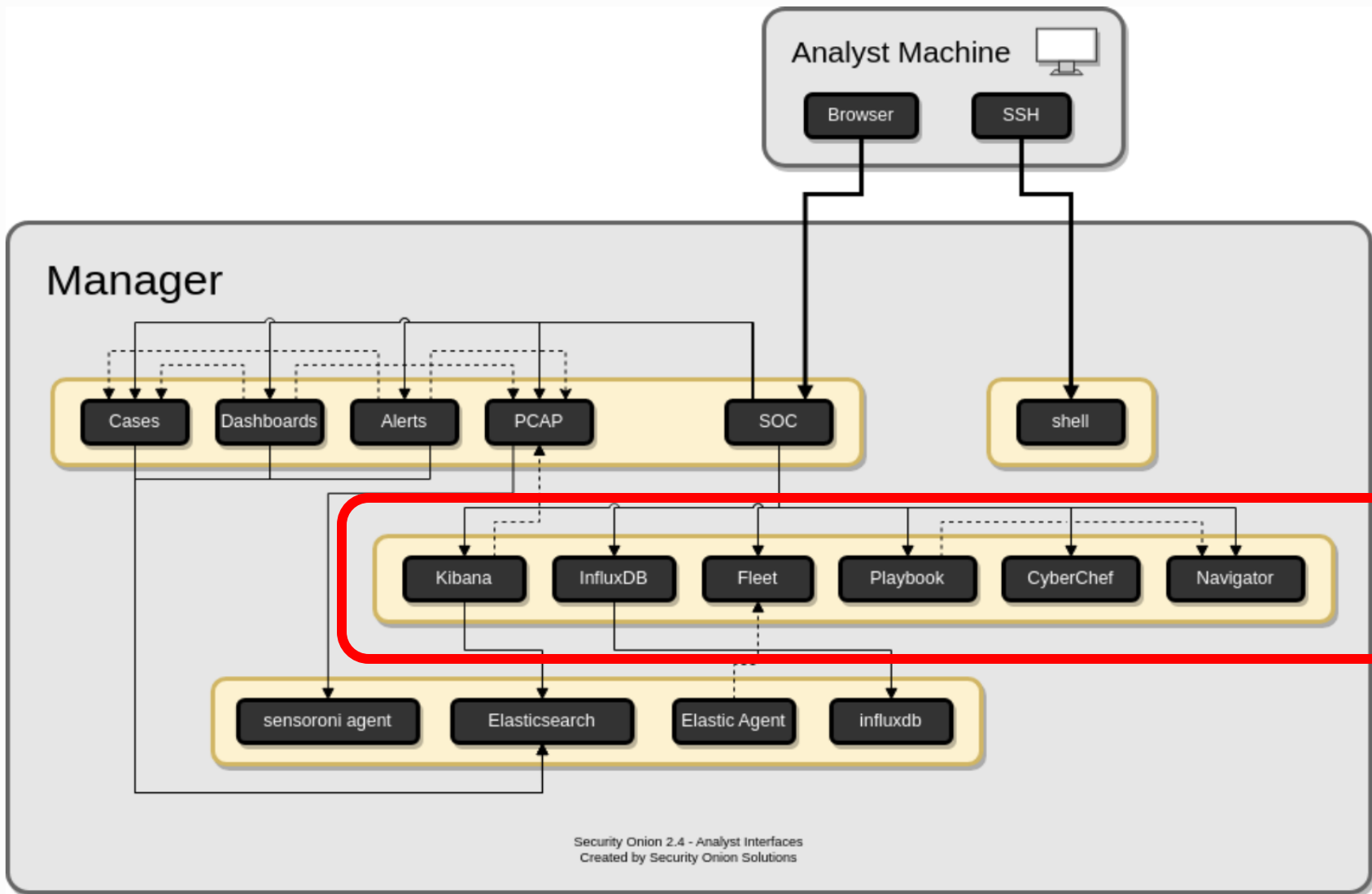


Project Resources (Kibana, CyberChef, Navigator, etc.)

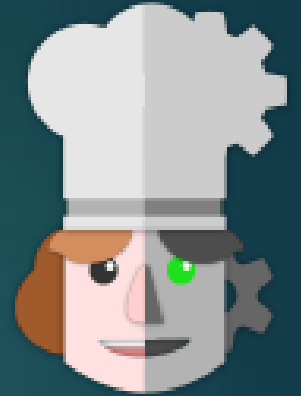
TEAM 29
GRID-SIEM
OCT. 10

Security Onion Console (SOC)



CyberChef

- The Cyber Swiss Army Knife
- A web app for encryption, encoding, compression and data analysis also an open source tool
- Helps security analysts handle complex data without dealing with complex tools.
- Four simple areas within cyberchef: input box, output box, operations list and recipe area.
- From the Security Onion Console, click the cyberchef hyperlink. You can send text from PCAPs to cyberchef for analysis.
- Other tools include: Hashing, compression tools, forensics options...



CyberChef cont.

The four areas:

The screenshot shows the CyberChef web interface. At the top, there's a navigation bar with "Download CyberChef", "Last build: 3 months ago", "Options", and "About / Support". The main area is divided into three columns: "Operations", "Recipe", and "Input".

- Operations:** A list of operations including Search..., Favourites, To Base64, From Base64, To Hex, From Hex, To Hexdump, From Hexdump, URL Decode, Regular expression, Entropy, Fork, Magic, Data format, Encryption / Encoding, Public Key, Arithmetic / Logic, Networking, Language, Utils, Date / Time, Extractors, Compression, and Hashing.
- Recipe:** A list of operations in a recipe: From Hexdump, Strip HTTP headers, Strip HTTP headers, and Strings. The Strings operation has configuration options: Encoding (Single byte), Minimum length (9), and Match (Alphanumeric...). There are also checkboxes for "Display total", "Sort", and "Unique". At the bottom of the recipe area, there's a "STEP" indicator, a "BAKE!" button, and an "Auto Bake" checkbox.
- Input:** A large text area containing hex dump data and a corresponding ASCII representation. Below the input is an "Output" section showing the results of the operations, including file names like "KERNEL32.DLL", "VirtualAlloc", "TstDll.dll", and "TstDll.dll".

View on SecOnion Dashboard:

The screenshot shows the Security Onion dashboard. The top navigation bar includes a menu icon and the "Security Onion" logo. The left sidebar contains a list of tools and features:

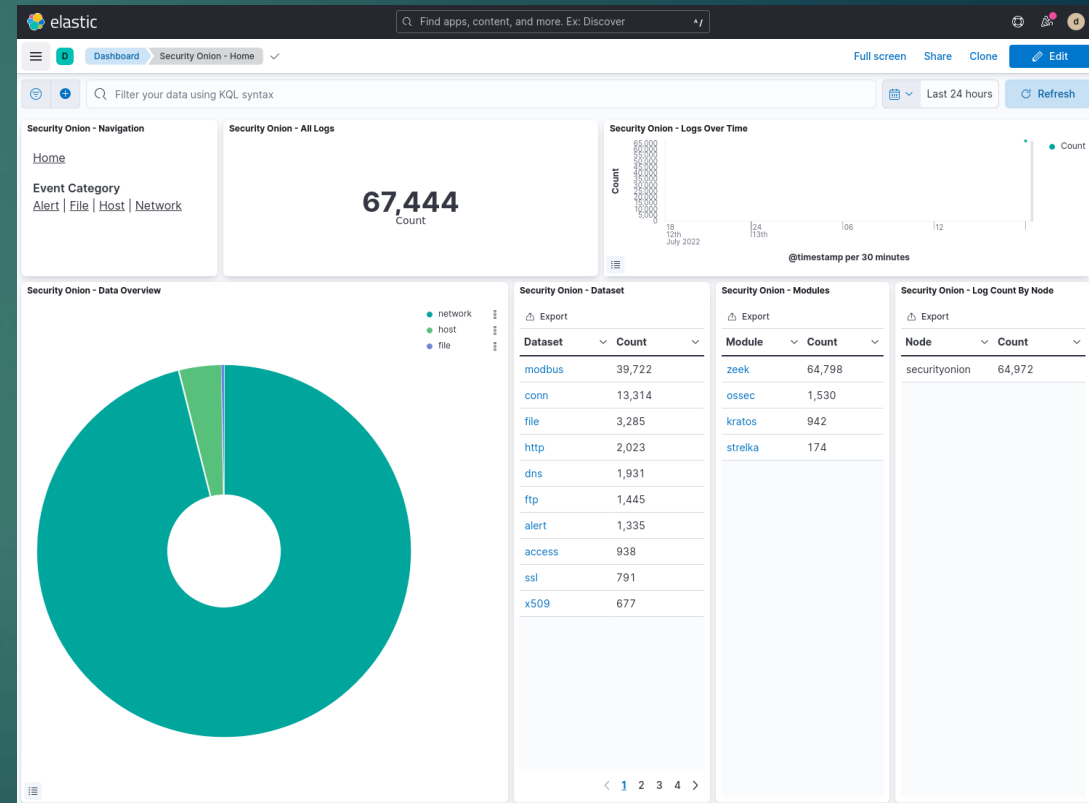
- Overview
- Alerts
- Dashboards
- Hunt
- Cases
- PCAP
- Grid
- Downloads
- Administration
- Users
- Grid Members
- Configuration
- License Key
- Tools
- Kibana
- Elastic Fleet
- Osquery Manager
- InfluxDB
- CyberChef** (highlighted with a red box)
- Navigator

The main content area is titled "Overview" and contains sections for "Getting Started", "What's New", and "Enterprise Appliances".

Version: 2.4.20 © 2023 Security Onion Solutions, LLC

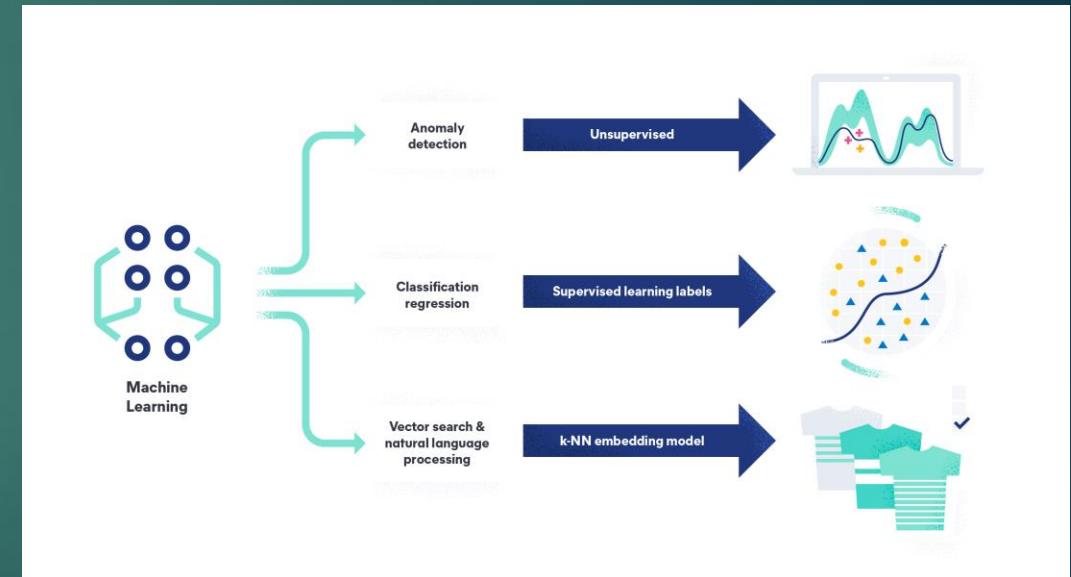
Kibana

- ▶ Kibana is an open-source tool that allows for the visualization of data from Elasticsearch
- ▶ Elasticsearch is required for Kibana to be used
- ▶ Kibana can also be used for data analytics
- ▶ Kibana also advertises machine learning capabilities for threat detection
- ▶ Though there is no hard limit, it is recommended to have 1 Gb of RAM for Kibana.



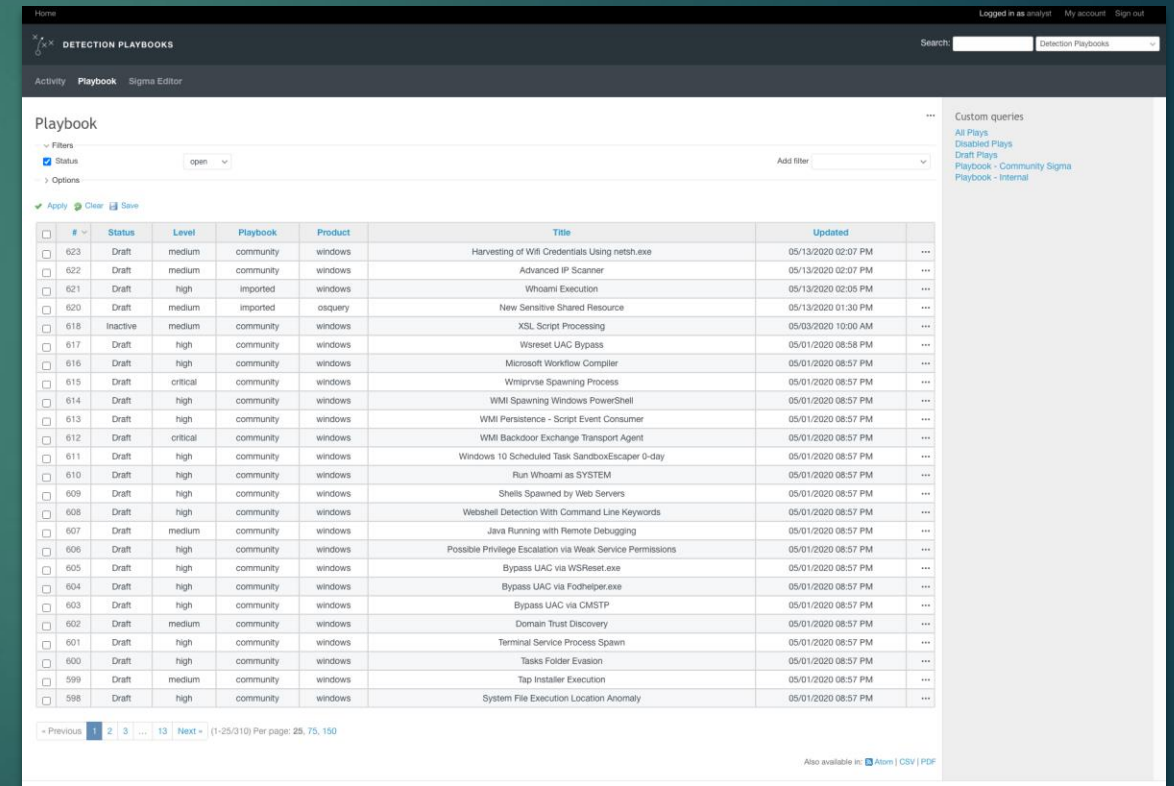
Kibana

- ▶ Having a tool like Kibana could be useful to our project since Elasticsearch is already in our architecture
- ▶ Kibana advertises machine learning tools that are preconfigured and are built on the PyTorch framework
- ▶ Since it is open-source it does not incur any extra cost to the project
- ▶ Data is stored already in Elasticsearch and only requires an extra Gb of RAM.



Detection Playbook

- ▶ <https://docs.securityonion.net/en/2.4/playbook.html#playbook>
- ▶ Outlines of how to detect malicious behavior within the network
- ▶ Use indicators of compromise like logs, network traffic patterns, alert signatures, etc.
- ▶ Can be integrated with Suricata, Zeek, and other threat detection tools
- ▶ Need continuous updates as threat landscape evolves
- ▶ Need adjustment to account for and false positives
- ▶ Results from a playbook can be viewed from kibana
- ▶ High or critical can be viewed in the alerts console



The screenshot displays the Sigma Editor web interface. At the top, it shows the user is logged in as 'analyst' and provides navigation links for 'Home', 'DETECTION PLAYBOOKS', and a search bar. Below the navigation, there are tabs for 'Activity', 'Playbook', and 'Sigma Editor'. The main content area is titled 'Playbook' and includes a 'Filters' section with a 'Status' dropdown set to 'open' and an 'Add filter' button. Below the filters are 'Options' and action buttons for 'Apply', 'Clear', and 'Save'. The central part of the interface is a table listing various playbooks. The table has columns for '#', 'Status', 'Level', 'Playbook', 'Product', 'Title', and 'Updated'. The playbooks listed include titles such as 'Harvesting of WMI Credentials Using netsh.exe', 'Advanced IP Scanner', 'Whoami Execution', 'New Sensitive Shared Resource', 'XSL Script Processing', 'Wreset UAC Bypass', 'Microsoft Workflow Compiler', 'Wtmpvse Spawning Process', 'WMI Spawning Windows PowerShell', 'WMI Persistence - Script Event Consumer', 'WMI Backdoor Exchange Transport Agent', 'Windows 10 Scheduled Task SandboxEscaper 0-day', 'Run Whoami as SYSTEM', 'Shells Spawned by Web Servers', 'Webshell Detection With Command Line Keywords', 'Java Running with Remote Debugging', 'Possible Privilege Escalation via Weak Service Permissions', 'Bypass UAC via WReset.exe', 'Bypass UAC via Fodhelper.exe', 'Bypass UAC via CMSTP', 'Domain Trust Discovery', 'Terminal Service Process Spawn', 'Tasks Folder Evasion', 'Tap Installer Execution', and 'System File Execution Location Anomaly'. The table also includes a pagination bar at the bottom with 'Previous', '1', '2', '3', 'Next', and 'Per page: 25, 75, 150'.

#	Status	Level	Playbook	Product	Title	Updated
623	Draft	medium	community	windows	Harvesting of WMI Credentials Using netsh.exe	05/13/2020 02:07 PM
622	Draft	medium	community	windows	Advanced IP Scanner	05/13/2020 02:07 PM
621	Draft	high	imported	windows	Whoami Execution	05/13/2020 02:05 PM
620	Draft	medium	imported	osquery	New Sensitive Shared Resource	05/13/2020 01:30 PM
618	Inactive	medium	community	windows	XSL Script Processing	05/03/2020 10:00 AM
617	Draft	high	community	windows	Wreset UAC Bypass	05/01/2020 08:58 PM
616	Draft	high	community	windows	Microsoft Workflow Compiler	05/01/2020 08:57 PM
615	Draft	critical	community	windows	Wtmpvse Spawning Process	05/01/2020 08:57 PM
614	Draft	high	community	windows	WMI Spawning Windows PowerShell	05/01/2020 08:57 PM
613	Draft	high	community	windows	WMI Persistence - Script Event Consumer	05/01/2020 08:57 PM
612	Draft	critical	community	windows	WMI Backdoor Exchange Transport Agent	05/01/2020 08:57 PM
611	Draft	high	community	windows	Windows 10 Scheduled Task SandboxEscaper 0-day	05/01/2020 08:57 PM
610	Draft	high	community	windows	Run Whoami as SYSTEM	05/01/2020 08:57 PM
609	Draft	high	community	windows	Shells Spawned by Web Servers	05/01/2020 08:57 PM
608	Draft	high	community	windows	Webshell Detection With Command Line Keywords	05/01/2020 08:57 PM
607	Draft	medium	community	windows	Java Running with Remote Debugging	05/01/2020 08:57 PM
606	Draft	high	community	windows	Possible Privilege Escalation via Weak Service Permissions	05/01/2020 08:57 PM
605	Draft	high	community	windows	Bypass UAC via WReset.exe	05/01/2020 08:57 PM
604	Draft	high	community	windows	Bypass UAC via Fodhelper.exe	05/01/2020 08:57 PM
603	Draft	high	community	windows	Bypass UAC via CMSTP	05/01/2020 08:57 PM
602	Draft	medium	community	windows	Domain Trust Discovery	05/01/2020 08:57 PM
601	Draft	high	community	windows	Terminal Service Process Spawn	05/01/2020 08:57 PM
600	Draft	high	community	windows	Tasks Folder Evasion	05/01/2020 08:57 PM
599	Draft	medium	community	windows	Tap Installer Execution	05/01/2020 08:57 PM
598	Draft	high	community	windows	System File Execution Location Anomaly	05/01/2020 08:57 PM

ATT&CK Navigator

- ▶ Very simple
- ▶ Provides basic annotation of ATT&CK matrices
 - ▶ Basically, just like Excel
- ▶ You can add layers
 - ▶ Default layer is Playbook
 - ▶ Allows you to see your playbook coverage across ATT&CK framework
- ▶ You can add any layers you want

The screenshot displays the MITRE ATT&CK Navigator v4.8.4 interface. The main area is a grid of techniques organized into columns representing different phases of an attack. The columns are: Reconnaissance (10 techniques), Resource Development (7 techniques), Initial Access (9 techniques), Execution (12 techniques), Persistence (19 techniques), Privilege Escalation (13 techniques), Defense Evasion (40 techniques), Credential Access (15 techniques), Discovery (29 techniques), Lateral Movement (9 techniques), Collection (17 techniques), Command and Control (16 techniques), Exfiltration (9 techniques), and Impact (13 techniques). Each cell in the grid contains a technique name and a small icon indicating its status or coverage. The interface includes a top navigation bar with search and filter options, and a bottom status bar with the version number and a legend.

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/2)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/2)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/15)	Boot or Logon Autostart Execution (0/15)	Boot or Logon Autostart Execution (0/15)	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Encoding (0/2)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (0/6)	Browser Session Hijacking	Data Obfuscation (0/3)	Defacement (0/2)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deploy Container	Forge Web Credentials (0/2)	Cloud Service Discovery	Clipboard Data	Remote Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Endpoint Denial of Service (0/4)
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Scheduled Task/Job (0/6)	Scheduled Task/Job (0/6)	Shared Modules	Event Triggered Execution (0/15)	Direct Volume Access	Input Capture (0/4)	Cloud Storage Object Discovery	Data from Cloud Storage Object	Replication Through Removable Media	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Firmware Corruption
Search Open Technical Databases (0/6)		Supply Chain Compromise (0/3)	Shared Modules	Create Account	Escape to Host	Execution Guardrails (0/1)	Modify Authentication Process (0/4)	Container and Resource Discovery	Data from Configuration Repository (0/2)	Software Deployment Tools	Fallback Channels	Exfiltration Over Physical Medium (0/1)	Inhibit System Recovery
Search Open Websites/Domains (0/2)		Trusted Relationship	Software Deployment Tools	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)	Exploitation for Defense Evasion	Network Authentication Process (0/4)	Domain Trust Discovery	Data from Information Repositories (0/3)	Taint Shared Content	Ingress Tool Transfer	Exfiltration Over Web Service (0/2)	Network Denial of Service (0/2)
Search Victim-Owned Websites		Valid Accounts (0/4)	System Services	Event Triggered Execution (0/15)	External Remote Services	Exploitation for Privilege Escalation	Network Sniffing	File and Directory Permissions Modification (0/2)	Data from Local System	Use Alternate Authentication Material (0/4)	Multi-Stage Channels	Scheduled Transfer	Resource Hijacking
			User Execution (0/3)	External Remote Services	Windows Management Instrumentation	Hijack Execution Flow (0/11)	OS Credential Dumping (0/8)	File and Directory Permissions Modification (0/2)	Data from Network Shared Drive		Non-Application Layer Protocol	Transfer Data to Cloud Account	Service Stop
				External Remote Services		Hijack Execution Flow (0/11)	Hide Artifacts (0/9)	File and Directory Permissions Modification (0/2)	Data from Removable Media		Non-Standard Port		System Shutdown/Reboot
				External Remote Services		Process Injection (0/11)	Hijack Execution Flow (0/11)	Hide Artifacts (0/9)	Protocol Tunneling				
				External Remote Services		Scheduled Task/Job (0/6)	Impair Defenses (0/9)	Steal or Forge Kerberos Tickets (0/4)	Data Staged (0/2)				
				External Remote Services		Valid Accounts (0/4)	Indicator Removal on Host (0/6)	Steal or Forge Kerberos Tickets (0/4)	Email Collection (0/3)				
				External Remote Services			Indirect Command Execution	Steal Web Session Cookie	Input Capture (0/4)				
				External Remote Services			Masquerading (0/7)	Two-Factor Authentication Interception	Screen Capture				
				External Remote Services			Modify Authentication Process (0/4)	Unsecured Credentials (0/7)	Video Capture				
				External Remote Services			Modify Cloud Compute Infrastructure (0/4)						
				External Remote Services			Modify Registry						
				External Remote Services			Modify System Image (0/2)						
				External Remote Services			Network Boundary Bridging (0/1)						