



- An EDR platform

A report by Pedapati Prem Kumar



INTRODUCTION

Cybereason is an advanced End Point Detection response (EDR) and Extended Detection and Response (XDR) platform that is designed to detect, analyse and respond to cyber threats across endpoints, networks, and the cloud. Cybereason was founded by three former Israeli military intelligence (unit 8200) operatives Lior Div, Yonatan Amit and Yossi Naar in 2012. The company was headquartered in Boston, Massachusetts (USA), with research and development operation in Tel Aviv, Israel. It has grown into major cybersecurity vendor, backed by investors including Soft Bank, CRV and Spark Capital. It leverages behavioral analytics, machine learning and threat intelligence to provide proactive defence against malware, ransomware, and advanced persistent threats (API's). The platform's widely adopted in enterprise environments for its strong correlation capabilities and automated response features.

Key Features:

Malop Operations: Proprietary feature that correlates multiple malicious activities into a single incident (Malop). It also helps security teams prioritize investigations by focusing on completing attack campaigns rather than isolated alerts.

Threat Intelligence Integration: Enriches detections with global threat intelligence feeds. Provides context around the threat actors, TTPs, (tactics, techniques, procedures), and known IOCs.

Endpoint Detection and Response: Monitors endpoint activities in real time and detect malicious behaviour using behavioral and machine learning models. Provides detailed attack timelines with visual maps for easier incident analysis.

Extended Detection and Response: Integrates telemetry across endpoint, cloud, identities and networks and provides holistic detection and correlation of attack chains. Enhances visibility into complex attacks like lateral movement and credentials abuse.

Artificial Intelligence and Machine Learning: AI assists threat hunters by flagging anomalies in large datasets. Analysts can run queries across billions of endpoint events, with ML modules surfacing likely malicious activity and reduces manual hunting time and enhances proactive detection.

Attack Storyline Visualization: Reduces manual hunting time and enhances proactive detection and instead of isolated alerts, Cybereason builds a visual timeline of the full attack chain. Each event (initial compromise, lateral movement, credential theft, exfiltration, etc.) is chronologically ordered.

Chronological Event Correlation: Collects detailed telemetry from endpoints (process creation, registry changes, files modifications, network connections) and it also correlates those logs into a unified forensic timeline. Provides precise timestamps for every malicious action, which is critical for investigations.

Cybereason Defense Platform

Future-Ready Cybersecurity



An overview of Cybereason Defense Platform

The Cybereason EDR solution, built upon Cybereason Technology, is composed of several integrated platform components that work together to provide comprehensive protection from the endpoint to the broader corporate structure. The core of the Cybereason is integrate with next generation antivirus (NGAV) and proactive threat hunting. This combination enables the platform to provide rich, detailed analysis for every part of a malicious operation. There are some optional dashboards that which are used to analyse and respond the attacks.

They are:

1. Discovery Board

2. Malop Inbox

3. Malware Alerts

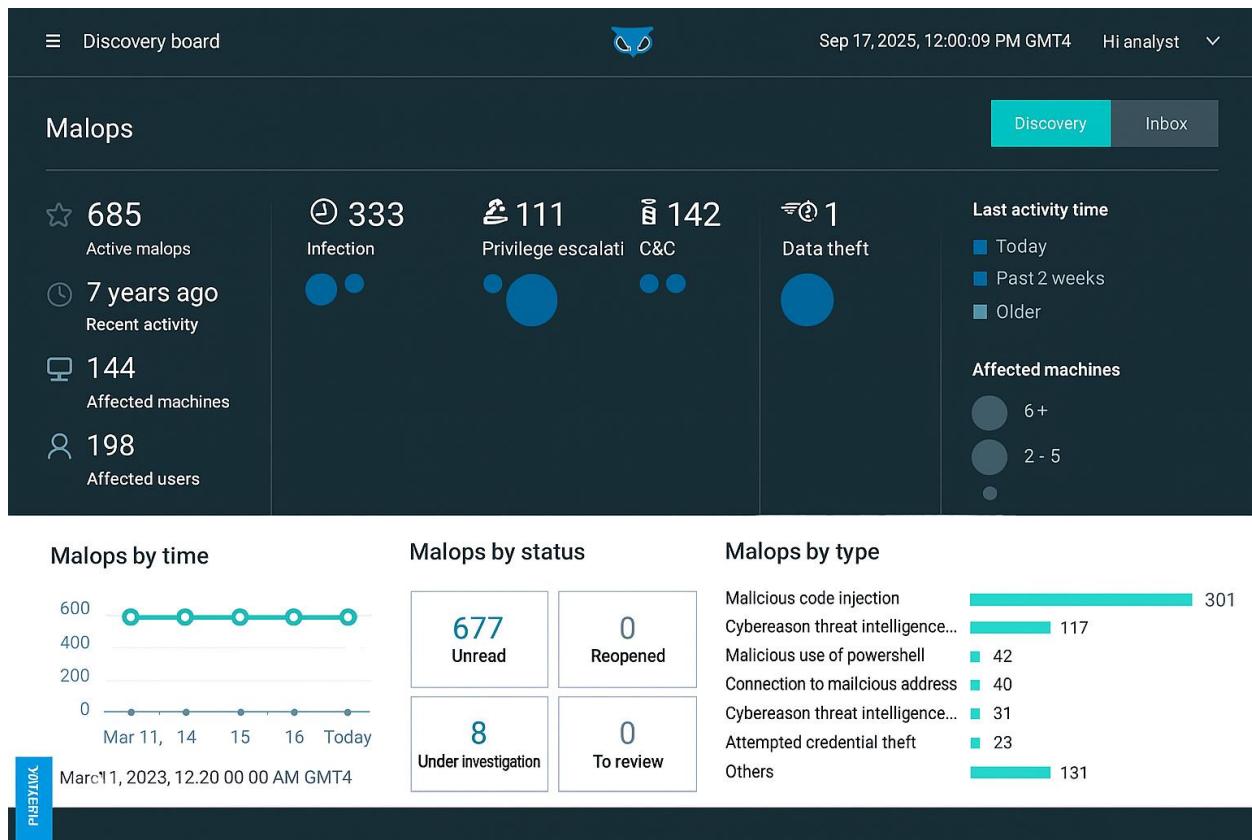
4. Investigation

5. Security Profile

Discovery Board

The Discovery Dashboard is a centralized interface used in Cybereason platform to provide analysts with a clear and consolidated view of potential malicious operations (MalOps) happening within an environment. Its main purpose is to help security teams quickly detect, categorize, and monitor suspicious activities across machines and users. By consolidating threat intelligence, attack stages, and investigation status into one place, the dashboard enables faster incident response, prioritization of threats, and overall better visibility into the security posture of the organisation. In short, it acts as a command center for identifying, tracking, and managing security incidents efficiently. Discovery Board categorizes the malops activities into different malicious activities into stages of the attack which was performed by the attacker.

The Bubbles/Circles in the discovery dashboard are a visual representation of different categories of malicious activities. Their primary purpose is to make complex security data easier to interpret immediately.



Dashboard Of Discovery Board

The size of the bubble reflects the volume or severity of incidents in that category. Larger bubbles indicate a higher number of detailed numbers and colour of bubble reflects the past/active stage of the attack like dark colour of the bubble represents older attacks and light colour bubbles indicates the recent/present activity.

Malop Inbox

The Malop Index is a central hub for managing ongoing and historical security incidents, giving analysts an easy way to track infections, understand the root cause, and take remediation actions. It highlights the root cause, so we know what triggered the attack in the first place. It helps to group and filter Malops to gain an understanding of your system status. It sorts the list by Type, Root causes, affected machines, detected activity, Labels, creation date, time of last activity, and Status. Malops provide visibility into lateral movement, privilege escalation and other attack techniques, using advanced threat intelligence and behavioral analysis.

The screenshot shows the Malop Index dashboard with the following details:

Type	Root cause	Affected machines	Detected activity	Labels	Created	Last activity	Status
File	dwn.exe Known malware Cybereason Threat Intelligence identified a malicious executable	2 machines	Infection		December 24, 2018 at 8:26:36 AM GMT-5	7 years ago	
File	sct1ob_r.ttf Malicious process Process opened a malicious file	AEP-S1-V104	Infection		November 27, 2018 at 2:25:51 PM GMT-5	7 years ago	
Module	dishful.dll Known malware Cybereason Threat Intelligence identified a loaded module as malici...	2 machines	Infection		November 27, 2018 at 9:23:15 AM GMT-5	7 years ago	
File	1.exe Known malware Cybereason Threat Intelligence identified a malicious executable	AEP-S1-V49	Infection		November 27, 2018 at 9:23:15 AM GMT-5	7 years ago	
File	luck.exe Known malware Cybereason Threat Intelligence identified a malicious executable	2 machines	Infection		November 27, 2018 at 9:23:15 AM GMT-5	7 years ago	
File	1.exe Known malware Cybereason Threat Intelligence identified a malicious executable	AEP-S1-V19	Infection		November 27, 2018 at 9:23:34 AM GMT-5	7 years ago	
13.68.93.109							
September 6,							

Dashboard of Malop Index

As per the picture above we can see the dashboard of the Malop Index which contain several categories and classifications of the attacks on the left side of the dashboard which shows the severity of the attacks – **High**, **Medium** and **Low**.

By clicking on any those attacks that are shown in the malop index can create and displays the graphical visual representation of the attack with the help of artificial intelligence and machine learning algorithms. These Malop Index contains four main tabs which are used to breakdown the attack into various stages and factors that are affected by the system. Those four tabs include:

A. Overview

B. Process Profile

C. Communication Profile

D. Machine Profile

E. Users Profile

These four tabs describes about various information of the attack at different stages and provides visual data representation of the attack at their perspective stage.

A. Overview: This section contains a detailed description page of the attack which contain information like Root-cause information, Scope of impact, Detection age, Timeline of events, Suspicious indicators and Isolate & Response options.

The screenshot displays the Malop dashboard for the process dwn.exe. At the top, there's a navigation bar with tabs for Overview, Processes, Communication, Machines, and Users. The main content area is titled 'dwn.exe' and shows a summary of the attack. It includes sections for 'Description', 'Timeline', and 'Suspicious'. The 'Timeline' section shows a timeline from May 12, 2018, to April 2, 2019, with key events like 'First execution on first machine' and 'Known malware' detection. The 'Suspicious' section lists 'Process has a suspicious hash' and 'Malware module indications'. A central diagram illustrates the attack flow, showing 'Affected machines' (2), 'Affected users' (2), and various connection types: 'No Connections Incoming connections', 'Unknown Connection Outgoing connections', and 'Infection'.

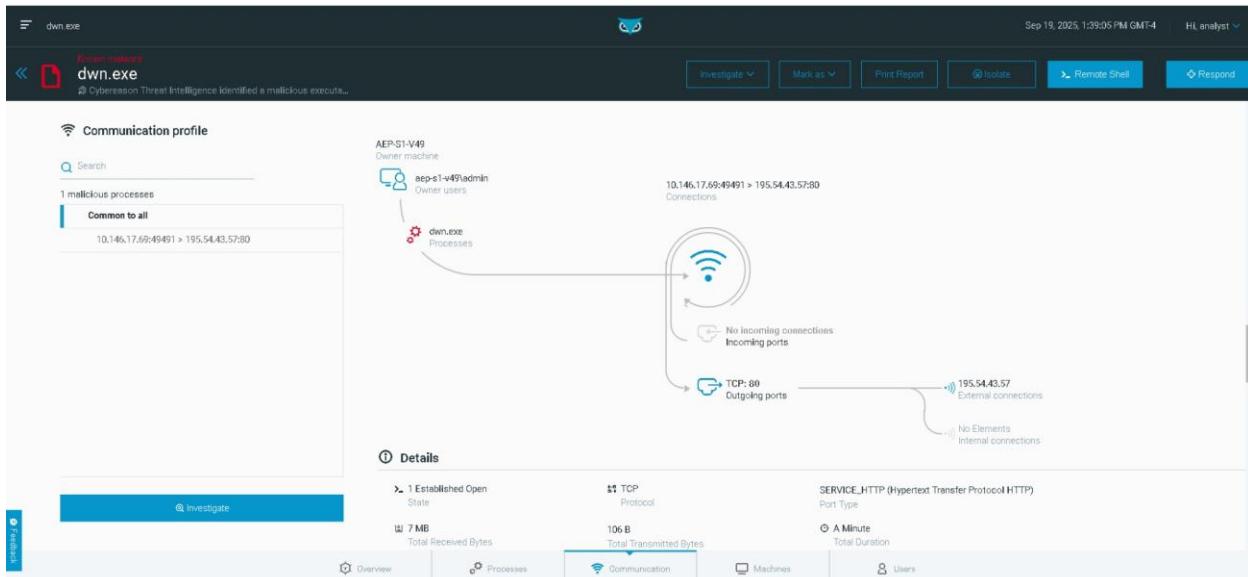
Dashboard of Overview Tab

B. Process Profile: The process profile tab contains details of the attack in a process's perspective. This dashboard shows details of the process that are part of the Malop which includes child processes, IDs, .exe files, execution commands, sessions and suspicious modules that are involved in the attack.

The screenshot displays the Malop dashboard for the process dwn.exe, specifically the 'Processes' tab. It shows a list of '4 malicious processes' under the heading 'Processes profile'. Below this, there's a 'File' section with details like 'Neutral Reputation', 'Unsigned Signature', and 'File Hash: 72c569a0bc3d3425c295ce12e79815e33f0155'. There's also an 'Execution' section showing 'multiple Command Line'. At the bottom, there are tabs for Overview, Processes, Communication, Machines, and Users, with the 'Processes' tab currently selected.

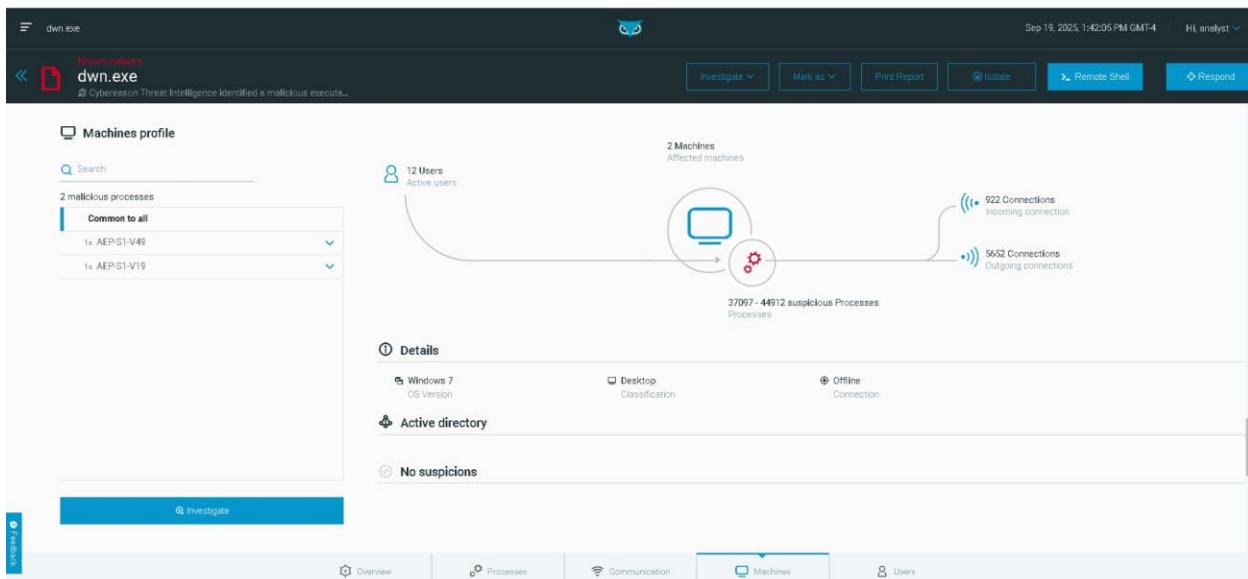
Dashboard of Process Profile

C. Communication Profile: Communication profile tab describes about details in network perspective. It contains details about User connections, ports, protocols, services, Internal/External connections and graphical representation of the attack. It also describes about the domains and data bytes that are transmitted through a network.



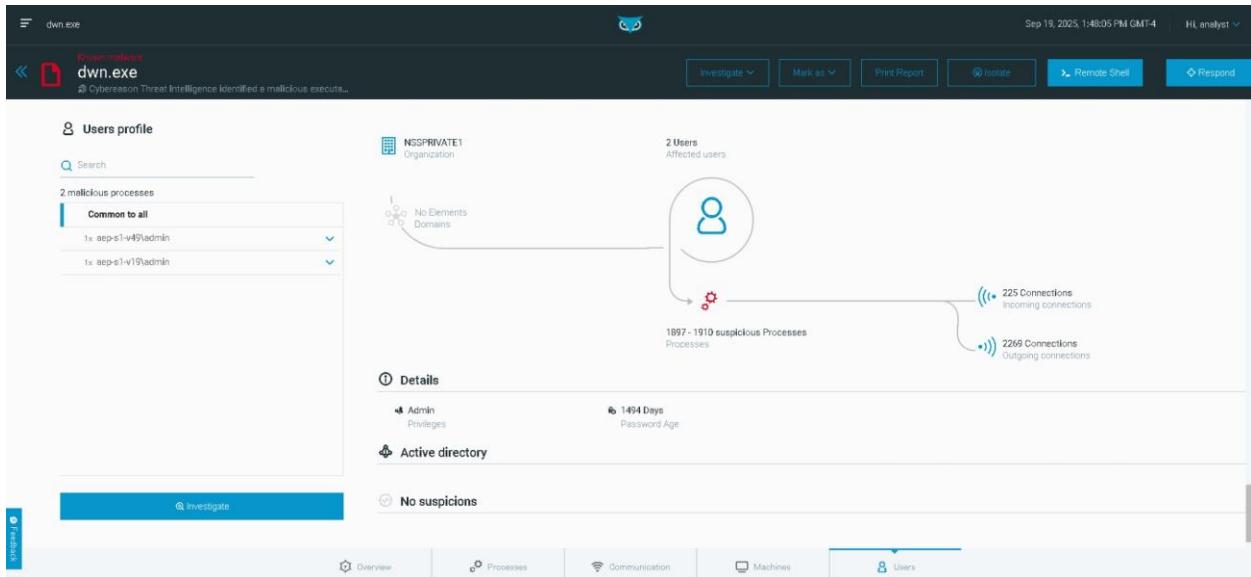
Dashboard of communication profile

D. Machine Profile: Machine profile describes about the machines that are involved and affected in the attack. It contains detailed information like Connections status, Domain controllers, OS, and DNS host name. These all are represented by visual tree representation.



Dashboard of Machine Profile

E. Users Profile: The Users profile shows the information about the users that are involved in the attack and associated with it. It shows detailed information of the Malicious users, user connections (incoming/outgoing), Admin privileges and visual graphical representation.



Dashboard of User profile

Investigation

Investigation tab in Cybereason EDR platform involves in which security analysts can build or use saved queries to detect malicious activity. It provides hunting queries for persistence mechanisms, privilege escalation, lateral movement and data theft.

The screenshot shows the 'Investigation' tab interface. At the top, there's a header bar with the date 'Sep 19, 2025, 11:20:32 AM GMT-4' and a user 'HL analyst'. Below the header is a 'Build a query' section with various icons for filtering: Machine, User, Process, File, Connection, Domain name, Malop process, Mount point, Malop logon session, DNS query unresolved from IP, and a 'See more' button. A search bar for 'My saved queries' is present. Below this is a list of seven saved hunting queries, each with a preview icon, a title, a description, and a timestamp. The queries are:

- Hunting Query: Persistence - Unsigned Services employing aut...
- Hunting Query: Privilege Escalation to System
- Hunting Query: Lateral Movement - Audit object access
- Hunting Query: Data Theft - Injecting process transmitting hig...
- Hunting Query: Persistence - Registry entry pointing to tempor...
- Hunting Query: Execution - Hiding executable by using an alter...
- Hunting Query: Execution - Suspicious files running from Temp...

Dashboard of Investigation tab

It is an interactive query-building screen which contain build a query workflow, connection analysis, timeline-suspicion filters, IP addresses and user-time analysis.

The screenshot shows the 'Build a query' tab interface. At the top, there's a header bar with the date 'Sep 19, 2025, 11:46:32 AM GMT-4' and a user 'HL analyst'. Below the header is a 'Build a query' section with 'Save Query' and 'Clear' buttons. A central diagram shows a 'Process' node connected to a 'Connections' node, which is then connected to a 'Remote address' node. From the 'Remote address' node, several lines extend to icons for 'Connection (Local address)', 'Connection (Remote address)', 'Machine', and 'Related DHCP Interfaces'. There's also a 'See more' button. Below the diagram is a search bar for filters and a button to 'Get results'. The results section shows a table with 30 rows, grouped by 'Element name'. The columns include 'Element name', 'Custom Reputation', 'Used by malware', 'Machine', 'Country name', 'Region', and 'City name'. The first few rows of the table are:

Element name	Custom Reputation	Used by malware	Machine	Country name	Region	City name
> 37.230.112.67	?	Unknown		Russian Federation		
> 162.244.32.39	?	Unknown		United States	CA	Fremont
> 68.227.31.46	?	Unknown		United States	NV	Las Vegas
> 46.243.179.212	?	Unknown		Russian Federation	47	Naro-fominsk
> 78.47.139.102	?	Unknown		Germany		

Dashboard of Build a query

By clicking on any of these element results that are processed by the investigation will show the details of the attack. It will completely elaborate the information like geolocation of the country, country code, IP address, longitude and latitude of the location.

The screenshot shows a detailed investigation report for the IP address 37.230.112.67. The top navigation bar includes tabs for 'Investigation' (selected), 'Logs', 'File', 'Process', 'Network', and 'Custom'. The date 'Sep 19, 2025, 12:00:05 PM GMT-4' and analyst 'H. analyst' are also visible. The main content area is divided into sections: 'Properties' (IP address, Address, Version), 'Geolocation' (Country name: Russian Federation, Country code: RU, Latitude: 55.7386, Longitude: 37.606796), and 'Reputation' (Unknown, Custom Reputation). A sidebar on the right indicates 'No custom reputation set' and 'Platform reputation: ? Unknown (?)'.

Dashboard of Element (machine)

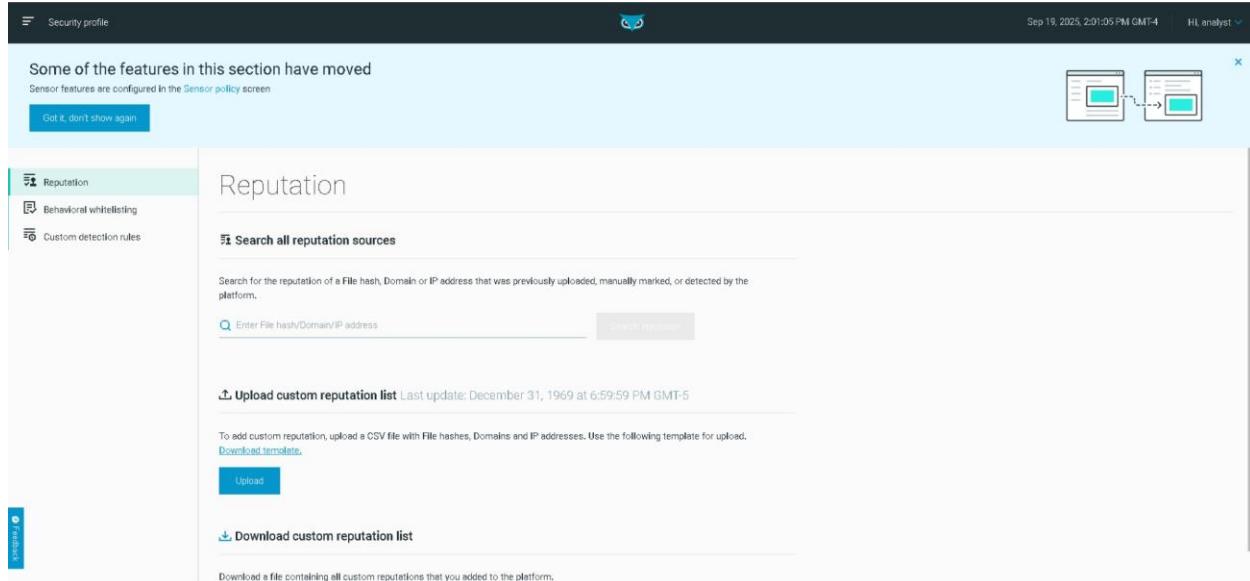
The investigation highlights communication between internal processes and multiple external destinations, some located in regions often associated with heightened cybersecurity risk. While no effective malicious attribution is provided in the current findings, the presence of unknown reputations suggests the need for further enrichment, monitoring, and potential escalation for deeper threat intelligence validation. This ensures that suspicious or high-risk communications are not overlooked. It allows analysts to build queries that trace how internal processes interact with external destinations, enabling the destination that could signal malware activity, command-and-control connections or attempts at data exfiltration.

By mapping communication flows and correlating them with contextual information such as geolocation and usage analysts gain visibility into whether connections are legitimate or potentially harmful. The platform also supports deeper forensic analysis by providing detailed insights into specific external entities, including their properties, origin and reputation status, which helps in assessing risk and correlating findings with threat intelligence feeds. This dual capability of broad mapping and detailed examination enhances proactive threat hunting, incident response, and compliance reporting. It not only enables faster detection of anomalies but also equips teams to make informed decisions on blocking, monitoring, or escalating suspicious activities.

Ultimately its application lies in strengthens an organisations ability to investigate complex security incidents, uncover hidden threats, and maintain resilience against evolving cyberattacks.

SECURITY PROFILE

Security profile section is designed to help analysis manage and analyze the trustworthiness of different digital entities such as file hashes, domains, and IP addresses. At the top, there is a notification banner indicating that some features related to sensors have been moved to a different configuration area that shows various functions like search all reputation sources, upload custom reputation list, and download custom reputation list.



The screenshot shows the 'Security profile' dashboard. At the top, a banner states: 'Some of the features in this section have moved. Sensor features are configured in the [Sensor policy](#) screen.' A 'Got it, don't show again' button is present. The main area is titled 'Reputation'. It includes a 'Search all reputation sources' input field with placeholder text 'Enter File hash/Domain/IP address' and a 'Search' button. Below this is a section for 'Upload custom reputation list' with a note about last update (December 31, 1969) and a 'Download template' link. An 'Upload' button is available. At the bottom, a 'Download custom reputation list' section allows for downloading a CSV file containing all custom reputations. The left sidebar has links for 'Reputation', 'Behavioral whitelisting', and 'Custom detection rules'. The top right corner shows the date 'Sep 19, 2025, 2:01:05 PM GMT-4' and the user 'HL analyst'.

Dashboard of Security Profile

Analyst can input a file hash, domain, or IP address to check its reputation within the platform. This helps in quickly identifying whether an entity has been flagged as safe, suspicious, or automated detections. Analysts can report a file containing all custom reputations that have been uploaded to the platform, making it easier to share, review, or migrate reputation data.

Download custom reputation list enables analysts to export a file containing all custom reputations that have been uploaded to the platforms, making it easier to share, review, or migrate reputation data.

1. Add details of 3 investigation added in malop inbox.

These are 3 investigations that are visualized in malop inbox. In these 3 Logs contain two executable files which contain malware activities and one command & control activity.

The screenshot shows the Malop inbox interface with three investigations listed:

Type	Root cause	Affected machines	Detected activity	Labels	Created	Last activity	Status
Older (675)	luck.exe Known malware	2 machines	Infection		November 27, 2018 at 9:32:15 AM GMT-5	7 years ago	
	1.exe Known malware	AEP-S1-V19	Infection		November 27, 2018 at 9:32:04 AM GMT-5	7 years ago	
	13.68.93.109 Command and Control	CYBERNIVYLAP	C&C		September 6, 2018 at 3:20:44 AM GMT-4	7 years ago	

1.1 The first investigation luck.exe is identified as malicious executable file which affected the systems and admin users to achieve privilege escalation.

The screenshot shows the detailed view of the luck.exe investigation:

Description: The image file hash of the process, luck.exe was identified by hash as malware. Status: Unread. Priority: High. First detected: 7 years ago.

Root cause info: luck.exe Cybersecurity Threat Intelligence identified a malicious executable. Unknown Company name. Unknown Product name. Malware Reputation type. Scope: 2 Machines - AEP-S1-V71, AEP-S1-V49. Communication: No communication.

Timeline: Malop started, Malop detected, Cybereason threat intelligence identified a malicious executable Go to processes. Timeline shows events from May 12, 2018, to Nov 27, 2018.

Affected machines: 2 Machines (AEP-S1-V71, AEP-S1-V49). **Affected users:** 2 Users (aep-s1-v49\admin, aep-s1-v71\admin).

Diagram: A circular diagram showing the infection process. It starts with "luck.exe Cybersecurity Threat Intelligence identified a malicious executable root cause". This leads to "2 suspicious Processes Malicious process". From there, it branches into "Infection" (with "No Connections Incoming connections" and "No Connections Outgoing connections") and "Malop detected".

Detected Activity- Malware infection

Affected Machines – AEP-S1-V71, AEP-S1-V49

Affected Users – aep-s1-v49\admin, aep-s1-v71\admin

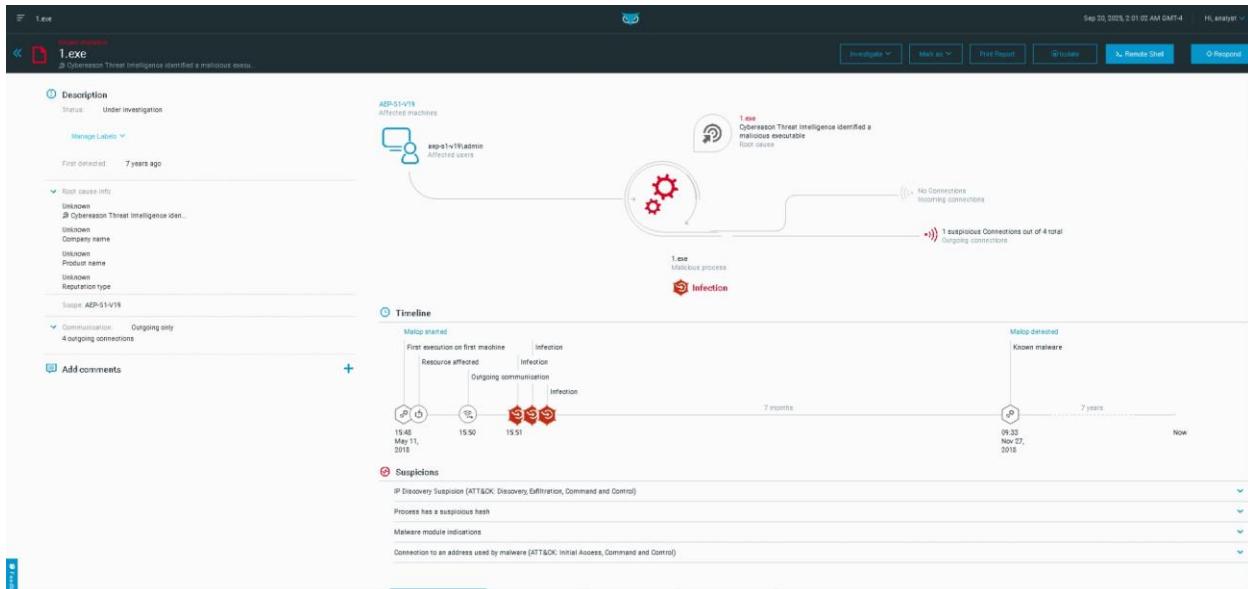
Parent Process – luck.exe

Child Processes - winspool.drv, VERSION.dll

Privileges- Admin level

Date and Time – May 12, 2018, at 9:32:07 AM GMT-4

1.2 The second investigation is malicious executable file 1.exe which is classified into Initial access and Command & control attack with help of MITRE ATT&CK framework.



Detected Activity – Malware Infection

Affected Machine – AEP-S1-V19

Affected users – aep-s1-v19\admin

Parent Process – cmd.exe

Suspicious Modules – AUTHZ.dll{floating}, SETUPAPI.dll{floating}, Securit.dll(floating)

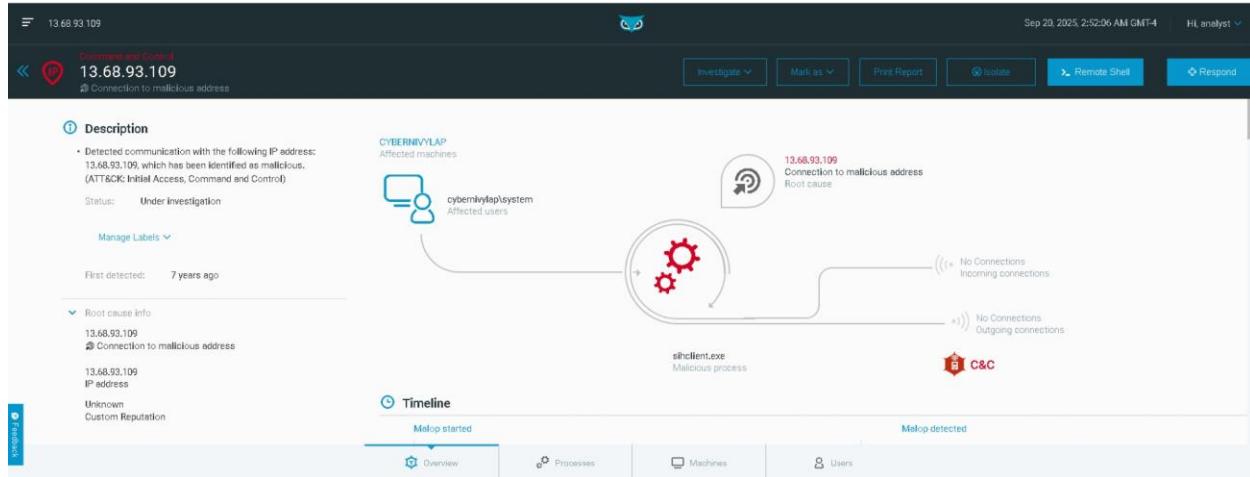
Privileges – Admin

Date and Time – May 12 ,2018 At 11:59:37 AM GMT-4

MITRE ATT&CK – Initial access and Command & Control

1.3 The third investigation is Command and Control stage log which showed the remote connection to unknown address and gained remote access to the owner machine by executing the commands. Detected the communication with the following Ip address 13.68.93.109 and 108.177.15.108 which has been identified as malicious. (MITRE ATT&K – Initial Access, Command and Control connection, Exfiltration)

An unresolved DNS query sls.update.microsoft.com {communication error} is detected which is used to establish the connection and made an error while connection to malicious address. By analysing the whole attack, we found that location of remote address was united states which they used ports like SMTP and HTTP.



Detection Activity – Remote Access (Initial access, Command and Control)

Machine effected – CYBERNIVYLAP

Malicious Process – svhost.exe, sihclient.exe, minidump.exe,

Affected User- cybernivylap\system

MITRE ATT&CK – Initial Accesses, Command and Control, Exfiltration

Remote Addresses – 13.68.93.109 and 108.177.15.108

Location of remote address – United states

Data Transferred – 9kB and 1367 bytes

Date and Time of start – August 28, 2018 at 3:58:29 AM GMT-4

Date and Time of End – September 6, 2018 at 4:32:59 AM GMT-4

2. Create a detailed report on detected alert as per lateral movement, C&C and Detected ransomware program

2.1 Lateral Movement – reverse_shell_exe_10.35.16.171_shikata.exe the image file of the process is identified by the hash tool that can facilitate malicious activity.

The screenshot displays a threat intelligence dashboard for a known malware entry. At the top, it shows the file name: reverse_shell_exe_10.35.16.171_shikata.exe. The status is "Under investigation". The first detection was 7 years ago. The scope is WIN-8U2A8SVQJDQ, and communication is listed as "No communication". Below this, there's a "Description" section with a note about the malware being identified as a malicious tool. A central diagram illustrates lateral movement from one machine to another. It shows two nodes: "WIN-8U2A8SVQJDQ Affected machines" and "win-8u2a8svqjdq\gamer111 Affected users". An arrow points from the machine node to the user node, labeled "Lateral movement". A circular icon with two red gears is positioned between them. To the right, a box for the user node contains the text: "reverse_shell_exe_10.35.16.171_shikata.exe Cyberreason Threat Intelligence identified a malicious tool Root cause". Below the diagram, a timeline shows the progression of the malware: "Malop started" (First execution on first machine), "Resource affected", "Lateral movement", and "Malop detected" (Known malware). There are also sections for "Add comments" and "Timeline".

Detected Activity – Lateral Movement

Affected Machine - –WIN-8U2A8SVQJDQ

Affected User – win-8u2a8svqjdq\gamer111

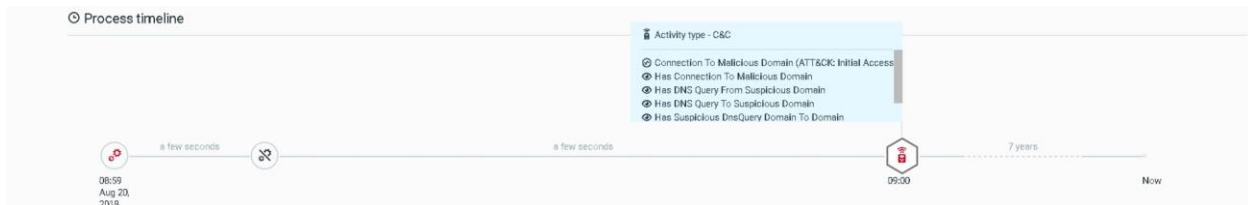
Parent Process – svhost.exe

Malicious Process - reverse_shell_exe_10.35.16.171_shikata.exe

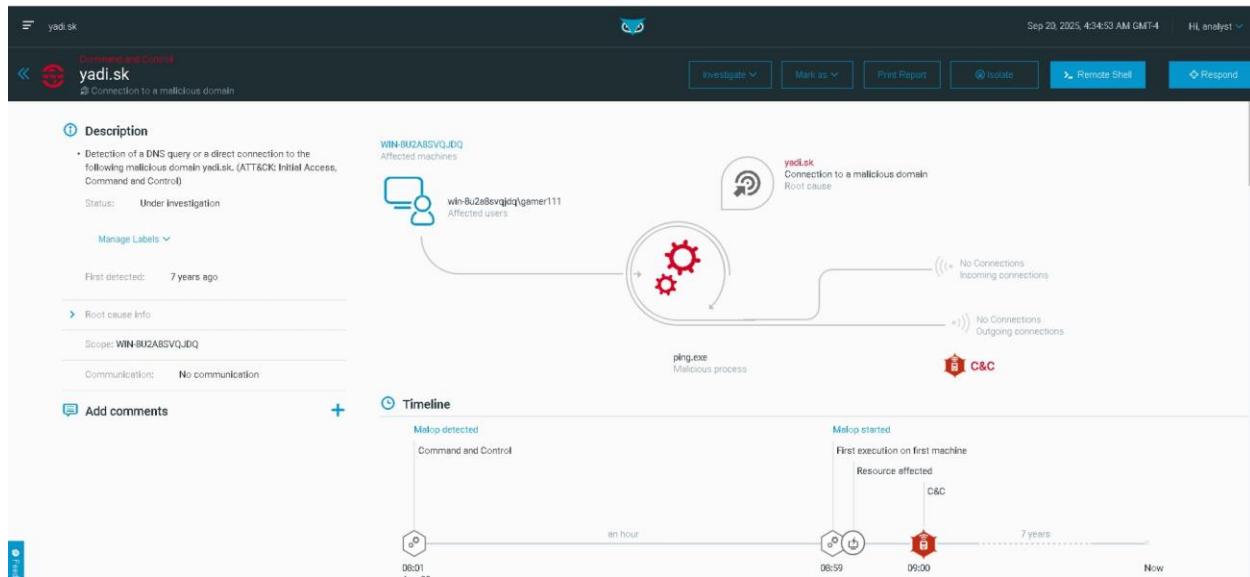
Connection – 192.168.203.129:62709 to 5.196.73.76:80

Date and time – September 5, 2018, 03:30 AM GMT-4

2.2 Command and Control – yadi.sk is a malicious domain that is used to establish a connection in command line with the help of ping.exe malicious process.



This process timeline shows the attack timeline of the command-and-control activity. As of redirecting the session to the malicious domain they executed ping.exe to load the domain.



Detection Activity – Command and Control

Affected Machine – WIN-8U2A8SVQJDQ

Affected User - win-8u2a8svqjdq\gamer111

Parent Process – cmd.exe

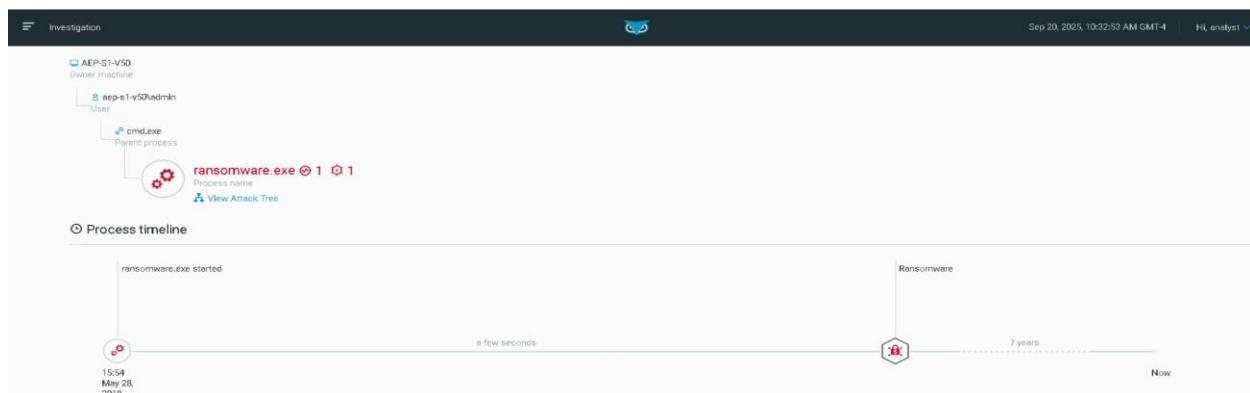
Malicious Process – ping.exe

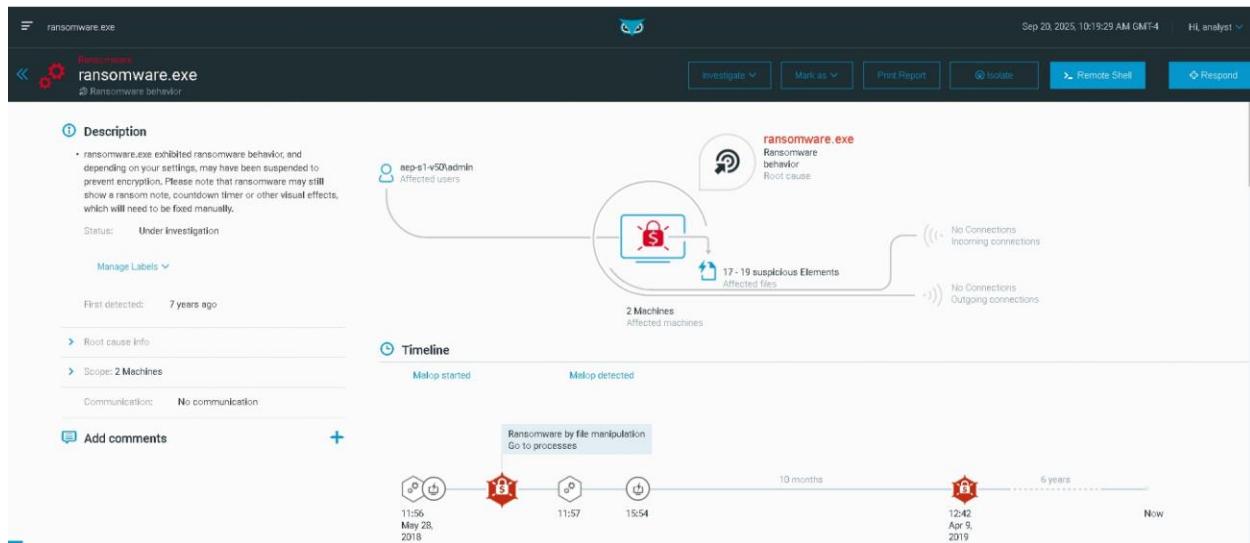
Malicious Domain – yadi.sk

Command line – ping yadi.sk

Date and time – Start = August 20, 2018, 08:59:45 AM GMT-4; End = 08:59:48 AM GMT-4

2.3 Detected Ransomware Program – ransomware.exe is an executable program which showed ransomware behavior that is used to encrypt the data in 2 systems and blocked to avoid encryption of the data.





Detected Activity – Ransomware Program

Affected Machines – AEP-S1-V50 and AEP-S1-V72

Affected Users – aep-s1-v50\admin and aep-s1-v72\admin

Parent process – cmd.exe

Malicious process – ransomware.exe

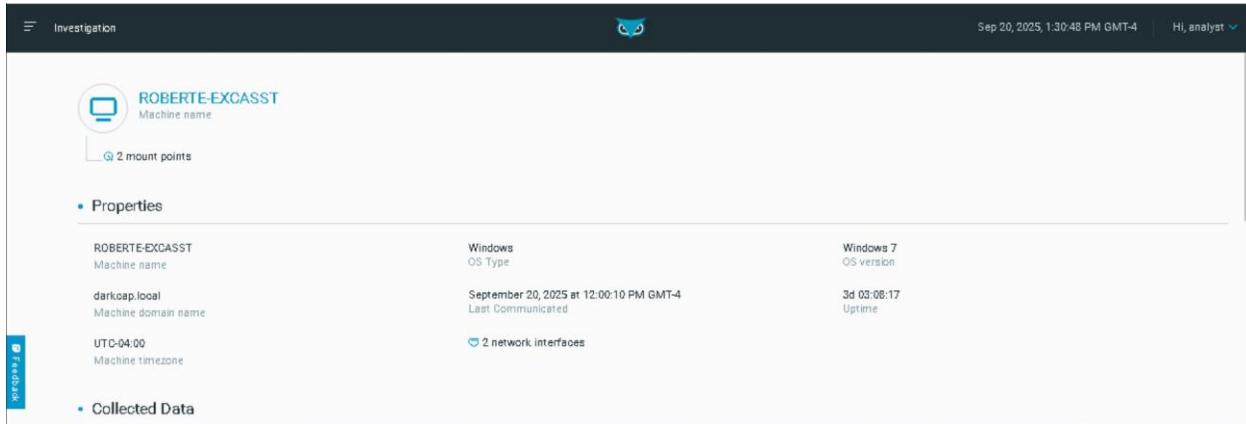
Command line – c:\users\admin\Desktop\ransomware.exe

Privileges – Admin level

Date and time – May 28 2018, 11:56:54 AM GMT-4

3. In Malop box write a detailed report on alert detected in Robert-excasst system.

The machine ROBERTE-EXCASST is an active endpoint running windows 7 within the darkcup.local domain. It is currently connected to the Cybereason platform, not isolated, and last communication very recently.



The screenshot shows the Cybereason investigation interface for the machine ROBERTE-EXCASST. The top navigation bar includes 'Investigation' and a user icon 'Hi, analyst'. The date and time 'Sep 20, 2025, 1:30:48 PM GMT-4' are also displayed. The main panel displays the machine's name 'ROBERTE-EXCASST' and its machine name 'darkcap.local'. It shows '2 mount points' and '2 network interfaces'. The 'Properties' section provides detailed information: OS Type (Windows 7), OS Version (Windows 7), Last Communicated (September 20, 2025 at 12:00:10 PM GMT-4), and Uptime (3d 03:08:17). The 'Machine' section lists the machine's domain name (darkcap.local), machine name (ROBERTE-EXCASST), and machine timezone (UTC-04:00). A sidebar on the left shows a 'Feedback' button.

Machine Name – ROBERTE EXCASST

Machine Domian Name - darkcap.local

Suspicious process - cmd.exe, chrome.exe, svhost.exe, logonui.exe, taskhost.exe

Last communicated - September 20, 2025, at 12:00 PM GMT-4

Remote Address – 172.217.165.202

No. Of Users – 8

Privileges – Admin

MITRE ATT&CK – Lateral movement, Command and Control,

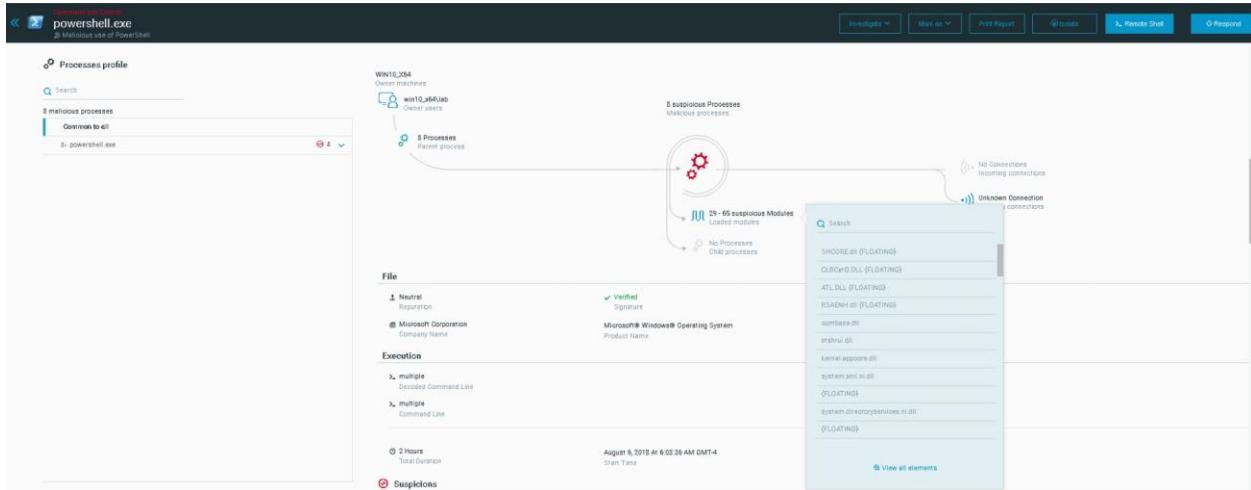
Drivers and Registries – 155 drivers and 5561 entries

This information shows that the Roberte Excassst system was affected by various malicious process and also had several remote connections that indicates the involvement of the unauthorised entry to the system network. Several executable files are analysed and alerted the execution of the files to run commands on the powershell and command line prompt to achieve lateral movemnet within the network.

In conclusion the Roberte excasst machine is affected by Lateral movement, Command and Control attack and remote connections to remote adresses.

4. Add details of any 5 modules based on PowerShell attack on machines/process.

There are several modules that are found on power shell attack. These modules play a specific task at each stage of the attack to achieve the motive of the attacks.



4.1 SHCORE.dll{floating}

Module Name: SHCORE.dll{floating}

Module Size: 733184 bytes

Machine name: WIN10_X64

Status: Floating module (not permanently mapped in process memory).

Evidence: This DLL was never loaded in standard loader database. It indicates suspicious behavior because legitimate DLLs are loaded by system loader.

4.2 CLBCatQ.DLL {FLOATING}

Module Name: CLBCatQ.DLL {FLOATING}

Module Size: 675840 bytes

Machine name: WIN10_X64

Function: Attackers may inject into it or replace it to execute code stealthy.

Status: Floating module (not permanently mapped in process memory)

Evidence: This DLL was never loaded in standard loader database. It indicates suspicious behavior because legitimate DLLs are loaded by system loader.

4.3 system.xml.dll

Module Name: system.xml.dll

Module size: 1.38 MB

Machine Name: WIN10_X64

Registry entry: False registry entry

Function: Commonly used by the attackers to avoid detection of the malware.

Evidence: Mimics System.xml.dll, a core .NET assembly to avoid suspicion and act as dropper for ransomware, spyware and remote access.

4.4 CRYPTBASE.dll

Module name: CRYPTBASE.dll

Machine name: WIN10_x64

Module size: 45056 Bytes

Regisrty entry: False Registry entry

Function: It is legitimate windows system file associated with cryptographic services.

Status: Floating module (unmapped or detached form the disk)

Evidence: This module is never loaded in standard loader database which indicates DLL injection, relocating and tampering.

4.5 Powershell.exe

Module name: Powershell.exe

Machine name: WIN10_X64

Module size: 469.00 KB

Registry entry: False Registry entry

File Path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Function: It can execute scripts, download payloads and manipulate system settings

Status: Running malicious scripts without dropping new files

Evidence: This module was never loaded in standard loader database which shows suspicious malicious activity.

5. Investigation option in the side bar - user & process option and add any 3 system details.

The screenshot shows the 'Investigation' panel with the following interface elements:

- Build a query**: Buttons for 'Save Query' and 'Clear'.
- Timeline**: Options for 'All data', 'Today', 'Last week', 'Last month', and 'Custom'.
- Suspicious**: A section indicating 'No events for selected element type'.
- User & Process Tree**: A diagram showing relationships between 'User (414)', 'Processes (80,769)', and 'Owner machine (166)'. Lines connect 'User' to 'Processes' and 'Processes' to 'Owner machine'. From 'Owner machine', three lines branch out to 'Users', 'Logon sessions', and 'Processes'.
- Search Bar**: 'Search for filters' with the query 'All machines, which are owner machines of any process, which are Processes of any user'.
- Buttons**: 'Filters' and 'Get results'.
- Feedback**: A small blue feedback icon.

Investigation panel is used to build a query to retrieve the data of the selected logs and make it easier to read the logs. Here are some systems that are shown in dteailed using user and process tree.

5.1 CYBERNOAPLAP

The screenshot shows the properties of the user 'CYBERNOAPLAP' with the following details:

Property	Value	Description
Domain\User Name	cyberdomain\noa.pinkas	User name
Domain	cyberdomain	User
Local system	False	Privileges
Organization	DETECTIONTEAM	Comment
Security identifier (SID)	S-1-5-21-883495937-1710221880-2480596416-4...	
Password age in days	65	
Is admin	False	

System name: CYBERNOAPLAP

Organization: DETECTION TEAM

User domain\Username: cyberdomain\noa.pinkas

Privileges: User

Processes: 439 processes and 4 Suspicious processes

Detected activity: Malware (powershe.exe)

5.2 ROBERTE-EXCASST SYSTEM

The screenshot shows the 'Investigation' interface for the 'ROBERTE-EXCASST' system. On the left, a sidebar lists 'Common to all' users: roberte-excasst\administrator, roberte-excasst\system, roberte-excasst\msgqsvr@darkcap.local, roberte-excasst\localsystem, darkcap\roberte-excasst\$, roberte-excasst\local service, darkcap\roberte, and roberte-excasst\network service. The main panel displays the 'ROBERTE-EXCASST' machine properties. It shows 8 users under the 'Domain\User Name' section. The properties table includes columns for User Name, Privileges, and Comment. Key entries include:

User Name	Privileges	Comment
roberte-excasst\administrator	Administrator	S-1-5-21-1630689363-2457423621-36887703...
roberte-excasst\system	System	S-1-5-18
roberte-excasst\msgqsvr@darkcap.local	msgqsvr@darkcap.local	S-1-5-19
Show 5 more ▾	Show 5 more ▾	Show 2 more ▾
Domain\User Name	User name	Security identifier (SID)
roberte-excasst	Admin	2472
darkcap	Privileges	Password age in days
Domain		
Local system	True	Built-in account for administering the comp...
False	7	Comment
	is admin	

Machine name: ROBERTE-EXCASST

Organisation: CRTRAINING

Domain\Username: roberte-excasst\administrator, roberte-excasst\system, roberte-excasst\ msgqsvr@darkcap.local, roberte-excasst\localsystem, roberte-excasst\localservice, roberte-excasst\network service, darkcap\roberte-excasst and darkcap\roberte.

Privileges: Admin

Processes: 738 processes

5.3 DESKTOP-L9F5T49

The screenshot shows the 'Investigation' interface for the 'DESKTOP-L9F5T49' system. On the left, a sidebar lists 'Common to all' users: desktop-l9f5t49\gamer111, desktop-l9f5t49\gamer111, desktop-l9f5t49, and DETECTIONTEAM. The main panel displays the 'DESKTOP-L9F5T49' machine properties. It shows 1 user under the 'Domain\User Name' section. The properties table includes columns for User Name, Privileges, and Comment. Key entries include:

User Name	Privileges	Comment
desktop-l9f5t49\gamer111	gamer111	S-1-5-21-2593778471-1471935282-21924008...
Domain\User Name	User name	Security identifier (SID)
desktop-l9f5t49	Admin	72
Domain	Privileges	Password age in days
False	True	Comment
Local system	is admin	
DETECTIONTEAM		
Organization		

Machine name: DESKTOP-L9F5T49

Organisation: DETECTION TEAM

Domain\Username: desktop-l9f5t49\gamer111

Privileges: Admin

Processes: 7 processes and 2 suspicious processes

Detected activity: Malware (shinobot.exe)

6. Find evidence points details of any 2 PowerShell based attack.

6.1 Evidence of PowerShell attack (1)

The screenshot shows a digital forensic investigation interface. At the top, it displays the machine name (DESKTOP-L9F5T49), organization (DETECTION TEAM), domain\username (desktop-l9f5t49\gamer111), and privileges (Admin). The date and time are Sep 21, 2025, 7:41:11 AM GMT-4, and the user is Hi, analyst. On the left, there's a sidebar with 'Investigation' and 'Feedback' buttons. The main area is titled 'Common to all' and lists three items: 'powershell.exe' (2), 'powershell.exe' (1), and 'powershell.exe' (1). To the right, under the heading 'Evidence (7)', are seven detailed evidence points, each with a dropdown arrow:

- Malicious PowerShell framework
- Has Low TTL DNS Query
- PowerShell executed by word process (ATT&CK: Defense Evasion, Execution - Scripting)
- PowerShell downloader
- Has External Connection To Well Known Port
- Unsigned with a signed version module
- Contains a module not found in loader db

Each item listed under Evidence points to suspicious or malicious behavior associated with powershell.

- 1. Malicious powershell framework:** Suggest use of a known offensive framework like Empire, Powersploit, or Nishang. These are often used for post-exploitation.
- 2. Has Low TTL DNS Query:** Indicates potential DNS tunneling or command and Control(C2) communication. Low TTL values are often used to avoid caching and maintain real-time control.
- 3. PowerShell executed by word process
 (ATT&CK DEFENSE Evasion, Execution scripting):** A word document triggering PowerShell is a classic sign of macro-based malware or phishing. This maps to MITRE ATT&CK techniques for evasion and script-based execution.
- 4. PowerShell downloader:** A script used to fetch and execute payloads from external sources often the first stage in malware delivery.

5. **Has External Connection to Well Known Port:** Indicates out band traffic to a known port (e.g., 443 for HTTPS), possibly for C2 for data exfiltration.
6. **Unsigned with a signed version module:** Suggests tampering or replacement of legitimate modules with unsigned ones used to bypass trust mechanisms.
7. **Contains a module not found in loader bin:** Implies the presence of unauthorised or injected modules, possibly used for stealth or persistence.

6.2 Evidence of PowerShell attack (2)

The screenshot shows a digital forensic interface with a dark header bar. On the left is a navigation menu icon, followed by the word "Investigation". In the center is a small blue owl logo. To the right are the date and time "Sep 21, 2025, 7:46:55 AM GMT-4" and a greeting "Hi, analyst". Below the header, there's a section titled "Evidence (4)" with four items listed:

- suspicious powershell commands were identified
- PowerShell executed by word process (ATT&CK: Defense Evasion, Execution - Scripting)
- PowerShell downloader
- Unsigned with a signed version module

1. **Suspicious PowerShell commands were identified:** Indicates detection of potentially malicious or obfuscated PowerShell commands. These may include encoded payloads, privilege escalation attempts, or lateral movements scripts.
2. **PowerShell executed by word process (ATT&CK Defense Evasion, Execution- scripting):** A non- standard process (wvcd) initiated PowerShell, suggesting process hollowing, masquerading, or indirect execution.
3. **PowerShell Downloader:** Script used PowerShell to fetch remote content typically malware or additional payloads. This is a common initial access or staging technique.
4. **unsigned with a Signed Version Module:** Indicates module swapping or DL

7. Find 3 suspicious DLL process details of any 2-ransomware alert.

7.1 CRYPT32.dll {FLOATING}

The screenshot shows a digital forensic interface with a dark header bar. On the left, there's a navigation menu with 'Investigation' selected. In the center, there's a search bar with a magnifying glass icon and the text 'CRYPT32.dll {FLO...}'. Below the search bar, it says 'Module name'. To the right of the search bar, the date and time are listed as 'Sep 21, 2025, 8:52:32 AM GMT-4' and 'Hi, analyst'. A blue owl icon is in the top right corner.

Evidence (1)

Is never in loader DB

Properties

CRYPT32.dll {FLOATING}	1966604288	1167360
Module name	Address (in Decimal)	Size Of Image

Characteristics

Module name: CRYPT32.dll {FLOATING}

Status: Floating (not loaded from standard location or not verified against known baseline.)

Evidence: This version of CRYPT32.DLL has never been seen before in the loader database, Suggests the module may be unauthorised or injected manually and obfuscated attack.

Date and Time: September 21, 2015, 8:53:21 AM GMT +4

7.2 PSAPI.DLL{FLOATING}

The screenshot shows a digital forensic interface with a dark header bar. On the left, there's a navigation menu with 'Investigation' selected. In the center, there's a search bar with a magnifying glass icon and the text 'PSAPI.DLL {FLOATI...}'. Below the search bar, it says 'Module name'. To the right of the search bar, the date and time are listed as 'Sep 21, 2025, 9:08:40 AM GMT-4' and 'Hi, analyst'. A blue owl icon is in the top right corner.

Evidence (1)

Is never in loader DB

Properties

PSAPI.DLL {FLOATING}	2000027648	20480
Module name	Address (in Decimal)	Size Of Image

Module name: PSAPI.DLL {FLOATING}

Status: Floating {status may imply its loaded in memory without proper registration or linkage}

Evidence: Not found in loader database which may indicate non-standard DLL injection or obfuscated malicious payload.

Date and Time: September 21, 2015, 08:08:40 AM (GMT +4)

7.3 VERSION.dll {FLOATING}

The screenshot shows a digital forensic investigation interface. At the top, it says "Investigation" and "Sep 21, 2025, 9:36:12 AM GMT-4 | Hi, analyst". On the left, there's a sidebar with "AEP-S1-V50 Machine" and a "Feedback" button. The main area shows a tree view with "VERSION.dll {FLO... Module name" under "Machine". Below the tree, there's a section titled "Evidence (1)" with the note "Is never in loader DB". A "Properties" section shows details: "VERSION.dll {FLOATING} Module name", "1952972800 Address (in Decimal)", and "36864 Size Of Image".

Module name: VERSION.dll {FLOATING}

Status: Floating (This DLL is not loaded through standard mechanisms)

Evidence: This module is not listed in the loader database, it may have been injected manually (e.g., via reflective DLL injection or process hollowing).

Date and Time: May 29, 2018, at 4:06:56 AM GMT-4

8. Find the 2 effected users name of phishing attack/any malware attack.

8.1 Affected user of malware attack

The screenshot shows a threat intelligence interface. At the top, it says "Known malware" and "3 modules". The main area displays a user profile for "cyberdomain\matan". On the left, there's a sidebar with a search bar and a list of "1 malicious processes" under "Common to all", which includes "powershell.exe", "excel.exe", and "cmd.exe". On the right, there's a summary of network activity: "121 suspicious Processes out of 10..." and connection statistics: "No Connections Incoming connections" and "1979 Connections Outgoing connections". Below the sidebar, there's a "Details" section showing "Non-Admin Privileges" and "42 Days Password Age". A large blue "Investigate" button is at the bottom left.

Username: matan (cyberdomain\matan)

Processes: powershell.exe, excel.exe and cmd.exe

Activity: Malware attack

8.2 Affected user of phishing attack.

The screenshot shows a threat intelligence interface. At the top, it says "Phishing" and "3 processes". The main area displays a user profile for "aep-s1-v111\admin". On the left, there's a sidebar with a search bar and a list of "37 malicious processes" under "Common to all", which includes "powershell.exe", "cmd.exe", and "excel.exe". On the right, there's a summary of network activity: "3 - 2869 suspicious Processes" and connection statistics: "15 Connections Incoming connections" and "6640 Connections Outgoing connections". Below the sidebar, there's a "Details" section showing "Non-Admin Privileges" and "42 Days Password Age". A large blue "Investigate" button is at the bottom left.

Username: admin(aep-s1-v111\admin)

Processes: cmd.exe and powershell.exe

Activity: Phishing attack

9. Find out 5 outgoing connections IP address based on any 2-malware alert.

The screenshot shows a network investigation interface. On the left, a 'Build a query' section has 'Connection (8,860)' selected, with arrows pointing to 'Local address', 'Remote address', 'Owner machine', and 'Owner process'. Below this is a search bar and a 'Get results' button. To the right is a timeline from Sep 21, 2025, at 2:21:48 PM GMT-4, with filters for 'All data', 'Today', 'Last week', 'Last month', and 'Custom'. The main area displays a table of 1K out of 8.9K results, grouped by element name. The columns include: Element name, Direction, Server address, Server port, Port type, Received bytes, Transmitted by..., Remote address..., Address Access..., Owner machine, and Owner process. The table lists five connections:

Element name	Direction	Server address	Server port	Port type	Received bytes	Transmitted by...	Remote address...	Address Access...	Owner machine	Owner process
> 10.146.17.48:49746 > 23.215.9.1	Outgoing	23.215.99.40	80	HTTP	0 B	0 B	United States	AEP-S1-V2B	bvs.exe	
> 10.146.17.69:49689 > 12.162.8.1	Outgoing	12.162.84.2	443	HTTP	0 B	0 B	United States	AEP-S1-V49	initiatorwarm...	
> 10.146.17.92:49695 > 23.215.99.25	Outgoing	23.215.99.25	80	HTTP	0 B	0 B	United States	AEP-S1-V72	ttnvo.exe	
> 10.146.17.40:49675 > 220.227.247.35	Outgoing	220.227.247.35	4143	Service	0 B	0 B	India	AEP-S1-V20	initiatorwarm...	
> 10.146.17.70:49731 > 12.162.84.2	Outgoing	12.162.84.2	443	HTTP	0 B	0 B	United States	AEP-S1-V50	initiatorwarm...	

1. Connection – 10.146.17.48:49746 > 23.215.99.40:80
2. Connection - 10.146.17.69:49689 > 12.162.84.2:443
3. Connection – 10.146.17.92:49695 > 23.215.99.25:80
4. Connection – 10.146.17.40:49675 > 220.227.247.35:4143
5. Connection – 10.146.17.70:49731 > 12.162.84.2:443

10. Create a full list of number of all alerts in C&C category.

The screenshot shows a malware inbox interface. On the left, there are filters for 'Type' (e.g., IP, Domain, File, Process), 'Root cause' (e.g., Command and Control, Malicious file, Process injection), and 'Labels' (High, Medium, Low). The main area displays a table of alerts, grouped by Type. The columns include: Type, Root cause, Affected machines, Detected activity, Labels, Created, Last activity, and Status. The table lists several C&C alerts:

Type	Root cause	Affected machines	Detected activity	Labels	Created	Last activity	Status
IP (214)	13.68.93.109 Command and Control Connection to malicious address	CYBERNIVYLAP	C&C		September 6, 2018 at 2:20:44 AM GMT-4	7 years ago	
IP	6 IP addresses Command and Control Connection to malicious address	DESKTOP-L4P0IBI	C&C		August 21, 2018 at 2:54:30 AM GMT-4	7 years ago	
IP	6 IP addresses Command and Control Connection to malicious address	WIN-BU2ABSVQJDD	C&C Infection		August 21, 2018 at 2:54:09 AM GMT-4	7 years ago	
Domain	yadi.sk Command and Control Connection to a malicious domain	WIN-BU2ABSVQJDD	C&C		August 20, 2018 at 2:01:30 AM GMT-4	7 years ago	
File	ldlixerofr.exe Command and Control Accessing address used by malware	AEP-S1-V2B	C&C		June 4, 2018 at 7:25:56 AM GMT-4	7 years ago	
File	8 processes Process injection Malicious Code Injection	AEP-S1-V29	C&C Infection		June 4, 2018 at 9:07:31 AM GMT-4	7 years ago	

1. 13.68.93.109 - Connection to malicious domain.
2. itldxerofr.exe - Accessing address used by malware.
3. 204.95.99.109 - Connection to malicious address and domain.
4. tttvc.exe - Accessing address used by malware.
5. 67.176.238.209 - connected to malicious address and has been identified as C&C activity.
6. bvs.exe - Accessing address used by malware.
7. xuzflja2bm.exe - It has an unknown reputation and connecting to the address that is used by malware. (ATT&CK: Initial Access, Command and Control).

11. Create a list of number of alerts in privilege access stage category.

The screenshot shows a list of security alerts from a platform. The title bar indicates the date as Sep 21, 2025, at 3:24:14 PM GMT-4, and the user as Hi, analyst. The main area is titled 'Privilege escalation' and contains a table of alerts. The columns are: Type, Root cause, Affected machines, Detected activity, Labels, Created, Last activity, and Status. There are 112 alerts listed under the 'Older' filter. The first alert is for 'lazagne_x64.exe' which is identified as 'Known malware'. Other alerts involve 'Process injection' and 'Malicious Code Injection' on various machines like WIN7_X64, AEP-S1-V2B, and AEP-S1-V29. Most alerts are categorized as 'Privilege escalation' and 'Infection'. The 'Created' column shows dates ranging from August 29, 2018, to May 30, 2019. The 'Last activity' and 'Status' columns show '7 years ago' for all entries. On the left sidebar, there are filters for 'Mark as ...', 'All active (664)', 'All archived (0)', 'Labels', and 'High (0)', 'Medium (0)', 'Low (0)'. The 'Labels' section is currently selected.

Type	Root cause	Affected machines	Detected activity	Labels	Created	Last activity	Status
lazagne_x64.exe	Known malware Cybersecurity Threat Intelligence identified a malicious executable	WIN7_X64	Privilege escalation Infection		August 29, 2018 at 8:53:00 PM GMT-4	7 years ago	
2 processes	Process injection Malicious Code Injection	AEP-S1-V2B	Privilege escalation C&C Infection		June 3, 2018 at 8:21:06 PM GMT-4	7 years ago	
2 processes	Process injection Malicious Code Injection	AEP-S1-V2B	Privilege escalation C&C Infection		June 3, 2018 at 7:59:59 PM GMT-4	7 years ago	
2 processes	Process injection Malicious Code Injection	AEP-S1-V2B	Privilege escalation C&C Infection		May 30, 2019 at 7:20:52 AM GMT-4	7 years ago	
2 processes	Process injection Malicious Code Injection	AEP-S1-V2B	Privilege escalation C&C Infection		May 30, 2019 at 7:19:41 AM GMT-4	7 years ago	
2 processes	Process injection Malicious Code Injection	AEP-S1-V2B	Privilege escalation Infection		May 30, 2019 at 7:58:02 AM GMT-4	7 years ago	
2 processes	Process injection	AEP-S1-V2B	Privilege escalation C&C		May 30, 2019 at 7:11:10 AM	7 years ago	

1. lazagane_x64.exe - The process has a module that was identified malicious software address.
2. server.exe - The process has identified as malicious executable. (ATT&CK; privilege escalation).
3. default.exe - It exhibited ransomware behavior, and depending upon settings, may have been suspended to prevent encryption. (ATT&CK; privilege escalation).
4. explorer.exe - Process has loaded a meterpreter agent.