***Playbook: Malware Incident Handling\_SOC***

**(Malware security event investigation and response)**

**Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Reason for Change** | **Author** | **Reviewer** |
| 22/10/2022 | 1.0 | Initial Document | Keval Patalamwala | Sunil Mukkamala |

**Vantage Risk Holdings**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Name** | **Title** | **Signature** | **Date** |
| **Reviewed By** |  |  |  |  |
| **Approved By** | Keval Patalamwala | SOC Manager |  |  |
| **Approval By** | Ganesh Patil | Capgemini Security Manager |  |  |
| **Approval By** | Joseph Brown | Vantage AVP, Security & Operations |  |  |
| **Approval By** | Nathan Boylan | Vantage VP, Security & Technical Architecture |  |  |

***This document contains policy and baseline information. ALL INFORMATION CONTAINED HEREIN IS RESTRICTED AND SHALL BE KEPT FOR INTERNAL USE ONLY. None of this information shall be divulged to persons other than Capgemini employees and contractors authorized by the nature of their duties to receive such information or individuals or organizations authorized by Capgemini in accordance with existing policy regarding release of company information.***

Table of Contents

[Overview 4](#_Toc118416975)

[Categories of Malware 4](#_Toc118416976)

[Incident Detection 6](#_Toc118416977)

[CrowdStrike Dashboard and Detections 6](#_Toc118416978)

[Analysis & Investigation 7](#_Toc118416979)

[Guidelines for Investigating any malware related alert 8](#_Toc118416980)

[Observation and Data Collation Table 9](#_Toc118416981)

[Response & Remediation 10](#_Toc118416982)

[CAT-0 (Known 12](#_Toc118416983)

[Malware/Riskware/Adware) 12](#_Toc118416984)

[CAT-1 (Known PUP's) 16](#_Toc118416985)

[CAT-2 (Unknown App/File) 17](#_Toc118416986)

[CAT-3 (OS Files) 19](#_Toc118416987)

[CAT-4 (Freeware) 19](#_Toc118416988)

[CAT -5 (Third Party/Vendor Licensed Application) 20](#_Toc118416989)

[Steps to creating a ticket in Service Now 22](#_Toc118416990)

[Criteria for closure 24](#_Toc118416991)

[Criteria for escalation 24](#_Toc118416992)

[Document Inquiries 25](#_Toc118416993)

[END OF DOCUMENT 26](#_Toc118416994)

# **Overview**

This document includes playbook that defines the procedures for common security event investigation and response. The playbook will allow responders to follow a structured method for validating and responding to each unique security alert. The playbook for each use case is a living document, and needs to be updated to capture the current procedure and unique guidance in order to quickly respond and contain the detected event or incident.

# **Categories of Malware**

|  |  |
| --- | --- |
| Category | Description |
| Ransomware | An application that encrypts data in order to extort the victim to pay a ransom, usually in the form of bitcoins, in exchange for the decryption key to recover their data. |
| Worm | An application that has the capability to spread from one system to another in an automated fashion. |
| Logic bomb | An application that destroys data on systems that it has access to, or is running on. |
|  |  |
| Backdoor | An application that provides remote access to a system outside of the normal remote access functionality that is used on such a system. |
| Hack tool | An application that is utilized to perform hacking operations on an information system, such as password-dumping utilities, privilege escalation applications, network scanners, service impersonation utilities, and more. |
| Adware or potentially unwanted programs | An application that attempts to inject advertisements into the victims computing experience, or other such obtrusive features such as toolbars, utilities, emoticon packs and more. |
| Keylogger | An application that records keystrokes (including confidential credentials) on the victim system and sends them to the attacker. |
| Trojan/remote administration tool (RAT) | Similar to a backdoor, a RAT provides remote access to a system, and typically includes a number of built-in mechanisms found in other categories of malicious code, such as keylogging capabilities, logic bomb capabilities, password dumping capabilities, and more. |
| Denial of service  Malicious code | An application that is primarily designed to perform some type of resource utilization attack, thereby causing degradation in service, or an entire denial of service.  Malicious code refers to all software or otherwise executable instructions on a computer, device or information system with the specific purpose of malicious activity, destruction, or are primarily leveraged to facilitate other malicious activity. Legitimate applications that are being misused and leveraged for malicious purposes are not classified as malicious code. The following table illustrates a variety of types of malicious code. |

# **Incident Detection**

SOC Analyst will monitor the Vantage Holdings using the available Security Tools to Detect all malware related alerts.

Below are the Products or sources using which SOC will detect, or will be notified of, regarding an Incident related to Malware:

|  |  |  |
| --- | --- | --- |
| **Incident Detection Medium** | **Detection Source(Product)** | **Detection Method** |
| **SOC Investigation** | **Azure Sentinel** | **Azure Sentinel Use Case** |
| **SOC Investigation** | **CrowdStrike** | **CrowdStrike Detections** |
| **Direct Reporting by User/Service Desk** | **Email/ Remedy Ticket** | **Direct Communication from User** |

The below Azure Sentinel rules are in place to detect any malware related activity and generate an Alert.

|  |  |
| --- | --- |
| Use Case | Rule |
| To detect possible malware infection | CrowdStrike - Crowdstrike alert detected |
| CrowdStrike - Critical or High Severity Detections by User |
| CrowdStrike - Multiple threats on same host |

**CrowdStrike Dashboard and Detections:** To Acquaint yourself with CrowdStrike and on the best practices for Monitoring the Dashboard and Detections on CS, explore the [**CrowdStrike SOP**](https://teams.microsoft.com/l/file/8F2C18F3-44AB-4240-8976-ECF0D340874A?tenantId=5a5d28b7-2b31-4397-b7b5-a3328b8f8d18&fileType=docx&objectUrl=https%3A%2F%2Fmaxis365.sharepoint.com%2Fsites%2FMaxisSOC%2FShared%20Documents%2FGeneral%2FSOP%2FMaxis_SOP_CrowdStrike_document_v1.1.docx&baseUrl=https%3A%2F%2Fmaxis365.sharepoint.com%2Fsites%2FMaxisSOC&serviceName=teams&threadId=19:4b4a2f8e6d644cbc99f5c99d855433e2@thread.skype&groupId=096a538b-cf5e-431f-8cdb-264f1f616a5f) Document.

SOC Analyst needs to monitor the CrowdStrike Detections and the priority on investigating alerts should directly be based on the Severity of the alert on CS, i.e., A Critical Alert on CS should be investigated and addressed on Priority, followed by High, Medium and Low.

# **Analysis & Investigation**

**For investigating incidents related to malware threats, the below steps and guidelines should be followed.**

**For Investigating Azure Sentinel Alerts, the following information should be collected from the Alerts:**

1. Log Source: This helps in understanding which category of device is triggering the alert and also gives an idea of what is the medium of attack for which the alert is triggered. Eg., If PaloAlto is the Log source, then the alert is detected for FW traffic. If the Log Source is Proxy, then the traffic is related to 80 or 443.
2. Source and Destination IP
3. Source & Destination Port
4. URL/Referrer, if any
5. Traffic Direction
6. Action: Allowed/Deny/Blocked
7. Application/Extension/Browser Plugin initiating the traffic: This helps to locate the underlying source of the traffic specially for network related threats which are initiated by a foreign infection on the host.

**For Investigating CrowdStrike Alerts, the following information should be collected from the alert:**

1. Host Name & Username
2. Action Taken
3. Objective
4. Tactic & Technique
5. IOC: File Hash and Associated File name
6. Local IP: Local IP is the IP assigned to the host from the DHCP. This helps to identify if the host is a part of Maxis network.
7. IP/Remote IP: This is the IP with Which the host connects to the Falcon Cloud. This gives an idea of the network segment or the geolocation that the host is currently present in. If the IP is not a part of the subnet of Internet facing, or VPN IPs for Maxis then it must be connecting from outside Maxis Network.
8. Host Name & Username
9. Parent Process/ File triggering the alert
10. Child process involved, if any
11. Command Line/File Path: This gives the execution location of the file or process which caused the detection.
12. Disk Operations: Traverse Through the Disk Operations to identify the suspicious file which is not a part of any genuine process or application
13. Registry Operations

**Guidelines for Investigating any malware related alert:**

* If the source of the alert is a Maxis asset, identify the hostname associated and also the aim should to be find the exact location of the host, machine owner, machine OS and machine owner Dept. Utilize the Asset Inventories, Server Inventories and any other inventory with SOC to map an IP to its owner.
* For all external IP, URL /Domains involved in the alert the reputation for the IP/URL should be checked using the below reputation engines

1. <https://mxtoolbox.com/>
2. <https://www.virustotal.com/>
3. <https://www.talosintelligence.com/>
4. <https://who.is/>
5. <https://www.hybrid-analysis.com/>
6. <https://www.brightcloud.com/tools/url-ip-lookup.php>

* For any file or process detected in the alert, check the reputation of the hashes using Virus Total.
* In case of presence of a file or executable on the host use the Category section described below to classify the files to a particular category and take appropriate action.
* For CrowdStrike alerts Check the process Tree to identity the actual services or processes triggering the activity.
* For any suspicious file, for which the actual information about the actions on execution as well as the reason for triggering the alert is not sure, the SOC Analyst needs to execute the file in Open Source Sandbox (<https://app.any.run/>) . Closely monitor the URL connections and DNS requests when the file is running to understand better the behaviour of the executable. This helps to further categorize the alert and file based on its behaviour.

**Observation and Data Collation Table:**

|  |  |  |
| --- | --- | --- |
| Field | Value | Observation/ Comments |
| Alert Source | Eg., CS, Azure Sentinel, Microsoft Defender |  |
| Source IP(Target IP/Victim IP) |  | For CS alerts, Local IP is the Source IP |
| Source Hostname |  | If information about hostname is not available in the alert, try to look for the hostname from the asset inventories. |
| Source Username |  |  |
| Source Domain |  |  |
| Source OS | Win-7, Win 10, RHEL, etc. |  |
| Destination IP( Attacker IP) | This is the IP of the Attacker that initiated the malware connection and delivered the payload to host | If Destination IP is External (Internet IP) check the Web reputation using below reputation engines and give a brief analysis from the reputation filtering (first priority for all reputation search is VT).   * + 1. <https://mxtoolbox.com/>     2. <https://www.virustotal.com/>     3. <https://www.talosintelligence.com/>     4. <https://who.is/>     5. <https://www.hybrid-analysis.com/>     6. <https://www.brightcloud.com/tools/url-ip-lookup.php> |
| Destination(Attacker) Hostname |  | Fill this information only when available from the alert logs |
| Destination(Attacker) Username |  | Fill this information only when available from the alert logs |
| Destination(Attacker) Domain |  | Fill this information only when available from the alert logs |
| Destination OS |  | Fill this information only when available from the alert logs |
| Action Taken | Allowed/Blocked/ Quarantined/Successfully Executed |  |
| Objective |  | Fill for CS Alerts |
| Tactic & Technique |  | Fill for CS Alerts |
| File Name |  |  |
| File Path |  |  |
| File Type |  |  |
| File Hash- Reputation | File hash & Reputation(Clean/Unknown/Malicious) | Check File hash reputation on <https://www.virustotal.com/> |
| Parent Process |  | For CS look for ‘Parent Process’ and Not ‘Process’ for exact process triggering the alert. |
| Process Hash-Reputation |  | Fill this information if available |
| Command Line | Paste the Command Line code executed. Don’t paste if the code is in encoded format. | For CS and FE HX alerts |
| Disk Operations |  | **For CS Alerts.** Traverse Through the Disk Operations to identify the suspicious file which is not a part of any genuine process or application. |
| Registry Operations |  | **For CS Alerts.** Traverse Through the Disk Operations to identify the suspicious file which is not a part of any genuine process or application. |
| External IP/URL involved call back in the malicious code/file/process | Callback URL/IP Reputation  Callback URL/IP Status(Allowed/Blocked) | Give Reputation of any callback URL/IP obtained from the alert or investigation. Also the status of callback whether allowed or blocked should be mentioned. |

# **Response & Remediation**

Any incident/alert that involves presence of executable/suspicious files/process with unknown extensions on host should be handled based on the structure defined below. Security alerts reported by CrowdStrike, FireEye HX, Qradar Offenses can fall under this category of incident. Below are the important pointers to be taken note of, and to be considered while investigating any such incident that involves presence of an executable/suspicious file or process on a host.

1. **Identify the victim machine, or the host where the file or threat actor is detected. Classify the host based on the below categories:**
   * 1. Vantage Asset/ Vendor Asset (whether listed in Asset Inventory, or not)
     2. Desktop/ Laptop/ Server (using Inventories for WINTEL/UNIX/SECURITY devices/Asset list classify the asset)
     3. Connecting to Vanatge Network or not (Check the Local IP and the remote IP of the host to identify whether it is connected to Vantage locally or remotely)
        1. *Note: For all alerts where the asset involved is found to be not connected to Vantage infrastructure based on IP/ Hostname and Asset inventory details, mark those alerts as false positive and close with appropriate reason of “Non Vantage Asset and Asset not in Vantage Network”.*
2. **Once the host/ Victim is identified, the next step is to identify to gather all relevant details regarding the activity which include, but is not limited to:**
   * 1. Filename
     2. File Type
     3. File Hash
     4. FileHash Repuation on VT
     5. Status of Execution- Process or file allowed/blocked/deleted/quarantined or cleaned
     6. Hostname and Username associated with the execution.
     7. Processes which are causing execution of the files/executables
3. **In order to exactly identify whether the file involved in a particular alert is a PUP, a genuine file required for business, a third party application, or a determined malware payload, the below examples in Category wise table structure should help to identify the file type. Mentioned alongside each Category is the standard Questionnaire to User to the user as well as the standard action steps that are expected for the file defined under each category.**

| CATEGOGY | APPLICATION (examples) | Category Description | Action Steps/Questionnaire to User |
| --- | --- | --- | --- |
| **CAT-0 (Known****Malware/Riskware/Adware)** | vc\_runtime.dll resource.dat  Goopupdate.dll | Known Malware: malicious files or applications which have been identified and detected by reputation engines or previous knowledge from incidents have confirmed them to be Malware or riskware for Vantage environment. | For any file or Application which was detected by any of the Security tools and is a known Malware (based on reputation of detections on VT and other reputation engines), the following steps need to be taken for investigation:   * Identify whether malware or file in question was blocked from execution or successfully executed. * Identify number of machines on which the file or application was detected. Perform investigation to identify the source of the malware and also identify the IOC’s to avoid future reoccurrence.   **Case1: The file execution is blocked or the malware traffic was unsuccessful.**   * Attempt deletion of files using CS * If deletion using CS failed in cases of Host offline or due to other authorization challenges, direct the users to uninstall the application or delete the file from Host as well as delete all items from Recycle Bin. * Send user steps to delete Temp files from host * If the Alert is triggered by any unwanted browser plugins, send instructions to remove the extensions. * Run Remote AV Scan using SEP. In case the scan is not initiated and is pending for long, send mail to user to start SEP Scan from machine (For any scanning done by user, ask for screenshots of scanning) * Close the Ticket as **True Positive**   **Actions steps for End user:**  Send an email to the user with the below action steps to be performed:   * Delete the file detected and also Empty the Recycle bin**. <This is to be asked only when we are unable to delete the file remotely>** * Please clear temp files under your account **<Process document attached to do the same>** * Remove unnecessary extensions from your browsers. * Perform full AV scan on the host and share the result with us. **<This is to be asked only when we are unable to do the scan remotely>** * Kindly refrain from accessing websites or using applications which are not required for your Job requirement at Maxis. * Install CrowdStrike sensors on the machine:   **Case2: The file execution is successful or the traffic to malicious domain is not blocked.**   * Analyze the threat associated and impact with respect to the malware and define the Incident Severity accordingly. * For all such incidents where successful connections to malware domains or successful execution of payload on host/server is observed, the first objective should be to contain the threat. If the SOC analyst is unable to delete the files using CS, the system should be contained using CS/FE/IAM support (ID disable). For suspicious traffic allowed, the traffic should be blocked on proxy as well as Firewall before proceeding this further investigation, to ensure that the threat is contained. * If required the host must be contained, on case by case basis if deletion of the files and blocking of traffic still does not guarantee that the malicious traffic if stopped. This happens usually in case of some hidden malware codes that might be calling functions in stealth mode. In such cases contain the host after taking approval from SIS Team. * All other investigation and cleanup is to follow-through using standard methods adopted as in Case 1, after the machine has been contained. * Close the Ticket as **True Positive**   **When to request reimaging?**  If reimaging the machine is required in cases where the exact threat cannot be found on the host or if there are multiple folders infected by the attack, then liaise with EUC/EUS/VDI teams and create a ticket to get the machine reimaged.  If the exact files were identified and deletion of the same resolves the issue, then send mail to user to follow the below steps.  **Actions steps for End user:**  Send an email to the user with the below action steps to be performed:   * Delete the file detected and also Empty the Recycle bin**. <This is to be asked only when we are unable to delete the file remotely>** * Please clear temp files under your account **<Process document attached to do the same>** * Remove unnecessary extensions from your browsers. * Perform full AV scan on the host and share the result with us. **<This is to be asked only when we are unable to do the scan remotely>** * Kindly refrain from accessing websites or using applications which are not required for your Job requirement at Maxis. * Install CrowdStrike sensors on the machine:   **For any Incident where a file/application has been determined as a malicious actor after our investigation, the following steps need to be performed to identify the exact IOC’s involved and to prevent against re-occurrence:**   1. Identify the file source and file behavior. Use a Sandbox on isolated machine to execute the file or application that is detected.      1. Check for the presence of the same file or behavior in Vantage environment using Azure Sentinel/CS/MS Defender. 2. If the IOC’s have been identified, check on proxy for all users whose machines tried communicating to the IPs and URLs discovered in the IOCs. For all such hosts/users with positive detection, a separate investigation has to be done to understand how the other users/hosts have been affected from the malware. 3. For all machines that are tagged to a particular malware incident, we need to ensure that all have CS and a full AV scan on all is to be done as a best practice.   **Future avoidance:**   * The IOC hashes discovered from any such malware incident need to be updated into CS Prevention hashes. * The IP’s and URL’s need to be blocked in Proxy under Blocked Domains, any email domain or IP needs to be blocked under bad senders in o365 email and to be blocked on Firewall by the network team.   ***\*Any machine (HOST or SERVER) that is contained, should be approved by Joseph Brown/Nathan Boylan by email or over call.*** |
| **CAT-1 (Known PUP's)** | PUBG Torrent Youtube Downloader  IDM EXE | PUP : Not required in Maxis Corporate Environment | **Questionnaire to User:**  Please share the business justification for using the application/file in Vantage environment?    **Action Steps Once Identified and confirmed as PUP:**  **Actions steps for End user:**   * Delete the file detected and also Empty the Recycle bin**. <This is to be asked only when we are unable to delete the file remotely>** * Please clear temp files under your account **<Process document attached to do the same>** * Remove unnecessary extensions from your browsers. * Perform full AV scan on the host and share the result with us. **<This is to be asked only when we are unable to do the scan remotely>** * Kindly refrain from accessing websites or using applications which are not required for your Job requirement at Maxis. * Install CrowdStrike sensors on the machine:   This alert is to be closed as **True Positive.** |
|
|
|
|
|
|
| **CAT-2 (Unknown App/File)** | ConsoleApp4.exe md5check.exe  wavebrowser.exe | Either PUP/malware or Known Application | **Questionnaire to User:**  Please share the business justification for using the application/file in Vantage environment?    **Action Steps after User response:**  **Case 1: User Confirms that the application or file is genuine and required by Vantage**   * Do further analysis of the alert to identify the reason for the triggering of the alert. * If the alert triggered is only due to the execution pattern of the file or behavior based and not due to any malicious hash detection**, SOC should request approval from SIS team to whitelist the application from EDR tools so as to avoid future triggering of alert.** * **Upon obtaining approval**, whitelist the hash/file on CS or FE (whichever tool detected the activity in the first place)   Close the alert as **False Positive.**  **Case 2: User is unaware of the presence of file on host.**  **Actions steps for End user:**  Send an email to the user with the below action steps to be performed:   * Delete the file detected and also Empty the Recycle bin**. <This is to be asked only when we are unable to delete the file remotely>** * Please clear temp files under your account **<Process document attached to do the same>** * Remove unnecessary extensions from your browsers. * Perform full AV scan on the host and share the result with us. **<This is to be asked only when we are unable to do the scan remotely>** * Kindly refrain from accessing websites or using applications which are not required for your Job requirement at Maxis. * Install CrowdStrike and on the machine:   After successful removal/deletion of files, close the ticket as ticket as **True Positive**. |
|
|
|
|
|
|
| **CAT-3 (OS Files)** | Powershell.exe explorer.exe winword.exe iexplore.exe dllhost.exe | Process files which run apps in background | **Investigate further registry/files/DNS Connections to get the exact file or application causing suspicious activity.**  Note: Powershell, explorer, winword, iexplore, etc are OS related files/applications which are themselves genuine but often there are tasks performed using these applications which might be malicious. Whenever ant alert related to a high level windows or UNIX OS file is triggered, make sure to investigate further to find the file/code or process which is being run using that OS file.  After identifying the file/process/application that is the original source of the alert, it must be categorized into either CAT 1 or CAT 2 and handled as mentioned against those categories. |
|
|
|
|
|
| **CAT-4 (Freeware)** | FileZilla.exe WinSCP.exe | Known Freeware which is used in Vantage by either employees or vendors for their business requirements. However, they are not licensed by Vantage or vendors. | **Questionnaire to User:**  Please share the business justification for using the application/file in Vantage environment?  **Action Steps after User response:**  **Case 1: User Confirms that the application or file is required for Business Operations in Vantage.**   * Do further analysis of the alert to identify the reason for the triggering of the alert. * Send notification to user to uninstall the current copy of the application and install it from the trusted link shared by SOC.   Close the alert as **False Positive.**  **Case 2: User is unaware of the presence of file on host**  **Actions steps for End user:**  Send an email to the user with the below action steps to be performed:   * Delete the file detected and also Empty the Recycle bin**. <This is to be asked only when we are unable to delete the file remotely>** * Please clear temp files under your account **<Process document attached to do the same>** * Remove unnecessary extensions from your browsers. * Perform full AV scan on the host and share the result with us. **<This is to be asked only when we are unable to do the scan remotely>** * Kindly refrain from accessing websites or using applications which are not required for your Job requirement at Vantage. * Install CrowdStrike sensors on the machine:   After successful removal/deletion of files, close the ticket as ticket as **True Positive**. |
|
|
|
|
|
| **CAT -5 (Third Party/Vendor Licensed Application)** | Barracuda VPN McAfee Antivirus | Known Applications which is used are Vantage by vendors for their business requirements. However, they are licensed directly to vendors and not Vantage. | **Questionnaire to User:**  Please share the business justification for using the application/file in Vantage environment?  **Case 1: User Confirms that the application or file is required for Business Operations in Vantage**   * Do further analysis of the alert to identify the reason for the triggering of the alert. If it is only Behavior based and no Malicious hashes or other reported IOC’s present, then close the alert as **False Positive.**   **Case 2: User is unaware of the presence of file on host**  **Actions steps for End user:**  Send an email to the user with the below action steps to be performed:   * Delete the file detected and also Empty the Recycle bin**. <This is to be asked only when we are unable to delete the file remotely>** * Please clear temp files under your account **<Process document attached to do the same>** * Remove unnecessary extensions from your browsers. * Perform full AV scan on the host and share the result with us. **<This is to be asked only when we are unable to do the scan remotely>** * Kindly refrain from accessing websites or using applications which are not required for your Job requirement at Maxis. * Install CrowdStrike sensors on the machine using the below links:   After successful removal/deletion of files, close the ticket as ticket as **True Positive**. |
|
|
|
|
|

**Containment & Escalation for Level 1**

|  |  |
| --- | --- |
| **Scenario** | **Action to be Taken** |
| Single Workstation (laptop or Desktop) – any alert (High /Medium/Low) | Follow action steps for end user based on the Category of Malicious File |
| Single Server – Any type of Alert - Any Action | Alert Level 2 Immediately |
| Multiple Workstations (laptop or Desktop) | Alert Level 2 Immediately |
| Multiple Server – Any type of Alert - Any Action | Alert Level 2 Immediately |
| Ransomware like detections or behaviour | Contain and Alert Level 2 Immediately |

**Steps to creating a ticket in Service Now**

Step-by-step instructions for opening a ticket, who to route it to, what detail to include in the ticket, and the incident template.

Follow the snow link for incident creation:

<https://vantagerisk.service-now.com/vrsp?sysparm_stack=no>

1. Click on “Incident” and select “Create New.”
2. Enter your name in the “Caller” field. This will automatically populate the “Location” field.
3. Enter “Security Event” in the “Business Service” field.
4. Assign it to ServiceNow group “Vantage- CG- CS- Endpoint Security (EPS)” in the “Assignment Group” field.
5. Impact and urgency must be “Low”.
6. In the "Short Description" box, enter the details of Alert name, host, and user.
7. Provide detailed analysis in the work notes adding to below template
8. Follow up with Team till incident closure with valid notes.

If required, contact **IT ServiceDesk** for password change related queries and **DL IN Vantage-CG-Endpoint Security** DL IN Vantagefirewall ([vantage-cg-endpointsecurity.in@capgemini.com](mailto:vantage-cg-endpointsecurity.in@capgemini.com) ) for any other technical assistance.

**Note:** Create a service request to disable the user account if you found suspicious activity or user not responded after three strike-rule.

**Mind Mapping**

**Criteria for closure**

This may start out as an empty stub, but part of maturing the service will be defining criteria for closing a ticket.

**Criteria for escalation**

Under the following conditions, the analyst will contact **VANTAGE** Service Desk and request the incident be raised to P2 or P1 status:

**Below are the contact details**.

Email: helpdesk@vantagerisk.com

US Helpdesk: 844609 2204

Bermuda Helpdesk: 866 376 1362

India Helpdesk: + 91 2071279227

* (Insert any specific criteria relevant to this use case)  
  or
* As defined in Appendix 2: Security Incident Severity Determination of the document <http://myteams/sites/InfoSec/Policy/Procedures/InfoSec-Proc-GBL714-Incident%20Handling.docx>

Under the following conditions, the analyst will immediately notify Information Security at, and contact the Security Operations Manager by phone:

**Reference contact table below**.

|  |  |  |  |
| --- | --- | --- | --- |
| **Title** | **Name** | **Contact** | **Email** |
| Security Operations Lead | Keval Patalamwala | +91 9701016330 | [patalamwala.keval@capgemini.com](mailto:patalamwala.keval@capgemini.com) |
| Security Operations Manager | Kiran Farde | +91 9766623476 | [kiran.farde@capgemini.com](mailto:kiran.farde@capgemini.com) |
| Capgemini Security Manager | Ganesh Patil | +91 9930777270 | [ganesh.a.patil@capgemini.com](mailto:ganesh.a.patil@capgemini.com) |
| Vantage AVP, Security & Operations | Joseph Brown | +1 (551) 233-8862 | [Joseph.Brown@VantageRisk.com](mailto:Joseph.Brown@VantageRisk.com) |
| Vantage VP, Security & Technical Architecture | Nathan Boylan |  | Nathan.Boylan@vantagerisk.com |

(Insert any specific criteria relevant to this use case)  
or

Any incident meeting the criteria for CRITICAL (P1) as defined in Appendix 2: Security Incident Severity Determination of the document <http://myteams/sites/InfoSec/Policy/Procedures/InfoSec-Proc-GBL714-Incident%20Handling.docx>

**Document Inquiries**

Contact VANTAGE Information Security if you have specific questions or suggestions about this and other Policies and Standards at:

* DL IN MSSP Sentinel GSOC, [msspsentinelgsoc@capgemini.com](mailto:msspsentinelgsoc@capgemini.com),
* DL IN Vantage-CG-SOC, [vantage-cg-soc.in@capgemini.com](mailto:vantage-cg-soc.in@capgemini.com),
* Keval Patalamwala, [patalamwala.keval@capgemini.com](mailto:patalamwala.keval@capgemini.com)
* Joe Brown, [Joseph.brown@vantagerisk.com](mailto:Joseph.brown@vantagerisk.com) **AVP, Security & Operations.**

# **END OF DOCUMENT**