MNSEC 2022

SOC process improvement

UNITEL LLC IDERBUKH.I

WHO AM I?

MUST-SICT

- Bachelor 2013-2017
- Master 2017-2020

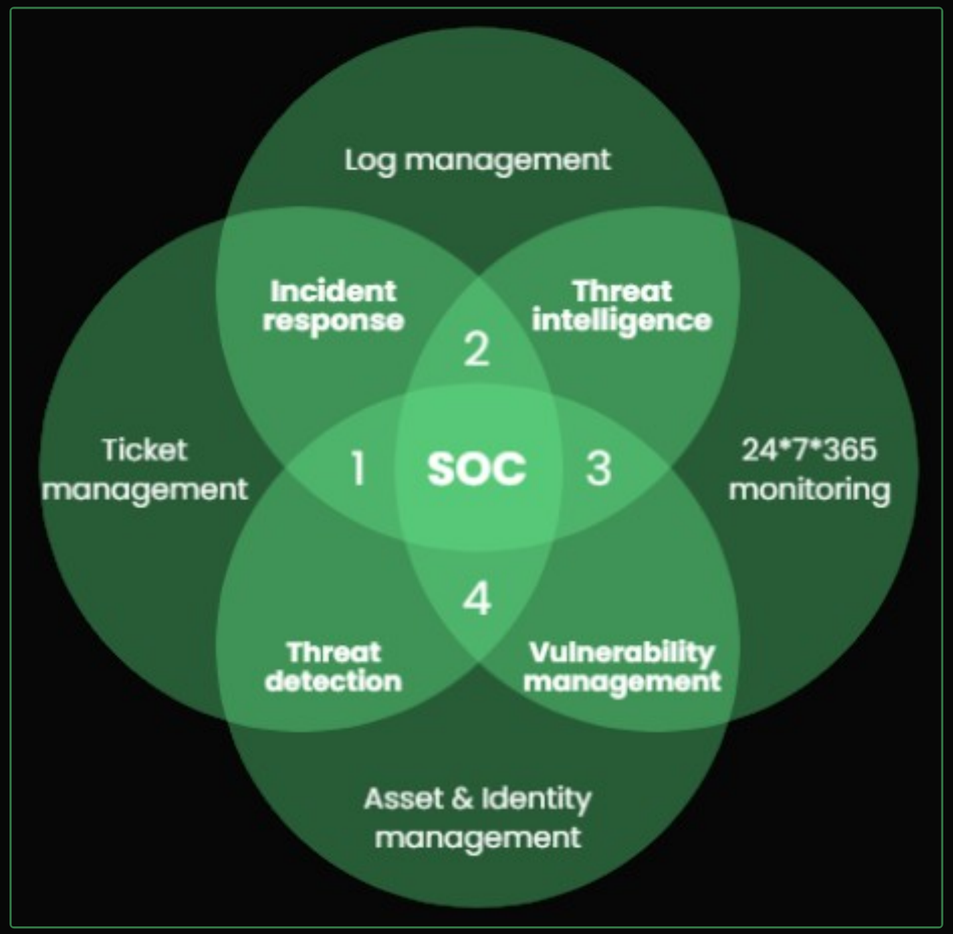
@MUST-SICT, Assistant teacher 2017-2019
@UNITEL LLC, Information security analyst

AGENDA

- Defination of Security Operation Center
- Endpoint security assessment
  - System and process monitor
  - Detection & prevention capability measure
  - Breach and attack simulation
- Detection coverage
- Result

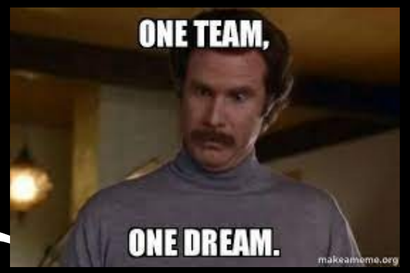
Security Operation Center

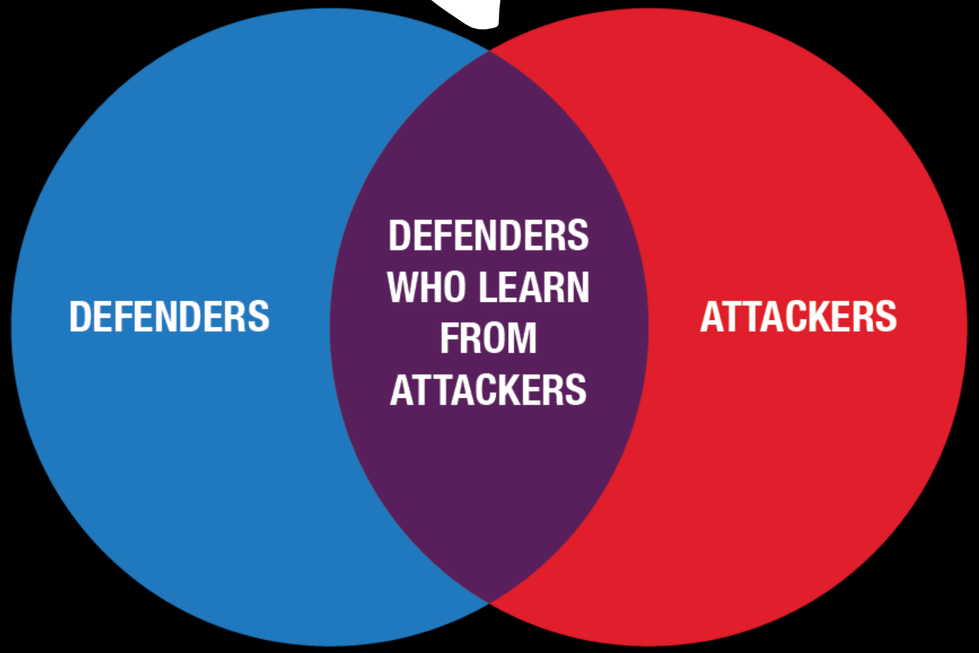
Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.



Endpoint Security Assessment

- According to a study by the Ponemon Institute, 68% of organizations have experienced one or more endpoint attacks that successfully compromised data and/or their IT infrastructure.
- 53% of organizations were hit by a successful ransomware attack in 2021, and around 77% of those were hit more than once.
- Virtual team, Red and Blue work together to improve the overall security of the organization.
- Goal - Red Team emulates adversary TTPs while blue teams watch and improve detection and response policies, procedures, and technologies in real time.





https://webinarcare.com/best-endpoint-protection-platforms-software/endpoint-protection-platforms-statistics/

MITRE ATT&CK MATRIX

RED ATOMIC TEAM

Tactic {

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark	Distributed Component	Clipboard Data
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Byp Acc				

Drive-by Compromise

A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation. This can happen in several ways, but there are a few main components:

Multiple ways of delivering exploit code to a browser exist, including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.[1]

Drive-by Compromise Technique	
ID	T1189
Tactic	Initial Access
Platform	Linux, Windows, macOS
Permissions Required	User
Data Sources	Packet capture, Network device logs, Process use of network, Web proxy, Network intrusion detection system, SSL/TLS inspection

Technique

Procedure

43 lines (28 sloc) 1.79 KB

Raw Blame History

T1007 - System Service Discovery

Description from ATT&CK

> Adversaries may try to get information about registered services. Commands that may obtain information about services using operating system utilities are "sc," "tasklist /svc" using Tasklist, and "net start" using Net, but adversaries may also use other tools as well.
> Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.
>
> Monitor processes and command-line arguments for actions that could be taken to gather system information related to services. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.
>
> Platforms: Windows
>
> Data Sources: Process command-line parameters, Process monitoring
>
> Permissions Required: User, Administrator, SYSTEM

Atomic Tests

- Atomic Test #1 - System Service Discovery

Atomic Test #1 - System Service Discovery

Identify system services

Supported Platforms: Windows

Inputs

Name	Description	Type	Default Value
service_name	Name of service to start stop, query	string	svchost.exe

Run it with `command_prompt` **!**

```
tasklist.exe
sc query
sc query state= all
sc start ${servicename}
sc stop ${servicename}
wmic service where (displayname like "${servicename}") get name
```

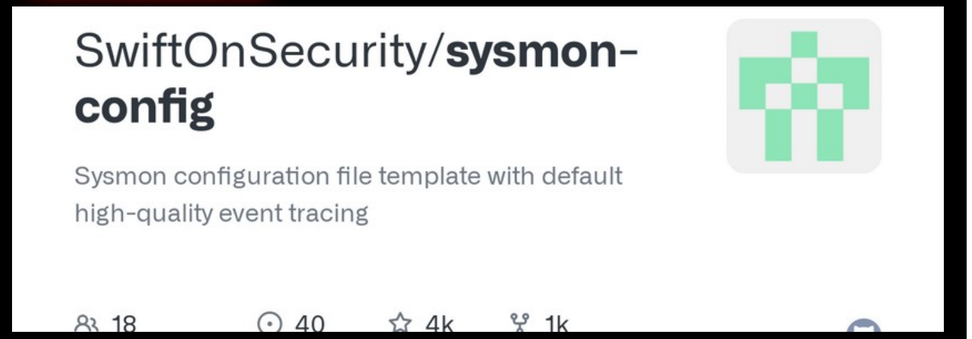
SYSMON

Sysinternals - System monitor v14

- Windows
- Linux - 2021

Created by: Mark Russinovich and Thomas Garnier - Defrag tools

RECOMMENDED



https://github.com/SwiftOnSecurity/sysmon-config

SYSTEM AND PROCESS MONITOR

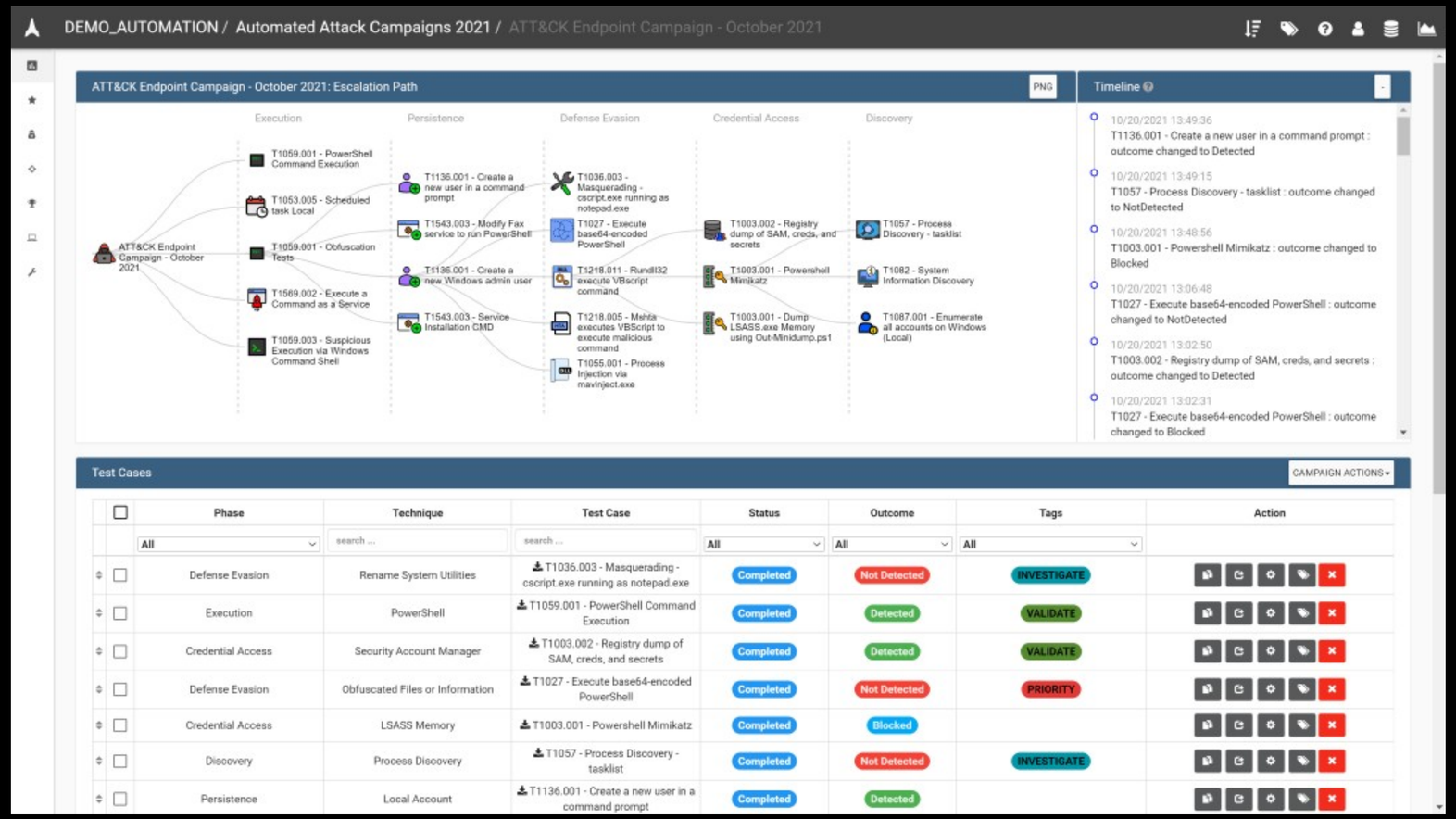
- Process Create & Terminated
- File create & delete
- Network connection
- Powershell & cmd command
- DNSQuery
- CreateRemoteThread
- Registry Event
- WmiEvent
- FileBlockExecutable NEW

DETECTION & PREVENTION CAPABILITY MEASURE

vectr

We believe purple teams using VECTR is the best way to assess and validate cybersecurity detections and improve SOC capabilities.

- Open source
- Planing and tracking Red team & Purple team
- Create new assessment template
- Powerful report
- Automated Adversary emulation



VECTR DASHBOARD

DEMO_ATOMIC_RED_CE / Atomic Red (MITRE) Assessment - 2018

Campaign Dashboard

NEW CAMPAIGN | EDIT

Name	Progress	Outcome	Tags	Action
Exfiltration	100%	38% 13% 50%		
Collection	100%	42% 58%		
Defense Evasion	22% 78%	2 8% 11% 78%		
Discovery	69% 31%	29% 40% 31%		
Privilege Escalation	100%	9% 66% 25%		
Lateral Movement	100%	26% 47% 26%		
Persistence	30% 70%	11% 19% 70%		
Execution	100%	11% 51% 38%		
Command & Control	40% 60%	10% 30% 60%		
Initial Access	100%	100%		
Credential Access	100%	11% 32% 57%		

VECTR USE CASE PANEL

Edit Persist via Userinit Winlogon Test Case

Status: Completed

Attack Start

08/22/2022 17:28:15
status changed to InProgress

Attack Stop

08/22/2022 17:28:16
status changed to Completed

Sources

Targets

192.168.1.105

Red Team Details

Name

Persist via Userinit Winlogon

Description

Persist on a system by creating an LNK in the user's startup folder that points an exe payload then adding the LNK to the userinit registry

Technique

Winlogon Helper DLL - T1547.004

Phase

Persistence

Operator Guidance

```
cmd> reg.exe add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v "Userinit" /t REG_SZ /f /d "C:\Windows\system32\userinit.exe,%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\{{ lnk_name }}.lnk"
```

Blue Team Details

Outcome

- [ ] TBD
- [ ] Blocked
- [ ] Alerted
- [ ] Logged
- [x] None
- [ ] N/A

Outcome Notes

No detection noted in SIEM logs around attack time 08/22/2022 17:28:15 for host 192.168.1.105 (pa-desktop-test01)

Tags

CHECK LOGGING

Rules

Sigma

Detection Tim

08/22/2022 17:2
outcome change

Defenses

SIEM

Endpoint Protec

Document Managament

- Overlap
- Use case manage, tune
- Created time, Report

Type	Key	Summary	P	Status	Resolution	Created ↓
	NFSC-259	T1003.004: LSA Secrets	=	DONE	Done	Jul 28, 2022
	NFSC-257	T1564.004 Alternate Data Streams (ADS)	=	DONE	Done	Jul 22, 2022
	NFSC-256	T1027.004 - Compile After Delivery	=	DONE	Done	Jul 19, 2022
	NFSC-255	T1218.007: Msiexec	=	DONE	Done	Jul 18, 2022
	NFSC-254	T1546.012 - Image File Execution Options Injection	=	DONE	Done	Jul 8, 2022
	NFSC-253	T1037.001 - Logon Script (Windows)	=	DONE	Done	Jul 8, 2022
	NFSC-252	T1574.008: Path Interception by Search Order Hijacking	=	DONE	Done	Jul 8, 2022
	NFSC-251	T1555.004 - Access Saved Credentials via VaultCmd	^	DONE	Done	Jul 7, 2022
	NFSC-250	T1505.004: IIS Components	=	DONE	Done	Jul 5, 2022
	NFSC-249	T1546.007 - Netsh Helper DLL	=	DONE	Done	Jul 5, 2022
	NFSC-248	T1574.002 - DLL Side-Loading	=	DONE	Done	Jul 1, 2022
	NFSC-247	T1041 - Exfiltration Over C2 Channel	=	IN PROGRESS	Unresolved	Jun 30, 2022
	NFSC-246	T1021.005: VNC	=	DONE	Done	Jun 29, 2022
	NFSC-245	T1087.004: Cloud Account	=	DONE	Done	Jun 29, 2022
	NFSC-244	T1087.003: Email Account	=	DONE	Done	Jun 29, 2022

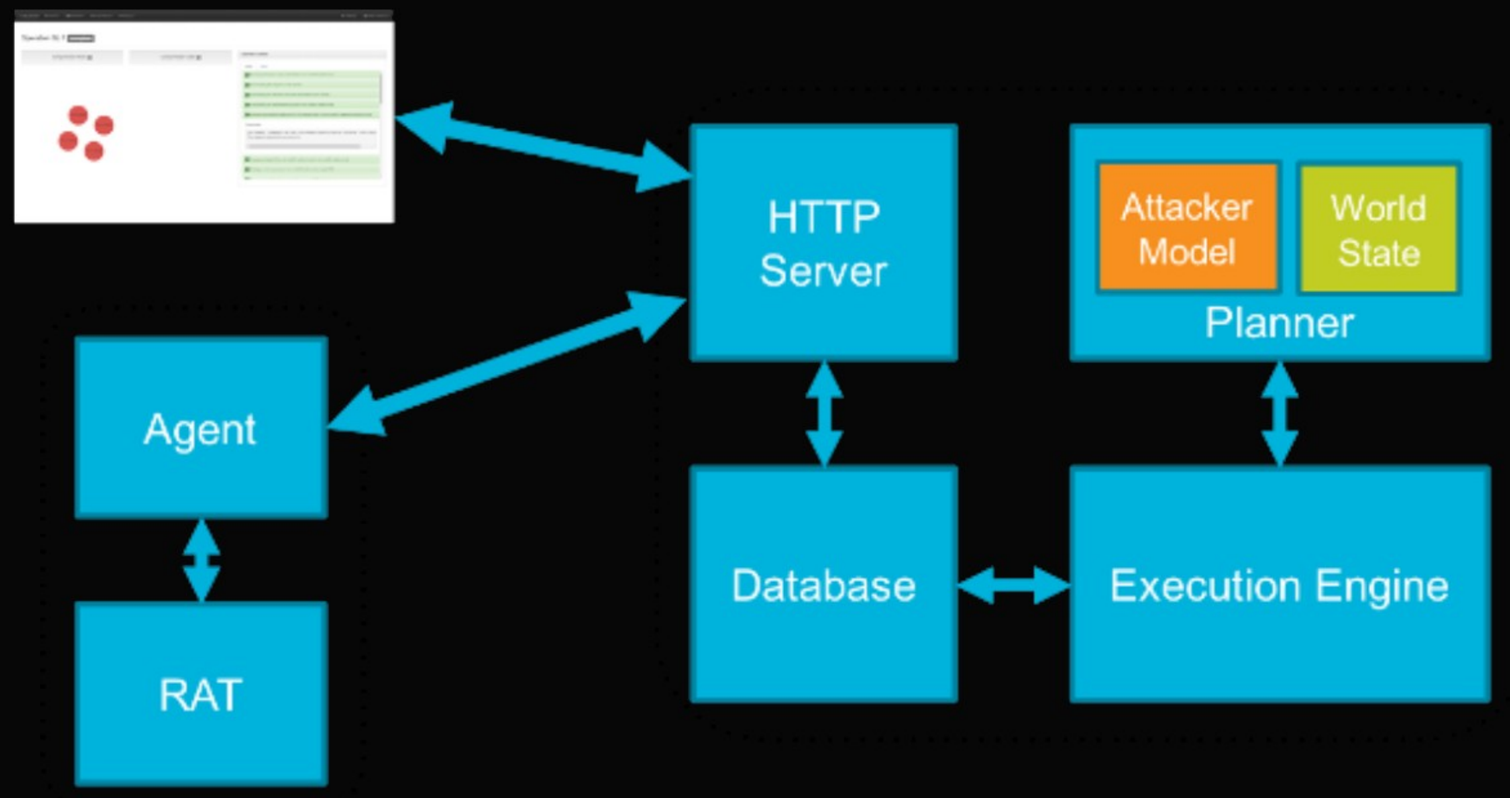
BREACH AND ATTACK SIMULATION

CALDERA

- Open Source project
- Test your SOC team against the latest threats used by real threat actors
- Gameboard plugin (Red team vs Blue team)
- Atomic red team plugin
- Manual adversary
- Automation

CALDERA ARCHITECTURE

- Server and agent python 3
- Rat wriiten in C#
- MongoDB
- Web interface JavaScript



One team One dream

1. Process update
2. New tasks to assign
3. New ideas

Detection coverage

STEP 1

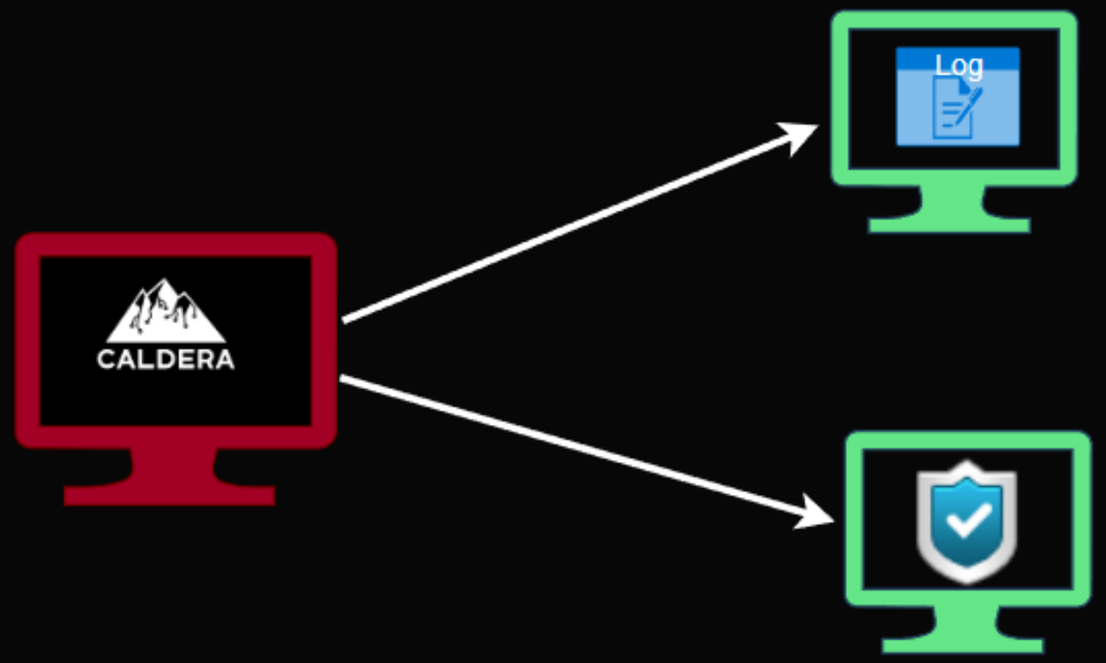
ONLY SYSMON

DETECTION

STEP 2

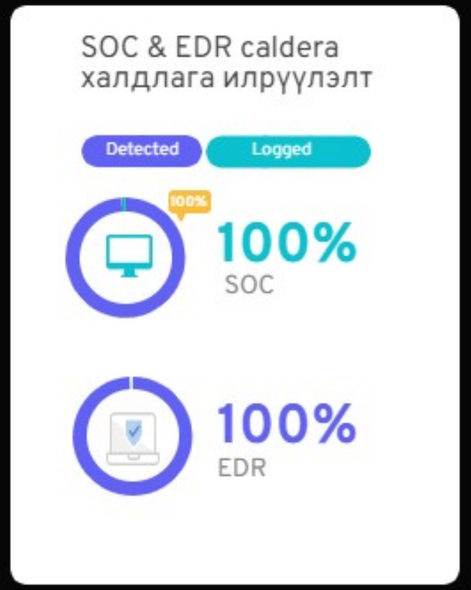
SYSMON + EDR

DETECTION + BLOCKED



RESULT

- False positive
- Caldera, Vectr update



MITRE ATT&CK	SOC	EDR
Collection	100%	100%
Execution	100%	100%
Credentials access	100%	100%
Lateral movement	100%	100%
Privilege escalation	100%	100%
C&C	100%	100%

MITRE ATT&CK	SOC	EDR
Defense evasion	100%	100%
Exfiltration	100%	100%
Initial access	100%	100%
Persistence	100%	100%

Thank you for your attention