Snare and the Mitre ATT&CK Knowledge Base

Part 1 of a series of white papers and blogs that illustrate how Snare helps you identify and resolve issues highlighted in the Mitre ATT&CK knowledge base

Snare and the Mitre ATT&CK knowledge base

Part 1 of a series of white papers and blogs that illustrate how Snare helps you identify and resolve issues highlighted in the Mitre ATT&CK knowledge base.

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cyber security product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world - by bringing communities together to develop more effective cyber security strategies and solutions. ATT&CK is open and available to any person or organization for use at no charge, and is available from https://attack.mitre.org/.

ATT&CK shares adversarial behaviours across the attack life cycle and provides a common taxonomy for threat analysis and research.

The ATT&CK framework can help cyber security teams assess the effectiveness of the processes and defensive measures deployed in security operations centre (SOC), to identify areas for improvement.

With this knowledge base, teams take on an adversary's perspective to better understand motivation and third party relationships and facilitate a more holistic approach to threat detection and response. This provides context to the individual parts of an attack to help teams predict the behaviour of an attacker, and quickly and effectively respond to an attack.

Improve Your Security Operations to ATT&CK with Snare

Detecting adversaries requires pervasive visibility across your security data and a proactive approach to efficiently identify suspicious behaviour. Teams can use Snare Central for high fidelity visibility into the tactics, techniques, and procedures of the most skilled adversary for accurate threat detection.

Security programs must continue to update methodologies, as fast as adversaries iterate, to detect new threats and prevent damaging breaches. Teams can use Snare Central as a diagnostic tool to assess their security program coverage and gaps, in order to prepare for future threats that leverage similar exploits.

Use MITRE ATT&CK's threat model with the Snare software suite for user analytics, compliance reporting, and threat feeds to generate higher-value alarms that more accurately detect adversaries and their activities.

Snare Central and Analytics for MITRE ATT&CK

Snare Central and agents are two pre-built solutions that can collect and process a wide variety of sources.

Snare Central is a server-side data processing pipeline that can ingest log information from a multitude of sources including Snare Agents, and any syslog source simultaneously.

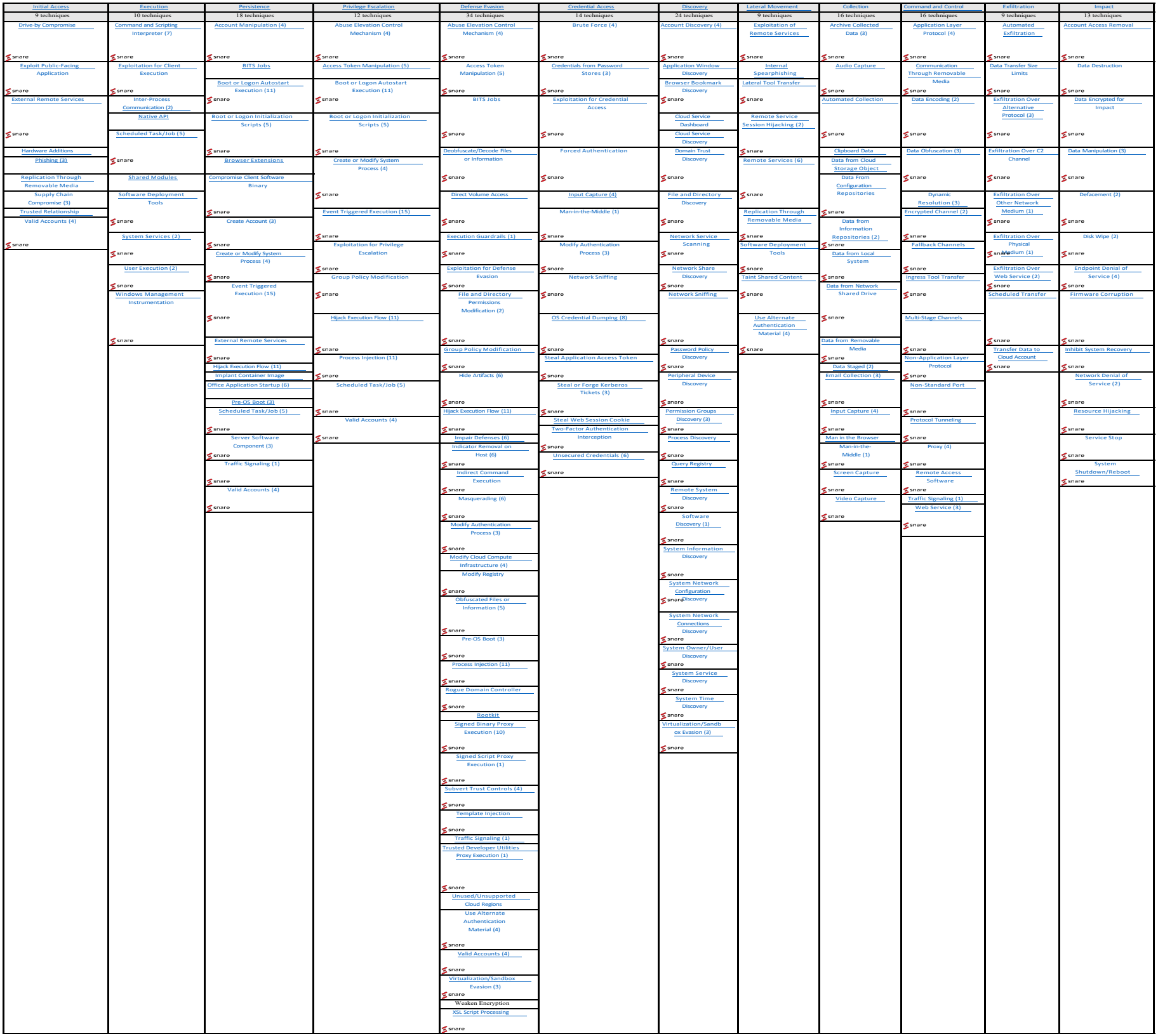
Snare Agents are a collection of lightweight, single-purpose agent based log collection and data shippers that can send data from thousands of machines and systems.

Snare Central collects, collates, normalizes, and forensically stores eventlog data, and includes powerful search functionality to support threat hunting and SIEM needs. With Snare, a security team can achieve extensive security visibility across organizational assets, and has the opportunity to perform comprehensive historical forensic analysis with a cost-competitive package that does not financially penalize you for collecting bulk audit data to support deep analysis. Snare Central is well-known in the security community for its speed, scalability, and cross application collection capabilities (security and otherwise). Snare Central uses open data structures which allow your specialists to export data to preferred toolsets or share content with third parties such as law enforcement, but also includes powerful interactive analysis tools (e.g., search, drill-down and pivoting, visualization) and automated analysis capabilities (e.g., alerting, anomaly detection) on-server. To streamline and strengthen the practitioner experience, Snare Central can process data in a normalized way to provide an interactive workspace for event triage and forensic investigations. Good coverage comes from unified data analysis, simplified analyst workflows, and ready communication and collaboration between different members of the security team.

The Snare Central Event Query Language (SnareQL) is a specialist time-series focused query tool built in-house by the Snare team to hunt down relationships between security-relevant events. SnareQL provides a subset and superset of SQL; mapping database-like query behaviour over the top of specialist security eventlog content stored in an open data structure format. Snare and SnareQL facilitates threat hunting through data stack pipes built into the language. Snare powers the ATT&CK-oriented search and detection experience using the power of the Snare Agents and Snare Centrals general syslog collection and reporting capabilities.

The table below highlights the Mitre Att&ck areas of coverage and also links to the respective techniques that are often used. Each area details some specific techniques used by adversaries to:

- gain access
- perform execution of commands
- provide persistence to the systems
- perform privilege escalation to access more data or systems implement defense and evasion so its hard to find them obtain credential access to gain access to more data or systems
- Discover other systems and accounts to gain more access Perform lateral movement around the network
- Collect sensitive information
- Implement backdoor command and control
- Perform Ex-filtration of data
- Perform some impact to the target system


Initial Access
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (3)
Replication Through Removable Media
Supply Chain Compromise (3)
Trusted Relationship
Valid Accounts (4)
Execution
10 techniques
Command and Scripting Interpreter (7)
Exploitation for Client Execution
Inter-Process Communication (2)
Native API
Scheduled Task/Job (5)
Shared Modules
Software Deployment Tools
System Services (2)
User Execution (2)
Windows Management Instrumentation
Persistence
18 techniques
Account Manipulation (4)
BITS Jobs
Boot or Logon Autostart Execution (11)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Client Software Binary
Create Account (3)
Create or Modify System Process (4)
Event Triggered Execution (15)
External Remote Services
Hijack Execution Flow (11)
Implant Container Image
Office Application Startup (6)
Pre-OS Boot (3)
Scheduled Task/Job (5)
Server Software Component (3)
Traffic Signaling (1)
Valid Accounts (4)
Privilege Escalation
12 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
Boot or Logon Autostart Execution (11)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (4)
Event Triggered Execution (15)
Exploitation for Privilege Escalation
Group Policy Modification
Hijack Execution Flow (11)
Process Injection (11)
Scheduled Task/Job (5)
Valid Accounts (4)
Defense Evasion
34 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
BITS Jobs
Deobfuscate/Decode Files or Information
Direct Volume Access
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Group Policy Modification
Hide Artifacts (6)
Hijack Execution Flow (11)
Impair Defenses (6)
Indicator Removal on Host (6)
Indirect Command Execution
Masquerading (6)
Modify Authentication Process (3)
Modify Cloud Compute Infrastructure (4)
Modify Registry
Obfuscated Files or Information (5)
Pre-OS Boot (3)
Process Injection (11)
Rogue Domain Controller
Rootkit
Signed Binary Proxy Execution (10)
Signed Script Proxy Execution (1)
Subvert Trust Controls (4)
Template Injection
Traffic Signaling (1)
Trusted Developer Utilities Proxy Execution (1)
Unused/Unsupported Cloud Regions
Use Alternate Authentication Material (4)
Valid Accounts (4)
Virtualization/Sandbox Evasion (3)
Weaken Encryption
XSL Script Processing
Credential Access
14 techniques
Brute Force (4)
Credentials from Password Stores (3)
Exploitation for Credential Access
Forced Authentication
Input Capture (4)
Man-in-the-Middle (1)
Modify Authentication Process (3)
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Kerberos Tickets (3)
Steal Web Session Cookie
Two-Factor Authentication Interception
Unsecured Credentials (6)
Discovery
24 techniques
Account Discovery (4)
Application Window Discovery
Browser Bookmark Discovery
Cloud Service Dashboard
Cloud Service Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (1)
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion (3)
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (4)
Collection
16 techniques
Archive Collected Data (3)
Audio Capture
Automated Collection
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repositories
Data from Information Repositories (2)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (2)
Email Collection (3)
Input Capture (4)
Man in the Browser
Man-in-the-Middle (1)
Screen Capture
Video Capture
Command and Control
16 techniques
Application Layer Protocol (4)
Communication Through Removable Media
Data Encoding (2)
Data Obfuscation (3)
Dynamic Resolution (3)
Encrypted Channel (2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (4)
Remote Access Software
Traffic Signaling (1)
Web Service (3)
Exfiltration
9 techniques
Automated Exfiltration
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (1)
Exfiltration Over Physical Medium (1)
Exfiltration Over Web Service (2)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
13 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (3)
Defacement (2)
Disk Wipe (2)
Endpoint Denial of Service (4)
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (2)
Resource Hijacking
Service Stop
System Shutdown/Reboot
snare

Initial Access

- Drive by Compromise
    - Snare agents running on end points can help collect the logs of the system and the commands executed on the system as part of a drive-by compromise. If a user were to click on a bad website and the normal malware protection did not prevent bad actions then the Snare Agents can collect the relevant commands and payload of the activity as the system is compromised. Web logs from proxy servers can also be collected using the Snare agents to help track and monitor the user activity.
    - As part of standard incident reporting processes, Snare Central can be used to report on suspicious commands and system modifications including registry changes, started tasks modifications, user and group changes etc. Web logs can be collected and analysed using the standard reporting options. If the adversary was to pivot from the drive-by system to other systems, snare agents deployed throughout the network will provide a trail of evidence allowing the security team to track the path of the attacker through the organisational infrastructure.
- Exploit Public facing Application
    - Snare agents including database activity monitoring running on server systems can collect the web server logs, application logs, database activity from the system to analyse application activity and highlight potential threats such as SQL injection, XSS and command injection attacks.
    - Snare Central can be used to report on the end system activity using the out-of-the box reporting or using the search features for adhoc threat hunting.
- External remote services
    - Snare Central can be used to collect logs from external systems like VPNs and Citrix servers. By using Snare agents on systems, forensic logs can be collected from external facing servers. Many out-of-the-box reports can be used to highlight suspicious activity. Customized reports can be created, or the advanced search option can be used to search for particular threats.
- Valid Accounts
    - Snare agents can collect logs from systems to track existing default accounts, domain accounts, local accounts and cloud accounts. If accounts are used for malicious activity, then Snare Agents can collect these logs for forensic analysis.
    - Snare Central has many default reports to analyse administrative and regular user activity, which will allow the security team to monitor the usage. Real time alerts and threshold reporting can also be used to provide alerts via email or SNMP traps for trigger points; ie 6 invalid login failures for administrative users or groups, actual logins for specific accounts and out of hours logins.

Execution

- Command and Scripting Interpreters
  - Snare Agents can capture logs using the out-of-the-box audit policies for PowerShell, AppleScript, Windows Command Shell, Unix Shell, Visual Basic, Python, and JavaScript running on systems and web servers.
  - Snare Central can report on the command execution activity for all end points, monitoring server, workstation and application logs using the out-of-the-box reporting and the advanced search options.
- Exploitation for Client Execution
  - Snare Agents can collect applicable user command execution of programs that try to exploit vulnerabilities on the local system. The execution of binaries through browser-based exploitation, Office applications, and other common third-party applications can be tracked by the Snare Agent.
  - Standard reporting or the advanced search capabilities can be used in Snare Central to track and monitor the execution of malicious command and can track and trace an adversary when they pivot from system to system.
- Scheduled Task or Job
  - Snare Agents can collect the logs of changes to the scheduled tasks or jobs on a system.
  - Snare Central has specific incident management reports that help track changes to scheduled tasks on the systems. The security team can also create custom reports to look these sorts of changes to other specific platforms.
- Software Deployment
  - Snare Agents can be used to collect logs and activities on Software deployment systems such as SCCM etc. If the systems were accessed by an adversary then the logs can be captured.
  - Snare Central can report on the commands and user login activities for the software deployment systems to see if unauthorized changes are made, or unauthorized access is occurring.
- System Services
  - Snare Agents can collect logs of system service installs and changes. If an adversary was to change or install a system service then the Snare Agents default audit policies will capture it.
  - Snare Central can be used to report on system service changes and execution using the standard incident reporting. The security team can also use the advanced search feature to perform adhoc searches for changes or execution.
- User Execution
  - Snare Agents can collect logs of user execution of programs or malicious payloads that are downloaded and executed. Agents can also collect data that can be analyzed for the presence of malicious links that have been accessed by organizational users.
  - Snare Central can be used to report on commands executed by end-users using standard reporting or adhoc searches using the advanced search feature.
- Windows Management Instrumentation
  - Snare agent can collect logs from the windows system via "filtering platform" events to track any access to the server at the network level. This enables the security team to track WMI connections to the system. Any command execution on the system will be tracked via the normal command tracking capabilities.

Persistence

- Account Manipulation
  - Snare Agents can collect system logs for account changes, additions and deletions. Any account changes logged by the system will be collected by the Snare Agent using the out-of-the-box audit policies. On Unix systems changes to SSH keys or sensitive configuration files, users and groups can be monitored and logged.
  - Snare Central has out-of-the-box reports to help track changes to users, groups for the various operating systems and syslog devices.
- Boot or Login Autostart Execution
  - Snare Agents can collect the logs and monitor sensitive locations where boot and login auto-start execution configuration resides on Windows and Unix platforms either using File Activity Monitoring and/or File Integrity Monitoring. Registry locations can be also be monitored on Windows platforms. Authentication package changes, time provider changes, Winlogin, Kernel modules, shortcut modifications, and reopened applications can all be tracked using the Snare Agents.
  - Snare Central has out-of-the-box reports to help monitor File Activity (FAM) and File Integrity (FIM).
- Boot or Logon Initialization Scripts
  - Snare Agents can track Login scripts for Windows, MacOS, Network Login scripts, RC/Systemd files on Unix systems. and startup items on the various OS platforms using the File Activity Monitoring (FAM) and File Integrity Monitoring (FIM) capabilities.
  - Snare Central can report on these changes either using the standard our of the box reporting or using custom reports. The changes can also be reviewed using the adhoc advanced search options.
- Compromise of Client Software Binaries
  - Snare Agents can all core software on the system using the File Integrity Monitoring (FIM) and File Activity Monitoring (FAM). Any changes to the monitored files will show up as a change, addition or delete of the files.
  - Snare Central can be used to report on FIM and FAM activity using the out-of-the-box reporting.
- Create an Account
  - Snare Agents can track all user account creation, deletion and modifications at the local system level or domain level where the agents are installed. If the accounts are added to groups to gain elevated privileges then these are also tracked and logged.
  - Snare agent can collect logs from the windows system via "filtering platform" events to track any access to the server at the network level. This enables the security team to track WMI connections to the system. Any command execution on the system will be tracked via the normal command tracking capabilities.

- Create or Modify System Processes
  - Snare Agents can collect the audit log activity for all system process changes and execution for Windows, Linux and MacOS platforms. If new services are installed and run then this activity will also be collected. Privilege escalation to administrator or root levels can also be tracked.
  - Snare Central has out-of-the-box reporting to report on system process changes and execution for Windows, Linux, Solaris and MacOS platforms.
- Event Triggered Execution
  - Snare Agents can collect the audit logs that cover Changes to files Associations and system policy configurations, WMI changes, Unix bash profiles, system traps, DLL changes, Application shimming, image files, PowerShell, component object model hijacking etc.
  - Snare Central can be used to report on these program executions and file system modifications either using the out-of-the-box reporting or by creating specific reports for the specific system components.
- External Remote Services
  - Snare Agents can run on systems that provide external services to collect user authentication and allow users to connect to internal systems.
  - Snare Central can take syslog feeds from VPNs, Citrix and other appliance-based systems. Snare Central has a number of out-of-the-box reports that can help with providing analysis such as credential farming or brute forcing of user access to the network.
- Scheduled Job or Task
  - Snare Agents can collect the system audit events for scheduled jobs and tasks and when they execute.
  - Snare Central has out-of-the-box reports to show the details of scheduled tasks and jobs on Windows systems and for Unix systems cronjobs and manual process execution.
- Traffic Signalling
  - Snare Agents can collect network port activity on workstations and servers when available, by creating custom rules to monitor specific network port activity
  - Snare Central can report on the logs the Snare Agents and other syslog devices such as firewalls and IDS/IPS system and report on specific port usage of systems and where it was accepted or denied from the device.
- Valid Accounts
  - Snare Agents can collect system logs for all valid accounts, domain accounts and local accounts used on both Windows and Unix based system.
  - Snare Central has many standard out-of-the-box reports that can report on valid accounts, invalid logins, password failures, domain accounts and local accounts.

Privilege Escalation

- Abuse Elevation Control Mechanism
  - Snare Agents can collect the escalation of user privilege escalation activity on Windows and Unix platforms. On Unix platforms we can track the specific activity for sudo, SUID or SGID program execution.
  - Snare Central has many standard out-of-the-box reports that can report on privileged user activity including administrator or group admin roles on Windows and SUDU, SUID, SGID activity on Unix platforms.
- Boot or Logon Autostart Execution
  - Snare Agents can track changes to existing files and monitor the addition or removal of system files or system settings using File Integrity Monitoring (FIM) or File Activity Monitoring (FAM) along with registry changes using Registry Integrity Monitoring (RIM) or Registry Activity Monitoring (RAM). Where changes occur to the system files that control the system boot and login process the files can be monitored and reported. The login process of the authentication method used is also tracked along with the time provider settings, kernel changes and configuration, applications that are opened such as file and short cut changes.
  - Snare Central has many standard out-of-the-box reports to report on FIM, FAM, RIM and RAM activity on the systems. this helps to detect any system changes and persistence that threat actors try to do.
- Boot or Login Initialization Scripts
  - Snare Agents can collect changes to system files such as File Integrity Monitoring (FIM) or File Activity Monitoring (FAM) along with registry changes using Registry Integrity Monitoring (RIM) or Registry Activity Monitoring (RAM) where this monitoring can track changes to existing files or the addition or removal of system files or system settings. Where changes occur to the system files that control the system boot and login process the files can be monitored and reported. The login process of the authentication method used is also tracked along with the time provider settings, kernel changes and configuration, applications that are opened such as file and short cut changes login script changes, network boot system changes.
  - Snare Central has many standard out-of-the-box reports to report on FIM, FAM, RIM and RAM activity on the systems. this helps to detect any system changes and persistence that threat actors try to do.
- Create or Modify System Process
  - Snare Agents have out-of-the-box standard audit policies that can track the launch of agents systemd services on Unix, Windows Services and the launching of system daemons. Specific FIM, FAM, RIM and RAM audit policies can be implemented to track sensitive applications and configuration items.
  - Snare Central has standard out-of-the-box reporting to report on the system activity of process activity on systems such
    as process execution. Custom reports can be created to report on customer specific application and systems settings.

- Event Triggered Execution
  - Snare Agents can collect changes to system files such as File Integrity Monitoring (FIM) or File Activity Monitoring (FAM) along with registry changes using Registry Integrity Monitoring (RIM) or Registry Activity Monitoring (RAM) where this monitoring can track changes to existing files or the addition or removal of system files or system settings. Where changes occur to the system files that control the system boot and login process the files can be monitored and reported. The login process of the authentication method used is also tracked along with the time provider settings, kernel changes and configuration, applications that are opened such as file and short cut changes.
  - Snare Central has many standard out-of-the-box reports to report on FIM, FAM, RIM and RAM activity on the systems. this helps to detect any system changes and persistence that threat actors try to do. Where system changes and activity has occurred then Snare Central can help with reporting on unusual system activity where the system is generating more events than normal or with changes to the event profile.
- Exploitation for Privilege Escalation
  - Snare Agent can collect the system login activity and the use of privileged users and their activity using its standard out-of-the-box audit policies. The rules can be customized for additional filtering for specific classes of users. Where programs are executed that exploit a vulnerability of another application on the system then the Snare Agent may detect the system change and then the new activity the exploit allowed where it gave them a shell or command prompt on the system.
  - Snare Central standard out-of-the-box reporting can be used to assist with detecting the exploitation of users and in appropriate usage of admin privileges and the execution of other commands.
- Group Policy Modification
  - Snare Agents can collect system policy changes from Windows Group Policy. Where changes occur, the events will indicate what was changed, when and by whom. Where this leads to other system changes such as scheduled tasks, jobs, changes to other software settings, creation of other accounts and program execution these events can be reported.
  - Snare Central has several standard out-of-the-box reports to report on group policy changes. The security team can create specific reporting to track their specific OU and container policy settings and usage.
- Hijack Execution Flow
  - Snare Agents can collect changes to system files such as File Integrity Monitoring (FIM) or File Activity Monitoring (FAM) along with registry changes using Registry Integrity Monitoring (RIM) or Registry Activity Monitoring (RAM) where this monitoring can track changes to existing files or the addition or removal of system files or system settings. Where changes occur to the system files that control the system program workflow the files can be monitored and reported. The program execution and workflow used is also tracked, kernel changes and configuration, applications that are opened such as file and short cut changes login script changes, network boot system changes.
  - Snare Central has many standard out-of-the-box reports to report on FIM, FAM, RIM and RAM activity on the systems. this helps to detect any system changes and process execution that threat actors try to do with manipulation of the path of applications being used.

- Process Injection
    - Snare Agents can collect changes to system files such as File Integrity Monitoring (FIM) or File Activity Monitoring (FAM) along with registry changes using Registry Integrity Monitoring (RIM) or Registry Activity Monitoring (RAM) where this monitoring can track changes to existing files or the addition or removal of system files or system settings. Where changes occur to the system files that control the system program workflow the files can be monitored and reported. The program execution and workflow used is also tracked, kernel changes and configuration, applications that are opened such as file and short cut changes login script changes, network boot system changes.
    - Snare Central has many standard out-of-the-box reports to report on FIM, FAM, RIM and RAM activity on the systems. this helps to detect any system changes and process execution and injection of other components that threat actors try to do with manipulation of the path of applications being used.

- Valid Accounts
    - Snare Agents can collect the logs of the systems for all valid accounts, domain accounts, local accounts used on both Windows and Unix based system.
    - Snare Central has many standard out-of-the-box reports that can report on valid accounts, invalid logins, password failures, domain accounts, local accounts

Defence Evasion

- Abuse Elevation Control Mechanism
    - Snare Agents can collect the escalation of user privilege escalation activity on Windows and Unix platforms. On Unix platforms we can track the specific activity for SUDO, SUID or SGID program execution.
    - Snare Central has many standard out-of-the-box reports that can report on user privileged activity either administrator or group admin roles on Windows and SUDU, SUID, SGID activity on Unix platforms.

- BITS Jobs, De-obfuscate/Decode files or Information, Direct volume access

    - Snare Agents can collect changes to system files such as File Integrity Monitoring (FIM) or File Activity Monitoring (FAM) along with registry changes using Registry Integrity Monitoring (RIM) or Registry Activity Monitoring (RAM) where this monitoring can track changes to existing files or the addition or removal of system files or system settings. Where changes occur to the system files that control the system boot and login process the files can be monitored and reported. The file and process executions of files used is also tracked along with the time provider settings, kernel changes and configuration, applications that are opened such as file and short cut changes login script changes, network boot system changes.
    - Snare Central has many standard out-of-the-box reports to report on FIM, FAM, RIM and RAM activity on the systems. this helps to detect any system changes and persistence that threat actors try to do.

- Execution Guard Rails
  - Snare Agents can be used to collect all system process execution to help detect suspicious processes being spawned that gather a variety of system information or perform other forms of discovery in the system or network.
  - Snare Central has out-of-the-box standard reports that can highlight suspicious of unusual programs that were executed on the systems.

- Exploitation for Defensive Evasion
  - Snare Agents can collect changes to system files such as File Integrity Monitoring (FIM) or File Activity Monitoring (FAM) along with registry changes using Registry Integrity Monitoring (RIM) or Registry Activity Monitoring (RAM) where this monitoring can track changes to existing files or the addition or removal of system files or system settings. Where changes occur to the system files that control the system boot and login process the files can be monitored and reported. The file and process executions of files used is also tracked along with the time provider settings, kernel changes and configuration, applications that are opened such as file and short cut changes login script changes, network boot system changes. Snare Agents can collect the actions performed by users and programs on systems, Where the attacker attempts to disable services and other programs these will be collected up to the point the system becomes unavailable.
  - Snare Central has many standard out-of-the-box reports to report on FIM, FAM, RIM and RAM activity on the systems. this helps to detect any system changes and persistence that threat actors try to do. Snare Central can collect the logs and report on the users actions up to the point the system becomes unavailable.

- File and Directory Permissions Modification
  - Snare Agents can collect changes to system files such as File Integrity Monitoring (FIM) or File Activity Monitoring (FAM) along with registry changes using Registry Integrity Monitoring (RIM) or Registry Activity Monitoring (RAM) where this monitoring can track changes to existing files or the addition or removal of system files or system settings. Where changes occur to the system files that control the system boot, login process and application files can be monitored and reported. The file and process executions of files used is also tracked along with kernel changes and configuration, applications that are opened such as file and short cut changes login script changes, network boot system changes, and system file access controls and permission changes.
  - Snare Central has many standard out-of-the-box reports to report on FIM, FAM, RIM and RAM activity on the systems. this helps to detect any system changes and persistence that threat actors try to do.

- Group Policy Modification
  - Snare Agents can collect system policy changes from Windows Group Policy. Where changes occur the events will indicate what was changed, when and by whom. Where this leads to other system changes such as scheduled tasks, jobs, changes to other software settings, creation of other accounts and program execution these events can be reported.
    Snare Central has several standard out-of-the-box reports to report on group policy changes. The security team can create
  - specific reporting to track their specific OU and container policy settings and usage.
- Hide Artifacts
  - Snare Agents can collect changes to system files such as File Integrity Monitoring (FIM) or File Activity Monitoring (FAM) along with registry changes using Registry Integrity Monitoring (RIM) or Registry Activity Monitoring (RAM) where this monitoring can track changes to existing files or the addition or removal of system files or system settings. Where changes occur to the system files that control the system boot, login process and application files can be monitored and reported. The file and process executions of files used is also tracked along with kernel changes and configuration, applications that are opened such as file and short cut changes login script changes, network boot system changes, as well as system file access controls and permission changes.
  - Snare Central has many standard out-of-the-box reports to report on FIM, FAM, RIM and RAM activity on the systems. this helps to detect any system changes and persistence that threat actors try to do.
- Hijack Execution Flow
  - Snare Agents can collect changes to system files such as File Integrity Monitoring (FIM) or File Activity Monitoring (FAM) along with registry changes using Registry Integrity Monitoring (RIM) or Registry Activity Monitoring (RAM) where this monitoring can track changes to existing files or the addition or removal of system files or system settings. Where changes occur to the system files that control the system program workflow the files can be monitored and reported. The program execution and work flow used is also tracked, kernel changes and configuration, applications that are opened such as file and short cut changes login script changes, network boot system changes.
  - Snare Central has many standard out-of-the-box reports to report on FIM, FAM, RIM and RAM activity on the systems. this helps to detect any system changes and process execution that threat actors try to do with manipulation of the path of applications being used.
- Impair Defenses
  - Snare Agents can collect changes to system files such as File Integrity Monitoring (FIM) or File Activity Monitoring (FAM) along with registry changes using Registry Integrity Monitoring (RIM) or Registry Activity Monitoring (RAM) where this monitoring can track changes to existing files or the addition or removal of system files or system settings. Where changes occur to the system files that control the system program workflow the files can be monitored and reported. The program execution and work flow used is also tracked, kernel changes and configuration, applications
    that are opened such as file and short cut changes login script changes, network boot system changes. Where other system settings are disabled such as firewall, attempt to disable system logging then the agent will send events.
  - Snare Central has many standard out-of-the-box reports to report on FIM, FAM, RIM and RAM activity on the systems. this helps to detect any system changes and process execution that threat actors try to do with manipulation of the path of applications being used. Where the system logging has stopped then the Snare Central healthchecker will report on the absence of system logs from that system providing an early warning of a system problem.

- Indicator Removal on Host
  - Snare Agents have out-of-the-box audit policies to collect special actions such as clearing of event logs, changes to audit policy, The agents can also collect changes to system files using the File Integrity Monitoring (FIM) or File Activity Monitoring (FAM) options along with registry changes using Registry Integrity Monitoring (RIM) or Registry Activity Monitoring (RAM) where this monitoring can track changes to existing files or the addition or removal of system files or system settings. Where changes occur to the system files that control the system program workflow the files can be monitored and reported. The program execution and workflow used is also tracked, kernel changes and configuration, applications that are opened such as file and short cut changes login script changes, network boot system changes. Where other system settings are disabled such as firewall, attempt to disable system logging then the agent will send events.
  - Snare Central has many standard out-of-the-box reports to report on FIM, FAM, RIM and RAM activity on the systems, clearing of event logs, changes to audit policies and user group changes. This helps to detect any system changes and process execution that threat actors try to do with manipulation of the path of applications being used. Where the system logging has stopped then the Snare Central Health Checker will report on the absence of system logs from that system providing an early warning of a system problem.

- Indirect Command Execution
  - Snare Agents can collect logs from the local audit system as as well as from other utilities installed such as Sysmon on Windows that allows the tracking of commands and sub commands/files child process execution along with the parameters used on the commands.
  - Snare Central can use customized reports to report on commands used and where other utilities are installed such as Sysmon then extract the additional information from those event logs showing the details of the commands being run.

- Masquerading
  - Snare Agents can also collect changes to system files using the File Integrity Monitoring (FIM) or File Activity Monitoring
    (FAM) options along with registry changes using Registry Integrity Monitoring (RIM) or Registry Activity Monitoring (RAM) where this monitoring can track changes to existing files or the addition or removal of system files or system
  - settings. Where file changes occur that are out of the normal change control process or are suspect the logs can be collected.

    Snare Central has many standard out-of-the-box reports to report on FIM for file hashing activity, FAM, RIM for registry hashing activity and RAM activity on the systems, clearing of event logs, changes to audit policies and user group changes. This helps to detect any system changes and process execution that threat actors try to do with manipulation of the path of applications being used. Where the files have unusual names or exist in non standard paths then Snare Central can report on those logs of activity. White list exceptions can be reported where files do not match known formats or naming conventions.

- Modify Authentication Process
  - Snare Agents can collect the activity and system changes to DLL files on the system. Registry changes and user password change events can also be collected from all systems the agents run on. On Unix systems PAM files can be monitored for changes and which users access them. System audit polices can be monitored and enforced with the Snare Agents.
  - Snare Central has out-of-the-box reports to look for when users login and which systems they logon to. If the users login during odd hours then out of hours reporting can be used to monitor specific working and after hours usage system accounts are being used. All of these reports can be used to help correlate user activity across systems and actions they perform.
- Modify Registry,
  - Snare Agents have specific audit functions to perform Registry Activity Monitoring that will show the before and after changes to a registry key value, when it occurred and who made the change. Combined with Registry Integrity Monitoring we can collect the hash information for the registry trees or keys.
  - Snare Central has out-of-the-box reports to report on Registry key changes such as new, change and delete RIM events and detailed key value changes using the RAM event reports.
- Obfuscate Files and Information
  - Snare Agents can collect audit logs of modification of files and the commands used to changes the files on the system as part of process execution. By using other tools such as Sysmon on the host we can collect additional forensic event details that show what commands were run to change the files. Other audit events and actions such as FIM and FAM tracking can be used to create hashes and track the user activities performed to change system files.
  - Snare Central can use its out-of-the-box reports to track system file changes from FIM and FAM activity along with process activity from the normal process execution's and the extra details provided by Sysmon.
- Pre OS Boot
  - Snare Agents assist with this by collecting logs from FIM and FAM, RIM and RAM system changes. Where the changes result in a change in file configuration and/or driver details then these changes can be collected.
  - Snare Central can be used to report on the changes to the system boot configuration.
- Process Injection
  - Snare Agents can collect process activity on the systems including network based activity, access or changes to files using FIM and FAM and registry keys using RIM and RAM. The can facilitate the tracking of unauthorized DLL files being used on systems or changes to existing files. System kernel calls and process activity on Linux systems can be tracked using the standard out-of-the-box audit policies configuration but can be tuned to look for specific actions on specific files and locations.
  - Snare Central can report on the user and system activity using the specific reports for FIM, FAM , RIM and RAM as well as the system process activity to report on unusual or unauthorized system changes and activity.

- Rogue Domain Controller
  - Snare Agent should be run on all internal authorized systems. In the case of domain controllers, the agents can collect all system policy and domain based events that come from the security event logs and custom event logs.
  - Snare Central has out-of-the-box reports to show changes and issues with domain controller's policies and replication events. Where there is specific Kerberos based authentication problems that could be attributed to a rogue domain controller trying to sync from the corporate domain controllers then specific reports can be customized for the customers domain environment.

- Signed Binary Proxy Execution
  - Snare Agents out-of-the-box audit policies can collect and monitor process execution on all systems the agents are installed on. Where Sysmon is installed on the systems then the event log data is enriched with addition meta data of what was executed with the command line parameters. Where unsigned binaries are executed then additional events can be collected for this activity.
  - Snare central can be used to report on the actions of commands and processes executed on systems. Other actions like file activity for creations, downloads, modifications etc can be reported using standard reporting.

- Signed Script Proxy Execution
  - Snare Agents can collect process execution activity on systems including scripts such as cscript and where the events include parameters then these will be shown in the logs
  - Snare Central can be used to report on the processes and commands executed on the systems.

- Subvert Trust Controls
  - Snare Agents can collect events and monitor certificate store locations to detect changes or additions of certificates to the systems. FIM capability also report on file attribute changes along with other FAM reporting actions.
  - Snare Central can report on file changes either via FAM or FIM actions on files and certificate stores including file attribute changes.

- Template Injection
  - Snare Agents can collect the event logs of process activity for such things as Office application is performing other actions and spawning child processes or running PowerShell commands
  - Snare Central can report on process activity and include details of the parameters used and child process creation where the event logs have been created.

- Traffic Signaling
  - Snare Agents can collect network traffic event activity such as filtering platform events on windows and Linux platforms Snare Central can collect the network traffic information from Snare Agents and other syslog devices
  - like firewalls to help correlate and look for extraneous network packets and unusual packet flows.
- Trusted Developer Utilities Proxy Execution
  - Snare Agents can collect and monitor process execution on systems which can help facilitate looking for abnormal system utilities and execution that are often linked to malicious activity.
  - Snare Central can be used to report on the system process activity either from the standard reporting or the dynamic searching capabilities.
- Use Alternate Authentication Material
  - Snare Agents can collect system user account activity and also force the system to enable the needed audit policies to ensure the systems generate the needed events.
  - Snare Central has out-of-the-box reports to report on user activity either during business hours or out of hours and specific administrative activity. Where accounts are used over multiple systems the activity can be correlated with other policy requirements.
- Valid Accounts
  - Snare Agents can collect system user account activity and also force the system to enable the needed audit policies to ensure the systems generate the needed events. Both local accounts and domain accounts can be tracked.
  - Snare Central has out-of-the-box reports to report on user activity either during business hours or out of hours and specific administrative activity. Where accounts are used over multiple systems the activity can be correlated with other policy requirements and process exaction activity. The standard reports allow customers to perform regular audits of all privileged users group and usage covering local system and domain groups.
- Virtualisation/Sandbox Evasion
  - Snare Agents running on all systems in the environment allows the security team to collect more information on what the activities are on the corporate network. the higher the quality of the information the better the fervencies will be for detecting the threats.
  - Snare Central can be used to perform log correlation of user activities and help detect issues such as lateral movement of users from one system to another and track the activities of the users from system to system.
- XSL Script Processing
  - Snare Agents can track user and system process activity such as msxsl.ese and wmic.exe which can be used for malicious activity.
  - Snare Central has out-of-the-box reporting that allows the security team to report on process execution. Specific reports can be created to look for these processes and where they are run on the network.

Credential Access

- Brute Force
  - Snare Agents can collect information from authentication logs on Unix systems and the event logs from Windows systems. out-of-the-box policies for the Snare Agents collect login both success and failures.
  - Snare Central has out-of-the-box reports to show login failures and where the failure rate is higher than threshold settings. Real time alerts can also be configured to alert staff which specific accounts or groups go over defined thresholds which can be indicators of a brute force in progress.

- Credentials from Password Stores
  - Snare Agents can collect system activity logs showing if someone is running commands on the system to look for particular files either from file watches on Linux systems or Windows secure stores.
  - Snare Central can report on the process activity on systems and search for accesses to specific locations of passwords stores and accesses to defined password storage location via file activity monitoring.

- Exploitation of Credential Access
  - Snare Agents can collect system activity logs showing if someone is running commands on systems, and can also monitor user login activity
  - Snare Central has out-of-the-box reporting to report on user login activity to help determine if lateral movement is occurring and what commands they are running on the systems. This can help determine is there is abnormal process or user behaviour is occurring.

- Forced Authentication
  - Snare Agents can track local system network activity to monitor for SMB traffic on TCP ports 139, 445, and UDP 137 attempting to exit the network to an unknown external system. File monitoring both FIM and FAM can be implemented to track the creation of links and other files on systems.
  - Snare Central can report on Snare Agent and firewall activity looking for specific accesses to systems and networks using SMB on TCP port 139, 445 and UDP 137 as well as file activity monitoring along with File Integrity Monitoring.

- Man in the Middle
  - Snare Agents can be used to collect logs from systems and detect changes to configuration files for applications that could affect network flow.

    - Snare Central can be used to report on changes to sensitive files and also with network accesses from system to system communication from firewall and networking logs.
- Modify Authentication Processes
    - Snare Agents can collect logs from systems for modifications to sensitive files and registry locations for and DLLs involved with authentication activity. On Unix systems PAM configuration locations can be monitored for changes, and user and account activity can be monitored.
    - Snare Central has out-of-the-box reporting to report on user activity, system administrative activity, policy changes FIM, FAM, RIM and RAM activity on systems. Other logs from VPN appliances can also be collected to enrich and allow correlation with other data sources.
- Network Sniffing.
    - Snare Central can collect logs from firewalls and IDS/IPS devices that can monitor the network for suspicious network packets. This data can then be correlated and report on in the context of other user activity from Snare Agents and other sources.
- OS Credential Dumping
    - Snare Agents can collect the process activity on systems where windows or Unix password stores are being dumped. On Windows the lsass.exe process controls and accessed from various programs to dump the password database.
    - Snare Central can report on specific process activity and can alert if access to specific files are accessed by programs other than the normal operating system access paths.
- Steam Application Access Token
    - Snare Agents can collect authentication logs and user activity and can also monitor sensitive configuration files on systems.
    - Snare Central can report on sensitive file accesses by users and what commands they used to access the files.
- Steal or Forge Kerberos Tickets
    - Snare Agents can collect the relevant windows logs such as 4624, 4672, 4634 and 4769 events using out-of-the-box audit policies and settings
    - Snare Central can report on the user login activity and the contents of the events. Specific reports can be made to look at specific parts of the events for missing or unusual contents. Normal process activity reporting can also be used to look for commands used to dump the credential database stores.
- Two Factor Authentication Interception
    - Snare Agents can track all process executions and software installation using out-of-the-box audit policies. If key loggers are installed or running on the system then the Snare Agent will see the process executions of these commands and send the logs.

        - Snare Central has out-of-the-box reports for process executions and software changes on systems that can report on potential keyloggers being used on systems.
- Unsecured Credentials
    - Snare Agents can collect log activity related to successful and failed user logins using out-of-the-box audit policies and settings. Where other tools like sysmon is installed on windows then additional command line parameters can also be collected to enhance other command activity. File activity and registry activity monitoring can also be used for additional tracking.
    - Snare Central can report on user login activity using standard out-of-the-box reports and can monitor failed login activity to detect unauthorised activity or access attempts which can be correlated with file and registry reporting.

Discover

- Account Discovery
    - Snare Agents being run on all systems will help facilitate forensic information from as many sources as possible to help determine what commands and systems have been accessed.
    - Snare Central can be used to report on regular and help detect unauthorised and unusual systems activity using standard out-of-the-box reporting and using the dynamic search capability to search many log types for specific data values.
- Browser Book Mark Discovery
    - Snare Agents can be used to collect process activity and the execution of PowerShell commands and logs that can be used to collect or harvest users browser details.
    - Snare Central can be used to report on sensitive file accesses as as well process activity on systems.
- Domain Trust Discovery
    - Snare Agents can be used to collect system logs related to process execution using out-of-the-box audit policies.
    - Snare Central has out-of-the-box reports to show process activity on systems. specific reports can be made to look for specific commands or whitelist approved ones and report on exceptions.
- File and Directory Discovery
    - Snare Agents can be used to collect system logs related to process execution using out-of-the-box audit policies for regular commands and PowerShell usage.
    - Snare Central has out-of-the-box reports to show process activity on systems. specific reports can be made to look for specific commands or whitelist approved ones and report on exceptions.
- Network Service Scanning
    - Snare Central can collect logs from firewalls, routers, switches, IDS and IPS systems to help determine and report on network traffic and which devices are scanning hosts looking for vulnerabilities or open ports.

- Network Sniffing
  - Snare Central can collect logs from firewalls and IDS/IPS devices that can monitor the network for suspicious network packets. This data can then be correlated and report on in the context of other user activity from Snare Agents and other sources.
- Password Policy Discovery, Peripheral Device Discovery, Permissions and Group Discovery, Query Registry, Remote Systems Discovery, Software Discovery, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, System/Owner User Discovery, System Service Discovery
  - Snare Agents can collect logs from system activity for processes and commands run on the system as well as tools like PowerShell. The Snare Agent can also collect events and activity for users and group changes and can also monitor users and group members from windows and Unix platforms.
  - Snare Central can report on system user activity and what process and commands they have run. Where other tools like sysmon has been loaded the events will contain additional information on the parameters used and what was searched for on the systems including password related details.
- System Time Discovery
  - Snare Agents can collect system commands and the usage of net.exe and time related command usage.
  - Snare Central can report on process execution related to the usage or the net command and other time related commands.
- Virtualization/Sandbox Evasion
  - Snare Agents can run in many sandbox-based environments and send logs in near real time destinations to allow tracking of system changes and user access activity.
  - Snare Central can be used to report on all user process and user login activity to systems using out-of-the-box reporting or the dynamic searching features.

Lateral Movement

- Exploitation of Remote Services
  - Snare Agent can be run on most end point platforms and allows the audit log collection from these systems to track user login activity and process and command activity.
  - Snare Central can be used to report on the user activity, lateral movement and access methods over remote desktop services or local logons. By tracking the system usage its possible to identify abnormal system and user activity.
- Lateral Tool Transfer
  - Snare Agents can collect user and system activity including file access and copying of data from one location to another on a system.

        - Snare Central can report on the user and file transfer activity by reporting on File Activity Monitoring (FAM) which can happen when data is being exfiltrated from the systems or network. Combined with logs from firewall and routers it is also possible to track the destination of where the data was copied to from host to host.
- Remote Services Session Hijacking, Remote Services
    - Snare Agents can collect logs from systems, login activity and the processes executions with command line parameters used to perform actions on systems.
    - Snare Central can be used to report on the process executions and correlate with user login activity on systems.
- Removable Media
    - Snare Agents can detect removable media and USB device access which is used to transfer and copy large amounts of data from system to system as a well as File Activity Monitoring (FAM) that also tracks the commands used to copy the files. The agents will collect the details from the USB device including its serial number where the manufacturer supplies it. Unix systems also have the file system mount operations tracked for the copying of data and USB, CDROM and DVD device usage.
    - Snare Central has out-of-the-box reports to report on USB and File Activity Monitoring that allows the tracking of access to sensitive information.
- Software Deployment Tools
    - Snare Agents can track the login activity, process execution activity and file activity monitoring that allows for the tracking of software installation and system changes. The Agents can also collect application logs where other unusual and suspicious activity can be logged.
    - Snare Central can report on user login activity, process execution activity and file activity monitoring and correlate this activity with other activity from application logs. Specific reports can be created to look for specific application error conditions.
- Taint Shared Contents
    - Snare Agents can monitor file locations on hosts to detect if the files change with details of who changed the file and what commands were used to change the files.
    - Snare Central can report on sensitive file locations and operations performed on these files.
- Use Alternate Authentication Material
    - Snare Agents can collect user activity including logins, logoffs, login failures, process execution, system policy configuration changes, user and group changes and privileged user activity.
    - Snare Central can be used to report on all the process activity, regular user as well as administrative user activity including privileged functions where it was from normal business hours or out of hours activity. Accounts that are being used over multiple systems from lateral movement of malicious user activity can also be reported.

Collection

- Archive Collected Data, Audio Capture, Automated Collection Techniques, Data from Local systems, Data from Network Share Drives, Data Staged, Email Collection, Input Capture, Man in the Middle Techniques, Screen Capture and Video Capture
  - Snare Agents can track the execution of commands on systems that can be used to archive files and data. FAM monitoring can be implemented for sensitive file locations to track who is accessing the files and data.
  - Snare Central has out-of-the-box reporting to show the types of FAM events and what processes are being run on systems. Custom reports can be made to report on customer specific data and files.
- Data from Configuration Repositories
  - Snare Central can be used to collect logs from firewalls, IDS, IPS and other networking devices to help correlate log data from various sources to identify traffic that it sent or received by untrusted hosts.
- Data from Information Repositories
  - Snare Agents can be used to track access to Information Repositories using FIM, FAM, Process monitoring, user logins, and group permission changes.
  - Snare Central can be used to report on access to sensitive information, the commands run to access the data, what the login, when it happened, along with creating alerts when there is access to sensitive information or data locations or based on threshold levels.
- Data from Removable Media
  - Snare Agents can collect activity from USB and removable media on windows and Unix platforms. For Windows it will collect the specific windows USB events for inserting or removing the media along with the serial number of the device where available. Access to files on removable media can be enabled from the advanced policy settings in Windows. On Unix platforms kernel events from connecting removable media and mounting of file systems can be tracked from the normal kernel calls to track access to the media and files copies to the media using file watch methods.
  - Snare Central can be used to report on removable media devices using out-of-the-box reporting. This allows tracking of USB events, mounting of file systems and access to data in specific locations.

Command and Control

- Application Layer Protocol, Data Encoding
  - Snare Central can be used to collect logs from firewall, routers, switches, and other appliances such as IDS and IPS systems and can help correlate and show systems that have a high or unusual traffic flow, using unusual ports and communications methods.
- Communication Through Removable Media. Ingress Tool transfers, Multi Stage Channels, Remote Access Software, Web Service
  - Snare Agents can collect activity from USB and removable media on windows and Unix platforms. For Windows it will collect the specific windows USB events for inserting or removing the media along with the serial number of the device where available. Access to files on removable media can be enabled from the advanced policy settings in Windows. On Unix platforms kernel events from connecting removable media and mounting of file systems can be tracked from the normal kernel calls to track access to the media and files copies to the media using file watch methods. The agents can also track process and command execution on the host systems to track user activity.
  - Snare Central can be used to report on removable media devices, user activity, command and process execution using out-of-the-box reporting. This allows tracking of USB events, mounting of file systems and access to data in specific locations and to track user activity on each host system. It also allows correlation of user and process activity to detect lateral movement and unusual patterns of activity.
- Data Encoding, Data Obfuscation, Encrypted Channel, Fallback Channels, Non Application layer Protocols, Non Standard Port, Protocol tunnelling, Proxy, Traffic Signalling
  - Snare Central reporting can be used to collect firewall and network device logs and then use standard reporting to identify devices and networks that do not normally have communications or have larger then normal traffic volumes maybe suspicious.

Exfiltration

- Automated Exfiltration, Exfiltration Over Other Network Medium, Exfiltration over Physical Medium, Scheduled Transfer
  - Snare Agents can collect activity from USB and removable media on windows and Unix platforms. For Windows it will collect the specific windows USB events for inserting or removing the media along with the serial number of the device where available. Access to files on removable media can be enabled from the advanced policy settings in Windows. On Unix platforms kernel events from removable media connections, and filesystem mounts, can be tracked from the normal kernel calls. These will track access to media, and files that are copied to the media, using file watch methods. The agents can also track process and command execution on the host systems to monitor user activity.
  - Snare Central can be used to report on removable media devices, user activity, and command and process execution using out-of-the-box reporting. This allows events to be tracked including USB events, file system mounts, access to data in specific locations and user activity on each host system. It also allows correlation of user and process activity to be performed in order to detect lateral movement and unusual patterns of activity.

- Data Transfer Size Limits, Exfiltration Over Alternative Protocols, Exfiltration Over C2 Channel, Exfiltration over Web Service, Transfer Data to Cloud Account
    - Snare Central reporting can be used to collect firewall and network device logs and then use standard reporting to identify devices and networks that do not normally have communications, have larger then normal traffic volumes maybe suspicious and using unusual ports and protocols.

Impact

- Account Access Removal
    - The Snare Agents can collect all user activity including user and group modifications, system policy settings covering user additions and deletions, and password resets on accounts. This combined with process monitoring on systems allows logs to be collected of who was making the system changes.
    - Snare Central has out-of-the-box reporting to highlight user activity and help detect unusual patterns of activity. It can also search for specific user actions and system changes.
- Data Destruction, Data Encrypted for Impact, Data Manipulation, Defacement, Disk Wipe, Endpoint Denial of Service, Firmware Corruption, Inhibit System Recovery, Network Denial of Service, Resource Hijacking, Service Stops
    - The Snare Agents can collect all user activity including FIM, FAM, RIM and RAM user activity and system changes on files and registry locations to detect file deletions or deletion of registry keys. Other user and group modifications, system policy settings covering user additions and deletions, and password resets on accounts. This combined with process monitoring on systems allows logs to be collected of who was making the system changes. It also tracks when a system performs a shutdown or reboot.
    - Snare Central can collect logs from Snare Agents and network syslog devices like firewalls, web application firewalls, IDS/IPS and other devices. It has out-of-the-box reporting to highlight user activity and help detect unusual patterns on logs from network devices, applications, FIM/FAM/RIM/RAM sources, and will allow the security team to monitor user activity and search on specific user actions and system changes.