinetic IT with financial authority. Individuals with financial authority are often targeted by financial scams. |
| system reported | SIEM Incident |
| Investigate | Investigate the source IP and the source user to determine if the email is suspicious.  Confirm with the end user if they were expecting an email or if they are familiar with the source user. |
| Remediate | Refer to the SOC Incident record for any remediation details.  Remove any suspicious emails that are detected upon being discovered by the SOC.  Potentially block source user and IP address.  Refer the user to Business Technology communications and Security Matters topics regarding to act cautiously when receiving emails from suspicious sources. |

|  |  |
| --- | --- |
| Initial Access - Remote Access - Login Attempt - Account Enumeration | |
| Priority | Priority 3 |
| Cause | Several user accounts attempting remote access authentication from a single IP address. This is a tactic employed by attackers to ensure they do not lock any accounts out by trying one password per account by attempting thousands of accounts. This tactic is often used to discover accounts with weak or default passwords. |
| system reported | SIEM Incident  Vendor reported |
| Investigate | Determine the source of the login attempts.  Assess the volume of login attempts. If the volume exceeds the threshold for reasonable human behaviour, proceed to remediation. |
| Remediate | Refer to the SOC Incident record for any remediation details.  Refer to details provided by the vendor, where applicable.  Block the external source IP at the network perimeter (firewalls or load balancer).  Re-evaluate account lockout thresholds for users to mitigate the risk of brute-force login attempts. |
|  | |
| Initial Access - Remote Access - Login Attempt - Malicious IP | |
| Priority | Priority 3 |
| Cause | A remote access login attempts from a known malicious IP. This is strong indicator that the offending user account being used has been compromised or an attempt is being made to obtain access. |
| system reporting | SIEM Incident |
| Investigate | This could indicate an attacker trying a set of legitimate credentials they have acquired.  Business Technology team to contact the user to ascertain whether the activity is legitimate. This should involve contacting the user to obtain their external source IP and whether they have recently attempted to login via remote access.  If the user has not tried to login, or the external source IP provided by the user does not match the events provided by the SOC, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.  Block the external source IP at the network perimeter.  Request the user to change their password to a strong password/passphrase. If the user is not contactable, lock their account for the interim. |

|  |  |
| --- | --- |
| Initial Access - Remote Access - Login Attempt – Overseas - Success | |
| Priority | Priority 3 |
| Cause | Successful remote access login from a location outside Australia which may be an indicator of a compromised account. |
| system reporting | SIEM Incident |
| Investigate | Contact the user and confirm the username and true location.  If the activity is deemed legitimate, no further action is required. If the activity is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.  Block the external source IP at the network perimeter.  Request the user to change their password to a strong password/passphrase. If the user is not contactable, lock their account for the interim.  If user is not contactable, contact their manager for further details. |

|  |  |
| --- | --- |
| Lateral Movement - Login Attempt - Domain Controller – Interactive - OBH | |
| Priority | Priority 3 |
| Cause | An interactive login to a domain controller outside business hours. |
| system reporting | SIEM Incident |
| Investigate | Determine which user initiated the login and whether the user is permitted to perform this task. This may involve:   * Determine if any changes were made by the user. * Follow up with the user to confirm they performed this action. * Other activity which should be investigated includes user/group changes in Active Directory or changes to other services which may be running on the same server such as DNS, File Services etc.   If the login is deemed legitimate, no further action is required. If the login is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Refer to the SOC Incident record for any remediation details.  End any current interactive sessions.  Lock the account and change its password.  Investigate host for compromise or misconfiguration. |

|  |  |
| --- | --- |
| Persistence - System Change - New Process Created | |
| Priority | Priority 3 |
| Cause | Creation of a process that is in the suspicious process watchlist. |
| system reported | SIEM Incident |
| Investigate | Investigate the specific process created and check to see if is suspicious or can be utilized in a malicious manner.  Determine which user creates the processes.  If the creations are deemed legitimate, no further action is required. If the change is deemed suspicious, proceed to remediation. |
| Remediate | Lock the account that created the process.  If the process is suspicious or does not have a legitimate purpose, stop the process and investigate host for compromise or misconfiguration.  Determine whether rebuild of the source computer or system is appropriate. |

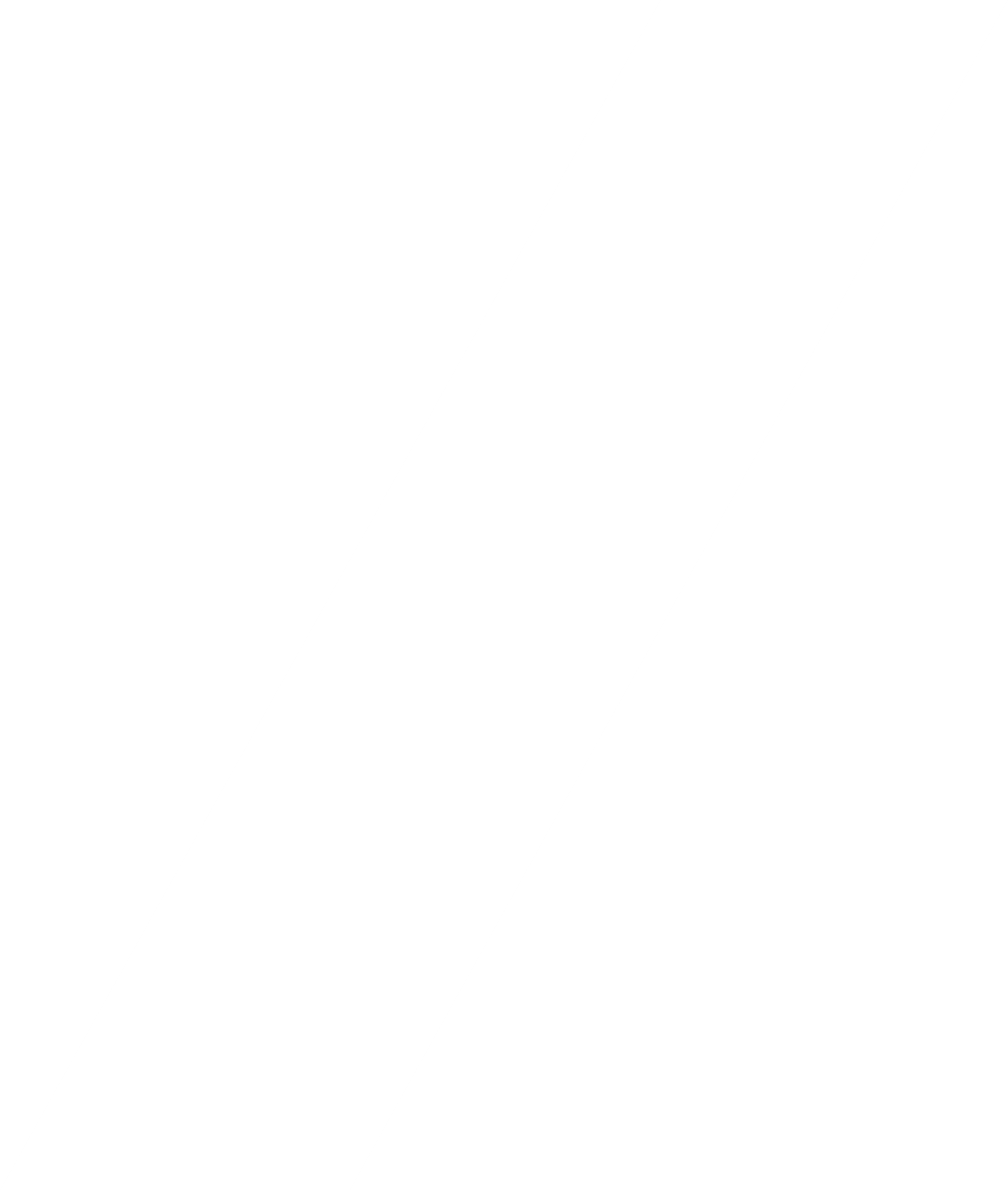
|  |  |
| --- | --- |
| Privilege Escalation - AD - Account Created - OBH | |
| Priority | Priority 3 |
| Cause | An active directory user account has been created outside business hours. |
| system reporting | SIEM Incident |
| Investigate | Verify the legitimacy of the account creation. This may involve:   * If the account was created by a user; follow up with the user who created the account to determine if the action was indeed performed by that user. * Verify whether the user is permitted to perform this task. * If the account was created by a computer object, determine whether this behaviour is expected.   If the account creation is deemed legitimate, no further action is required. If the account creation is deemed suspicious, proceed to remediation.  Request additional information from the SOC as required. |
| Remediate | Locate the computer and investigate for compromise or misconfiguration.  If the user reports that they did not create the account, lock their account and request they change the account’s password. |

|  |  |
| --- | --- |
| Initial Access - Email - Phishing Campaign | |
| Priority | Priority 3 |
| Cause | Potential phishing emails which may contain malicious attachments or attempt to persuade users to send out sensitive information. Phishing campaigns can imitate legitimate businesses. |
| system reporting | SIEM Incident |
| Investigate | Investigate the source IP and the source user to determine if the email is suspicious  Confirm with the end user if they were expecting an email/ are familiar with the source user |
| Remediate | Remove any suspicious emails that are detected upon being discovered by the SOC. Refer to KB0010190.  Potentially block source user and IP address.  Discussed with leadership if an awareness communication is appropriate, depending on the severity of the Phishing Campaign. |

# Incident Remediation Processes – Priority 4

The following incidents describe in detail the priority category, what caused the incident and the suggested investigation and remediation required to resolve this incident.

|  |  |
| --- | --- |
| Discovery - Network - Recon Activity - External | |
| Priority | Priority 4 |
| Cause | This rule has been built to pick up suspicious scanning and reconnaissance events coming from external source IP. |
| system reported | SIEM Incident |
| Investigate | Assess whether the traffic was permitted or dropped by the firewall.  Assess the volume of traffic. |
| Remediate | If the traffic was blocked, either ignore or consider denial of service mitigation strategies (if traffic volume is significant).  If the traffic was allowed, block source IP at network perimeter and consider denial of service mitigation strategies (if traffic volume is significant). |



1300 782 072

[info@kineticit.com.au](mailto:info@kineticit.com.au)

[www.kineticit.com.au](http://www.kineticit.com.au)