CYBERSECURITY
Incident Response Plan

VERSION 1.4

Created for Anderson Group Services Limited
and in partnership with NewCMI Ltd

August
2021

Contents

Version History

Version Number	Version Date	Items Revised	Author
1.0	May 2021	Initial Creation	Michael O'Neill
1.1	May 2021	CMI Branding Added + Typos/Grammar	Michael O'Neill
1.2	May 2021	Error correction	Michael O'Neill
1.3	June 2021	Adding detail to samples scenarios	Michael O'Neill
1.4	August 2021	Completed with client specific information	Ian Bell

Introduction

This document serves as a central source of information to aid and assist a structured approach and response to a cybersecurity incident. Cyber incidents can cause panic and confusion and it is vital that a plan is made clear and updated with new guidance where necessary over time.

Items covered in this document will help address the common tasks and requirements needed to properly report, remediate and where possible provide evidence for further forensic follow up if possible. In addition, this document provides a guidance notes and templates that can be used to provide responses to internal and external stakeholders as well as to prepare critical evidence for regulatory bodies, insurance companies and law enforcement officials.

Basic principles of the NIST framework are followed specifically around the DETECT, RESPOND and RECOVER sections of the framework. Please see here for more information on the NIST framework

Definition: Security Operations Centre (SOC)

A security operations centre (SOC) is an information security team responsible for monitoring and analysing an organization's security status on an ongoing basis. Security operations centres monitor and analyse activity on networks, servers, endpoints and other cloud systems, looking for anomalous activity that could be indicative of a security incident or compromise. The SOC is responsible for ensuring that potential security incidents are correctly identified, analysed, defended, investigated, and reported.

Contact Information – Incident Response Team

Upon detection or report of a cyber incident the following contact information will be used throughout the incident to communicate information.

Organisation:	**Anderson Group Services Limited**
Date:	**08 July 2021**

NewCMI Technical Contacts

Role	Company	Name	Pri. Number	Sec. Number
Main NewCMI contact	NEWCMI LTD	Ryan McCracken	02890 735638	07803 045124
Secondary NewCMI contact	NEWCMI LTD	Michael O'Neill	02890 735623	07739 931995
Primary Cyber Expert	RocketCyber	To Be Assigned	[NUMBER]	To be Assigned
Secondary Cyber Expert	NEWCMI	To Be Assigned	02890 735600	To be Assigned
All email communications will go to and come from servicedesk@newcmi.com				

Client Contacts

Role	Title/Name	Name	Pri. Number	Sec. Number
Primary contact	IT Manager	Leigh Cummings	07989 476 371	
Secondary contact	ICT Technician	Gareth Bannister	07387 419 840	
DPO	Group Finance Director	Mark Aldridge	07896 270 245	
Insurance Reps	Director	Darren Carter	07967 381 994	
Regulator	Delivery Systems Manager	Richard Knight	07970 893 759	

Cyber Insurance Contact Details

Insurance provider/broker	Policy numbers	Contact information
N/A	N/A	N/A

Overview of Process

Again, following the basic principles of the NIST incident response lifecycle, below is a description of how typically NewCMI and its partners would deal with a cybersecurity incident.

1. Inform the Incident Response Team
2. Control the Event
3. Restore service or put in place workaround
4. Confirm affected systems are ready for normal operations
5. Root cause analysis and next steps

1. Prepare for the event

This document is the first step to prepare for a cybersecurity incident. The page above is step one which is to know who is part of the cyber security incident response team (CSIRT). All employees or agents must report any suspected or confirmed data breach or other cyber incident to their managers and the CMI servicedesk will clearly mark the ticket as a cyber Incident or data breach. If you have the NewCMI SOC service and they determine there has or an incident is in progress the CSIRT will inform the client contacts above.

2. Identification and assessment

In some cases, an event can be a false positive or miscommunication. At this stage it is vital to conduct an assessment to confirm the event or not. The assessment should determine the scope, impact and extent of the damage caused or in progress. Where possible every attempt should be made to preserve the digital evidence for potential forensic review by third parties or later legal requirements.

3. Control and contain the incident

This stage (more than other stages) requires an open channel with all the stakeholders as events could move very quickly. It is important that notes are made for reference in later stages but also to keep the client up to date. With the assessment above, steps need to be taken to minimise the incident spreading to other systems or resources. The client may also choose to update insurance or regulatory authorities with the information provided.

4. Removal of affected systems

The affected systems will most likely need to be removed or isolated for the rest of the network and all other symptoms noted, addressed and confirmed no longer affecting the rest of the service or systems. A focus on looking for secondary compromises that may have been installed will also be addressed.

5. System or service recovery

This stage requires various steps needed to bring the system or service back to a working and healthy state. This may be restoring from a previous backup (after confirming the backup works in isolation) or may require the client's disaster recovery process to be invoked. Once completed the incident should be declared as resolved and communicated as such.

6. Root cause analysis and lessons learnt

Usually post incident, CMI will detail our findings and if possible at this time declare what we believe the root cause analysis (RCA) of the incident was. In some instances a specialised third party will be required to review the evidence to help determine a root cause. The template in this document will be used to record an official record of the RCA. A cybersecurity incident can develop quickly and following the incident, we will review any lessons learned, and also provide guidance or identify areas of concern that the client should address going forward.

Incident Response – Client Checklist/Notes

Does your company how and where to report a cybersecurity incident?	☐
Communicate incident to your internal stakeholders	☐
Communicate responses to internal staff and remind users it's not for outside sharing	☐
Communicate incident to cyber insurance company if required	☐
Do you need to inform 3rd party's or clients about lack or degrade of service?	☐
Review plan to address media if applicable – consider your carefully worded statement	☐
Review insurance policy to cover cybersecurity threat	☐
Review plan to address ICO if PII data breach	☐
	☐
	☐

Incident Response – NewCMI Recorded Actions

All incidents must be logged in the NewCMI ticketing system regardless of whom has discovered or reported the issue.

Date of incident:	**[DATE]**	
Initial NewCMI engineer responding:	**[ENGINEER NAME]**	
Initial RocketCyber engineer responding:	**[ENGNEER NAME]**	
Client contact made aware of incident:	**[CLIENT NAME – CONTACT DETAILS]**	☐
NewCMI Ticket Reference:	**[TICKET REFERENCE]**	
Category of incident:	Choose an item.	
Functional Impact:	Choose an item.	
Informational Impact:	Choose an item.	

Actions taken (Detect, Respond, Recover)

Guidance notes, delete/add as appropriate (see additional notes in appendix 3)

1. *Where possible do not power off affected system, disconnect or isolate from network (backup systems)*
2. *How was this indent detected and what the timeframe?*
3. *Disable all accounts, reset all active sessions and passwords local and cloud*
4. *Create temp admin accounts for this incident*
5. *Disable access to affected or all systems*
6. *If restoring from backup seriously consider fresh builds*
7. *If possible, restore isolated and test as well as look for IOC's*
8. *Run non OS based scans to check for viruses/malware/APT's*
9. *How was the affected system restored online?*
10. *Confirm that patch levels on all devices are updated (including rebuilds)*
11. *Confirm that firewalls are enabled and advanced features are enabled – block unused ports*
12. *Enforce MFA at least on admin level accounts*
13. *Install SOC client to monitor systems for reinfection or secondary compromises*
14. *Confirmation of testing process on items above*

Root cause analysis and recommendations

Guidance notes, delete/add as appropriate

1. *Add description of issues, time lines and actions taken*
2. *What at this stage do we believe the root cause to be?*
3. *Exact timeline of events*
4. *How was this incident handled, what hindered the efforts?*
5. *Collect information from end users/witnesses of what they say/did*
6. *If applicable secure camera footage*
7. *Secure logs of various related systems (firewalls, end user devices, servers etc.)*
8. *Review email rules cloud logs etc.*
9. *Collate data captured during and post incident (screenshots, memory dumps, images etc.)*
10. *Update and review site documentation*
11. *Prepare report for ICO or other related bodies if required*
12. *Do we need to store this evidence for a long period of time?*
13. *What recommendations are we putting forward at this stage?*
    a. *Response times*
    b. *Documented procedure quality improvements*
    c. *Unexpected delays?*
    d. *What are NewCMI recommending be installed/added/updated?*
    e. *Other…*

Appendix 1 – Guidance and Containment Notes

Containment strategies

Containment requires critical decision-making related to the nature of the incident. Below are some common strategies to assist with the decision-making process. All attempts to contain the threat must consider the impact on the business operations and where possible should be made with the approval of the client.

All attempts to contain the threat must carefully consider preserving the evidence.

- **Stolen credentials – disable account credentials, reset all active connections, review user activity, reverse changes, increase alerting, harden from future attacks.**
- **Ransomware – isolate the impacted system, validate the ransomware claim, contact insurance carrier, identify whether additional systems have been impacted and isolate as needed. Block access to command and control servers. Check ownership of encrypted files to determine the potential patient zero.**
- **DOS/DDOS - control WAN/ISP. Block IPs, domains and sinkhole domains if required.**
- **Virus outbreak – contain LAN/system. Boot into antivirus/antimalware offline disk for deep cleans. Submit sample files to third party AV vendors for further analysis and information.**
- **Data loss – review user activity, implement data breach response procedures**
- **Website defacement – repair site, harden from future attacks.**
- **Compromised API – review changes made, repair API, harden from future attacks.**

Notification Requirements

Requirement	Notification timing	Notes
PCI DSS	**Immediately, no later than 24 hours**	
GDPR	**72 hours after becoming aware of a breach**	

Responses to media inquiries

Whether it be local media or other enquiring third parties, getting the facts is a priority. The client should not be pressured into confirming or releasing information before you have confirmation of the facts.

The following responses should give you the necessary time to collect and report the facts.

If on the phone to the media:

- **"We've just learned about the [situation, incident, event] and are trying to get more complete information now. How can I reach you when I have more information?"**
- **"All our efforts are directed at [bringing the situation under control]. I'm not going to speculate about [the situation]. How can I reach you when I have more information?"**
- **"I'm not the authority on this subject. Let me have [name] call you right back."**
- **"We're preparing a statement now. Can I get back to you in about [number of minutes or hours]?"**
- **"You may check our website for background information, and I will fax/e-mail you with the time of our next update."**

If in person at the incident site or in front of a press meeting:

- **This is an evolving [situation, incident, event], and I know you want as much information as possible right now. While we work to get your questions answered, I want to tell you what we can confirm right now:**
- **At approximately [time], a [brief description of what happened].**
- **At this point, we do not know [how long the advisory will last, how many customers are affected, etc.].**
- **We have a [system, plan, procedure, operation] in place. We are being assisted by [local officials, experts, our legal team] as part of that plan.**
- **The situation is [under, not yet under] control. We are working with [local, national, international] authorities to [correct this situation, determine how this happened].**
- **We will continue to gather information and release it to you as soon as possible. I will be back to you within [amount of time in minutes or hours] to give you an update. As soon as we have confirmed information, it will be provided.**
- **We ask for your patience as we respond to this [situation, incident, event]**

Statements Should Avoid

- **Confrontation - the objective of media statements in a crisis is to diffuse the situation – not make it worse. Avoid blaming/buck-passing because it will simply result in a media-based argument between opposing parties – remember journalists love confrontational stories. e.g. 'They were wrong', 'it is not our fault'…**
- **Ambiguity - weak, ambiguous statements have no place in handling negative media situations and can leave room for the journalist to re-interpret your response. Be robust and clear at all times. Use strong positive words e.g. 'we are committed to X and will not tolerate Y'. Make sure your statement is completely unambiguous.**
- **Personal pronouns - try and avoid referring to your organization by name in your media statement as doing this could reinforce the link between your organization and the negative issue concerned. You may simply use the first-person plural ('we'/'us'). This also has the advantage of adding a slightly personal and less bureaucratic feel to the statement.**

Appendix 2 – Response Level Classification

Response Level Classification		Informational Impact			
		None	Limited	Moderate	Critical
Functional Impact	None	N/A	Sev. 3	Sev. 2	Sev. 1
	Limited	Sev. 3	Sev. 3	Sev. 2	Sev. 1
	Moderate	Sev. 2	Sev. 2	Sev. 2	Sev. 1
	Critical	Sev. 1	Sev. 1	Sev. 1	Sev. 1

Severity Level	SLA
Sev. 3	Within three days
Sev. 2	Within 24 hours
Sev. 1	Within 2 hours

Informational Impact	Definition	CSIRT Response
None	No information was accessed, exfiltrated, changed, deleted or otherwise compromised.	No action needed at this time
Limited	Public or non-sensitive data was accessed, exfiltrated, changed, deleted or otherwise compromised	Notify data owners to help determine appropriate next steps
Moderate	Internal information was accessed, exfiltrated, changed, deleted or otherwise compromised	Notify the CIO or DPO. NewCMI will work with DPO to determine the best course of action.
Critical	Protected data was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the MD/CEO CIO or DPO. NewCMI will work with DPO to determine the best course of action.

Functional Impact	Definition	CSIRT Response
None	No effect with client being able to provide services to users	Create ticket and await follow-up work if any.
Limited	Minimal effect: client can continue to work but has lost some efficiency or productivity	Create ticket and assign for remediation. Notify critical contacts.
Moderate	The client has lost the ability to provide service to a subset of users	Create a ticket and assign for remediation. Notify all contacts
Critical	The client has lost the ability to provide a service to all users.	Create ticket and remediate. Notify all contacts and make decision on any available Disaster Recovery plans.

Appendix 3 – Typical Scenarios and Responses

The purpose of any incident response plan is to minimise the damage caused by a cyber incident or attack. The summarised guidance below whilst not exhaustive and will need updated as time goes by will help you recover in the shortest time possible whilst attempting to minimise the amount of money spent and reputational damage to your organisation.

This document assumes an incident has happened or will happen, this guidance is to help manage and coordinate the tasks, communications and future preventative measures suggested after an event.

Computer/Server malware infection

In this scenario malware has been detected and CMI are dealing with the infection to close it down but also ascertain if it's spreading elsewhere on the clients network. Malware is malicious software designed to damage or destroy computers systems, you may also know malware as viruses, worms, trojans, ransomware, adware or bitcoin miner virus.

Malware if initialised commonly installs other types of malware to gain a greater foothold or persistence on systems, so its extremely important machines are scanned with multiple scanning tools and access to systems carefully monitored and examined going forward.

- **Create incident in ticketing system if not created already**
- **Acknowledge the report if not detected by automated systems**
- **Disconnect all outside access to network and or device using SOC tool if available**
- **Immediately inform the CSIRT and DPO if applicable, potentially consider reporting to law enforcement (101)**
- **Reset all passwords including admin level passwords and confirm MFA/2FA status**
- **Determine and query recent new account creations on machines and network**
- **Get a message to all staff to be extra vigilant at this time and report anything unusual**
- **Confirm if isolated device or threat of malware spreading to other parts of the network**
- **The threat maybe active and key to track down as soon as possible – check newly created files ownership**
- **How did this malware get installed, phishing link, website or other (blacklist/block where appropriate)**
- **Preserve running memory via SOC tool, export computer logs and save malware files if possible**
- **If possible image backup the affected device and don't reboot systems just yet**
- **Review backup status of this data and inform CSIRT on next steps**
- **Restore data and or invoke DR/BC plan if appropriate, check restores in isolation**
- **In most cases rebuild affected machines(s) and confirm fully patched**
- **If possible submit sample files to Virus Total for analysis and further intelligence**
- **Work with RC to understand if there are other remediation options and Kill Chain**
- **If source known or discovered work with SOC to remove email or files from clients devices**
- **Initiate malware and AV/Malware scans on all devices including offline scans**
- **Continue to monitor for re-infection or other activity via backdoors or secondary compromises**
- **Write up future recommendations and discuss next actions with client**
- **Review the data breach response plan, what didn't work well and inform NewCMI CSIRT**

Computer/Server ransomware infection

In this scenario a computer or server has been infected with a type of malware generally referred to as ransomware, data has been encrypted with no means of decrypting the data, in addition a third party is trying to extort money or bitcoin from the organisation in order to restore access to the data.

NewCMI do not recommend paying the third party's any money as this is no guarantee to get data back and may become an illegal action in the future.

Modern ransomware practices may also threaten to release data into the public domain if the fee is not paid. It is also assumed that data is encrypted already so no way to stop the encryption if preventative measures have already failed.

- **Create incident in ticketing system if not created already**
- **Acknowledge the report if not detected by automated systems**
- **Disconnect all outside access to network and or device using SOC tool if available**
- **Immediately inform the CSIRT and DPO if applicable, potentially consider reporting to law enforcement (101)**
- **Reset all passwords including admin level passwords and confirm MFA/2FA status**
- **Get a message to all staff to be extra vigilant at this time and report anything unusual**
- **Confirm if isolated device or threat of malware spreading to other parts of the network**
- **The threat maybe active and key to track down as soon as possible – check encrypted files ownership**
- **Ascertain if this data is of a PII nature and has been exfiltrated, if so the ICO may need to be informed**
- **Client may also need to inform other third party's or data leakage or service disruptions**
- **How did this malware get installed, phishing link, website or other (blacklist/block where appropriate)**
- **Preserve running memory via SOC tool, export computer logs and save malware files if possible**
- **If possible image backup the affected device and don't reboot systems just yet**
- **Review backup status of this data and inform CSIRT on next steps**
- **Restore data and or invoke DR/BC plan if appropriate, check restores in isolation**
- **In most cases rebuild affected machines(s) and confirm fully patched**
- **Which group of hackers has encrypted the machine as decryption key may be available**
- **If possible submit sample files to Virus Total for analysis and further intelligence**
- **Work with RC to understand if there are other remediation options and Kill Chain**
- **If source known or discovered work with SOC to remove email or files from clients devices**
- **Initiate malware and AV scans on all devices including offline scans**
- **Continue to monitor for re-encryption or other activity via backdoors or secondary compromises**
- **Write up future recommendations and discuss next actions with client**
- **Review the data breach response plan, what didn't work well and inform NewCMI CSIRT**

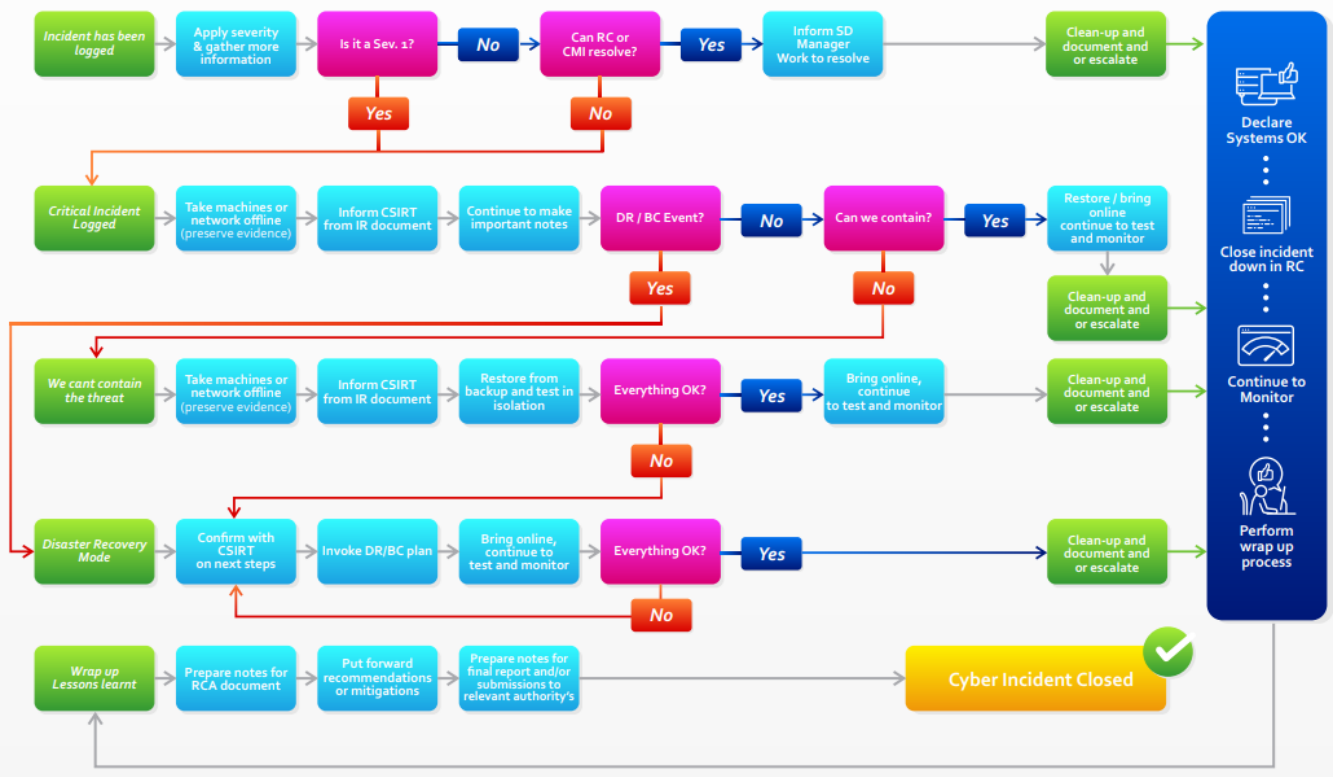
It is most important that the affected device is not turned off or rebooted. On occasion the encryption keys can be saved in running memory and could be vital for file recovery when forensically examined.

Sensitive data leakage or security breach

In this scenario it is considered PII data has been taken or removed from authorised systems and is being used without the proper authorisation or consent given by the data owners.

- **Create incident in ticketing system**
- **Acknowledge the report to whomever submitted the information and advise we will investigate**
- **Inform the CSIRT and especially the clients DPO if one exists to the facts of the incident and next steps**
- **Investigate and document the incident, keep CSIRT up to date on all next steps**
- **Try to confirm if a data breach or leakage has in fact occurred**
- **Where applicable take backups of logs or reports**
- **Advise client on procedure and timeframes to report to the ICO**
- **Try to confirm or estimate the type and amount of data that has been misused**
- **Stop or close the gap that contributed to the data breach, run multiple malware/AV scans**
- **If applicable restore any missing data from backups, confirm no compromises in backups**
- **Prepare statement to relevant stakeholders**
- **If data was PII related help to prepare a response to the ICO – see here and here for submission steps**
- **The client should decide to alert the data owners, facilitate the required information**
- **Write up future recommendations and discuss next actions with client**
- **Review the data breach response plan, what didn't work well and inform NewCMI CSIRT**

Appendix 4 – Incident Response Flow Diagram



What our SOC service monitors

Below is a list of ever evolving services that our SOC agent and SOC team are constantly monitoring and responding to. Should a serious threat be found, our agent has the ability to isolate the device from the rest of the network but not NewCMI engineers. This allows further investigations without exposing threats to the rest of your systems.

Our SOC has multiple cyber intelligence feeds that help inform many of the services below and many new emerging threats that are generated every single day. We also scan hosts with our agents for other software or setup vulnerabilities and present these in reports that can be actioned.

ADVANCED BREACH DETECTION

Our SOC agent identifies computers that are compromised where security defences have been circumvented. Malicious activity reported by our SOC agent requires immediate investigation.

CRYPTO MINING DETECTION

Our SOC agent detects crypto mining activity form browser based crypto miners as well as common crypto mining client software.

CYBER TERRORIST NETWORK CONNECTIONS

Our SOC agent detects network connections to various nation states that have been known to engage in cyberterrorist activities.

DNS FILTER MONITOR

Our SOC agent collects information from DNS filtering services

ENDPOINT EVENT LOG MONITOR

Our SOC agent monitors the Microsoft Windows or macOS Event Log for suspicious events. Detected events are security related activities such as failed logins, clearing security logs, unauthorized activity, etc.

FIREWALL LOG ANALYSER

Our SOC agent acts as a syslog server collecting log messages from edge devices on your network. Messages are parsed and analysed for potential threat indicators. When a potential threat or security related event is detected, our SOC agent will report the message to the Cloud Console.

MALICIOUS FILE DETECTION

Our SOC agent monitors and detects suspicious and malicious files that are written to disk or executed.

MICROSOFT EXCHANGE HAFNIUM EXPLOIT DETECTION

Our SOC agent will look for specific Indicators of compromise (IOCs) related to exploitation of Microsoft Exchange 2010, 2013, 2016 and 2019 via CVE CVE-2021-26855 , CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. It will also report the patch status for mitigations against these vulnerabilities.

OFFICE 365 SECURE SCORE

Overall description of cloud security posture with itemized remediation plans across all Office365 tenants

OFFICE 365 LOG MONITOR

Multi-tenant event log monitor for aggregated data representing all accounts linked to Microsoft365

OFFICE 365 RISK DETECTION

We focus on the riskiest accounts, users, and behaviours. Determined risk through a combination of industry heuristics and machine learning.

PASSLY MONITOR

Our SOC agent will monitor the logon data from Passly.

SUSPICIOUS NETWORK SERVICES

Our SOC agent detects suspicious network services running on an endpoint. While there are 65,535 available network services for legitimate use, suspicious detections are defined as well-known ports and services that are leveraged for malicious intent.

SUSPICIOUS TOOLS

Our SOC agent detects programs that can negatively impact the security of the system and business network. Detected suspicious tools should be investigated and are categorized as hacking utilities, password crackers, or other tools used by attackers for malicious purposes.

SYSTEM PROCESS VERIFIER

Our SOC agent detects and analyses system processes for known suspicious or malicious behaviours based on various factors including disk image location, timestamp fingerprinting and Levenshtein distance calculations.

WEBROOT MONITOR

Our SOC agent reports on detections from Webroot

ACTIVE DIRECTORY MONITOR AND SYNC

Our SOC agent will monitor for changes to user accounts in Active Directory and synchronize changes to the Breach Secure Now Cloud. Optionally reporting changes to the Console.