cynet

Solution Brief

Cynet 360 AutoXDR™

Cybersecurity made easy

Intro

Security stacks are costly and complex – leaving lean security teams overwhelmed and struggling to manage operations. Meanwhile, number of common and advanced threats are increasing. These security teams must resort to using numerous technologies to prevent breaches.

As a result, security teams face the following challenges:

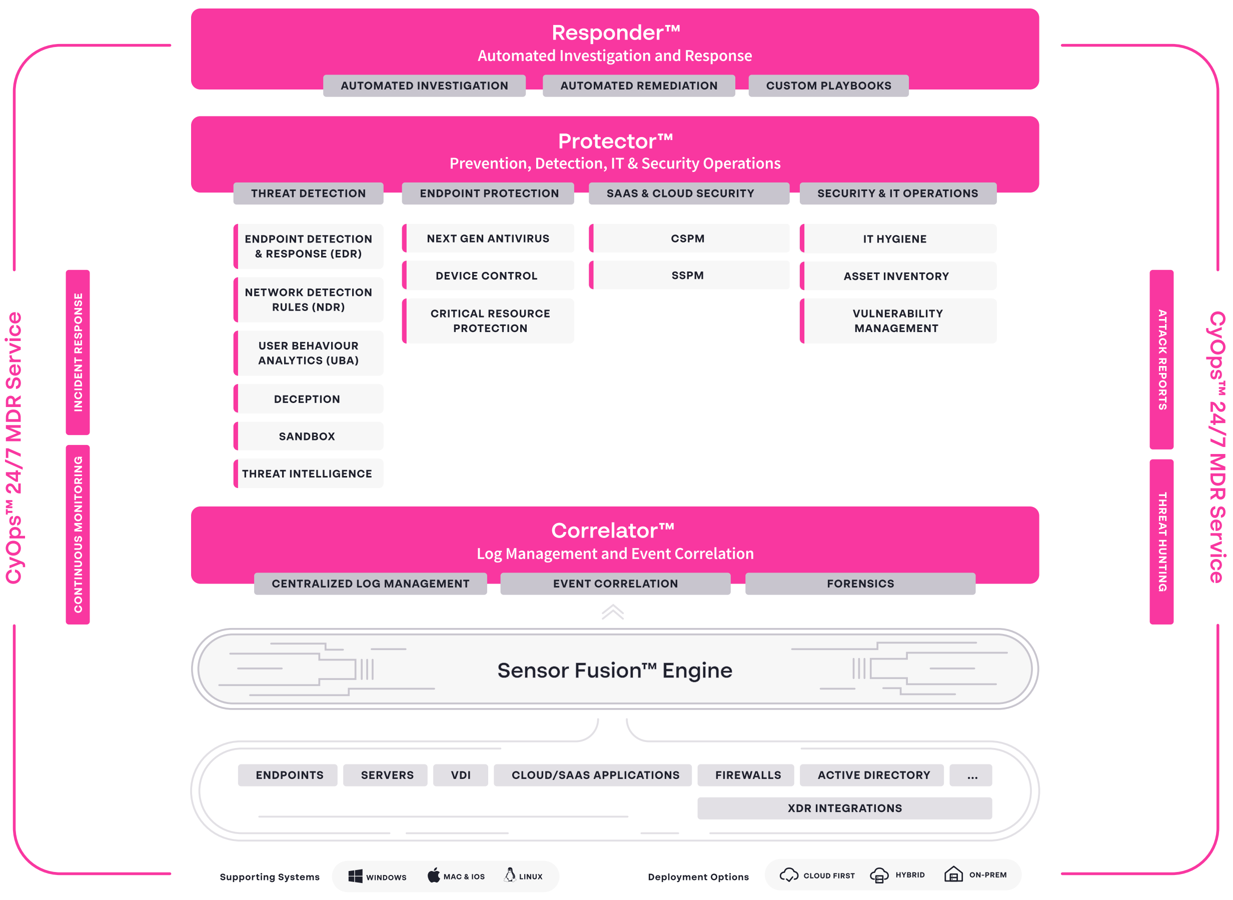
- Complex deployment: piecing together disparate products that were not designed to work together.
- Inefficient and ineffective security stack: disparate technologies results both in overlaps and blind spots.
- Manual workflows: post - compromise breach protection technologies require manual operation that, by definition, cannot scale to the volume of generated alerts.
- Dedicated skill sets: there's a shortage of the skill sets required to efficiently operate and maintain these technologies, practically placing security out of reach for most organizations.

The irony of the security stack despairs most security teams. While the point of adding technologies is to protect the organization, the more technologies stacked on means that the security teams cannot operate them efficiently to properly protect the organization.

About Cynet 360 AutoXDR™ Cybersecurity Platform

Cynet makes cybersecurity easy. The 360 AutoXDR™ platform enables even the leanest security teams to reach comprehensive, effective protection and visibility across endpoints, users, networks, and SaaS applications – regardless of their resources, size of their team, or skills.

It does it by delivering the first natively automated end-to-end extended detection and response (XDR) platform that's instantly deployed, radically simple to use, and super efficient. The platform provides automated visibility, prevention, detection, correlation, and investigation and response through a single platform.



Cynet 360 AutoXDR™ platform manages the day-to-day security operations, enabling IT security teams to focus their limited resources on managing security rather than operating it.

- **Cynet Protector™** provides multiple native sensor technologies needed to detect and prevent threats across the environment, delivering the capabilities of EPP, EDR, Deception, network detection rules, user behavior analytics rules, threat intelligence, sandbox, Cloud and SaaS Security Posture Management (SSPM/CSPM).

- **Cynet Correlator™** analyzes and correlates all pertinent signal data from Cynet, third-party sensors and log data into actionable incidents, including centralized log management.

- **Cynet Responder™** investigates threats and automatically orchestrates threat response and remediation actions across the entire environment.

- **Cynet complementary CyOps™** 24/7 MDR service provides monitoring, investigation, on-demand analysis, incident response, and threat hunting.

Our vision is to enable security teams to put their cybersecurity on autopilot and focus their limited resources on managing security rather than operating it.

Bring sanity back to cybersecurity with a fresh approach that makes protecting your organization easy and stress-less. Between the broad visibility across your environment, fully automated protection, and complimentary 24/7 MDR service, Cynet eliminates the complexity, cost, and worry of cybersecurity.

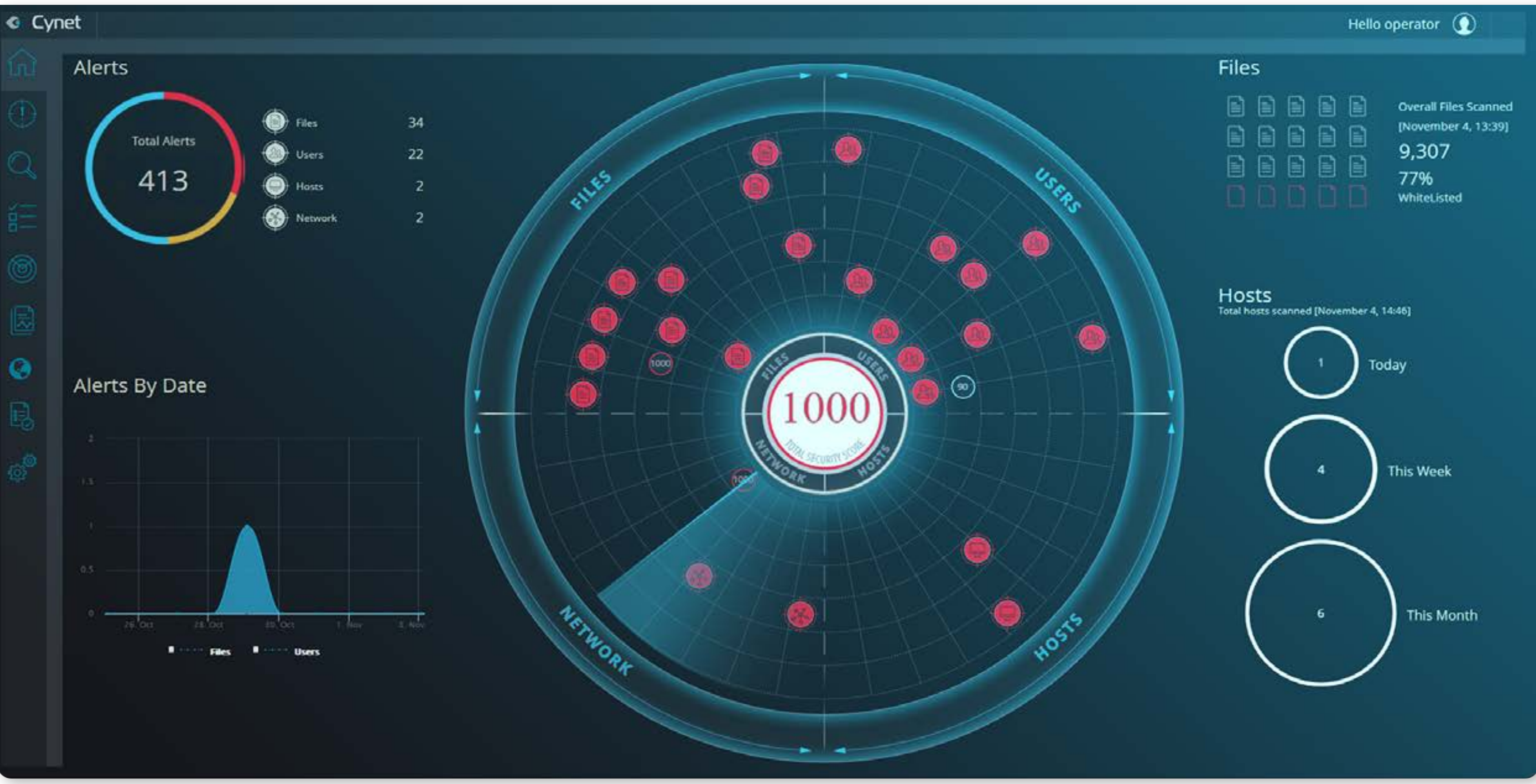
LEARN MORE

Cynet Protector™: Prevention, Detection, IT & Security Operations

Cynet's Protector component natively combines several prevention and detection capabilities out of the box, providing teams with seamless multi-layer protection. This saves teams the time and effort of purchasing, integrating, and managing multiple third-party solutions.

360 Alert View

Receive an immediate view into the threat activity status across the entire environment.



Endpoint Protection

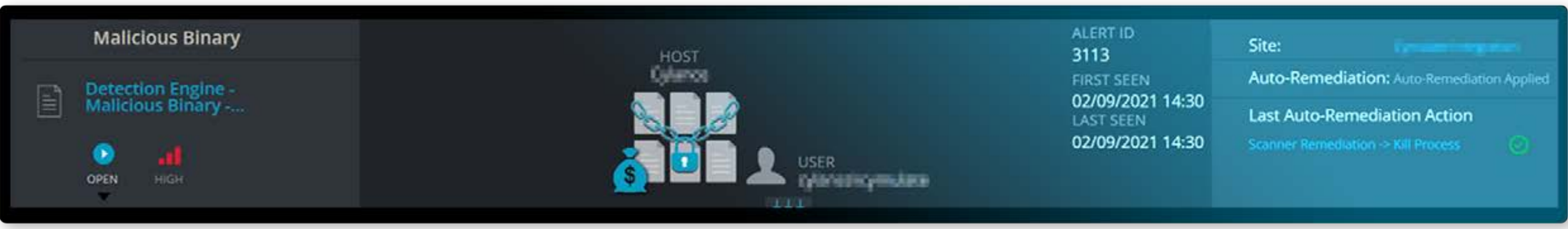
1. NGAV

Scans files at rest and non-executable files to protect against known malware.

- Intelligence-based malware protection
- AI static analysis malware protection
- Behavioral-based exploitation protection
- Behavioral-based fileless, Macro, and script protection

Alert Example 1: Malicious Binary Alert

Cynet's intelligence-based malware protection blocks a file with a malicious binary from executing.



Malicious Binary

Detection Engine - Malicious Binary -...

OPEN HIGH

HOST [redacted]

USER [redacted]

ALERT ID 3113

FIRST SEEN 02/09/2021 14:30

LAST SEEN 02/09/2021 14:30

Site: [redacted]

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

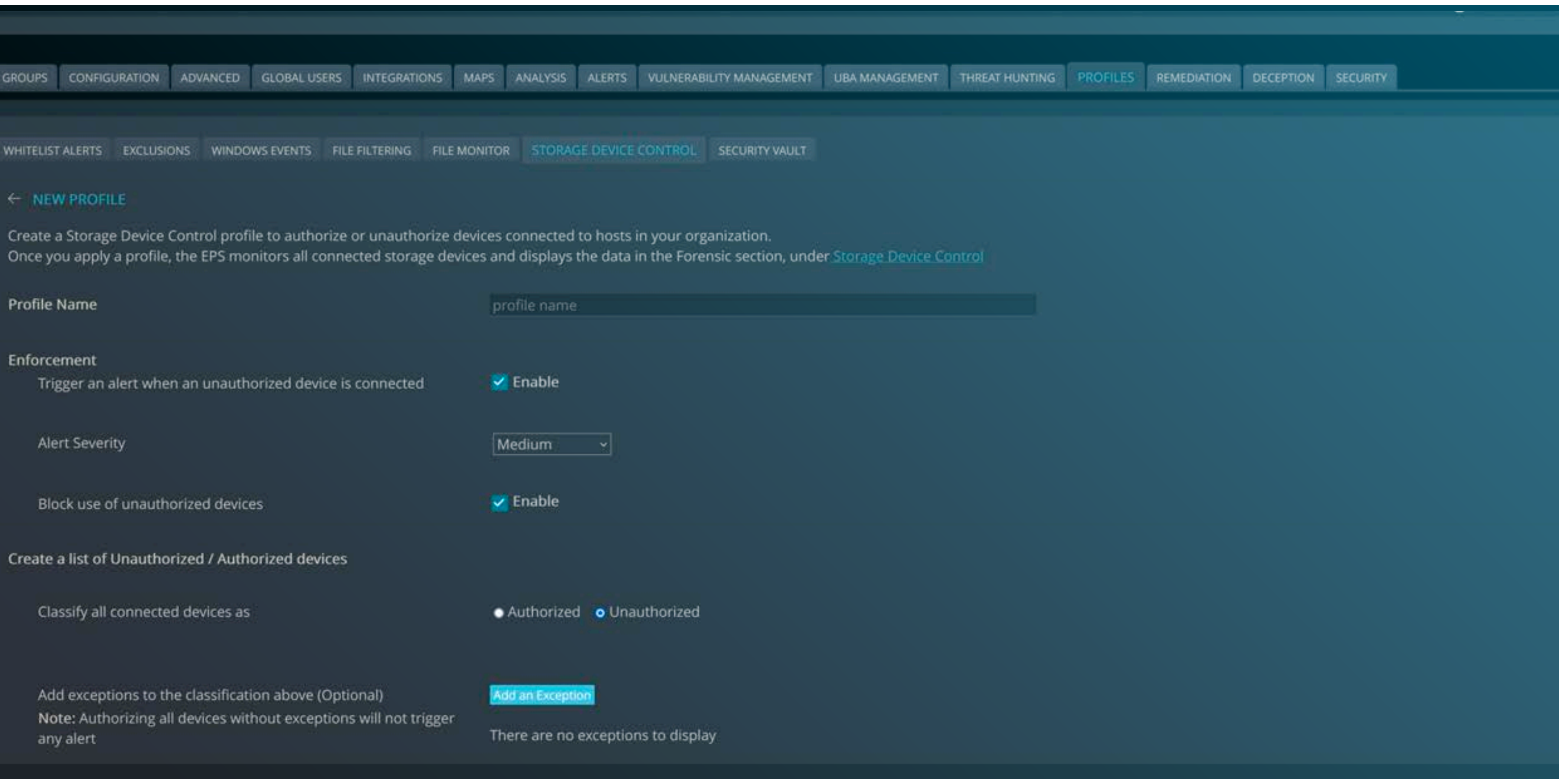
Scanner Remediation -> Kill Process

2. Device Control

Detects and blocks external storage devices that are inserted into the endpoint (for example, a USB device or SD card).

You can create storage device control profiles. Each profile can be assigned to a different scan group and can include rules like:

- Authorized or Unauthorized connecting device based on Device ID
- Authorized or Unauthorized connecting device based on Device Type
- Authorized or Unauthorized connecting device based on Vendor or Product ID Combination of Rules



Create a Storage Device Control profile to authorize or unauthorize devices connected to hosts in your organization.
Once you apply a profile, the EPS monitors all connected storage devices and displays the data in the Forensic section, under Storage Device Control

Profile Name: profile name

Enforcement

Trigger an alert when an unauthorized device is connected: ☑ Enable

Alert Severity: Medium

Block use of unauthorized devices: ☑ Enable

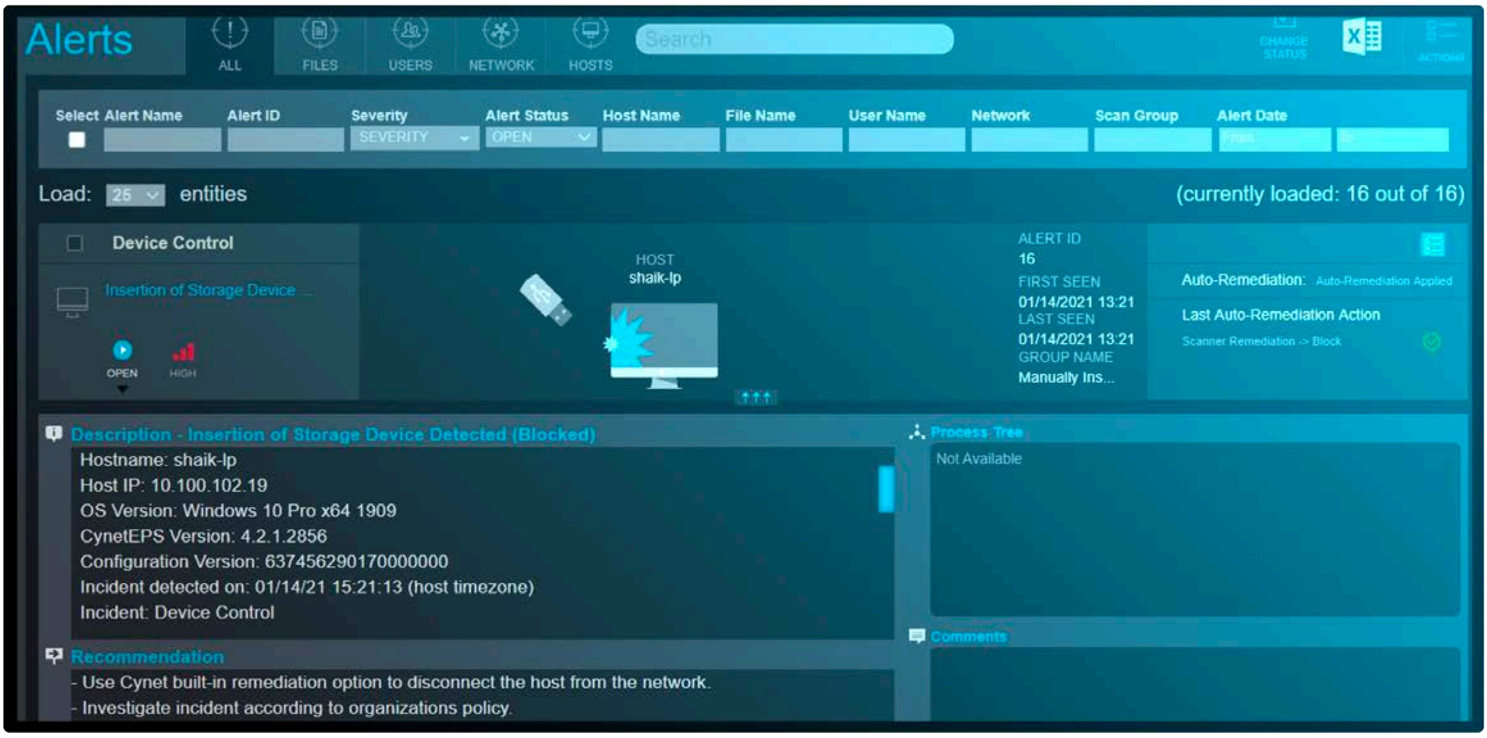
Create a list of Unauthorized / Authorized devices

Classify all connected devices as: ● Authorized ○ Unauthorized

Add exceptions to the classification above (Optional)
Note: Authorizing all devices without exceptions will not trigger any alert

There are no exceptions to display

Alert Example 2: Alert on an inserted storage device
Detecting and blocking an inserted storage device against security policy.



Load: 25 entities (currently loaded: 16 out of 16)

Device Control
Insertion of Storage Device ...

ALERT ID
16
FIRST SEEN
01/14/2021 13:21
LAST SEEN
01/14/2021 13:21
GROUP NAME
Manually Ins...

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action
Scanner Remediation -> Block

Description - Insertion of Storage Device Detected (Blocked)
Hostname: shaik-lp
Host IP: 10.100.102.19
OS Version: Windows 10 Pro x64 1909
CynetEPS Version: 4.2.1.2856
Configuration Version: 637456290170000000
Incident detected on: 01/14/21 15:21:13 (host timezone)
Incident: Device Control

Process Tree: Not Available

Recommendation
- Use Cynet built-in remediation option to disconnect the host from the network.
- Investigate incident according to organizations policy.

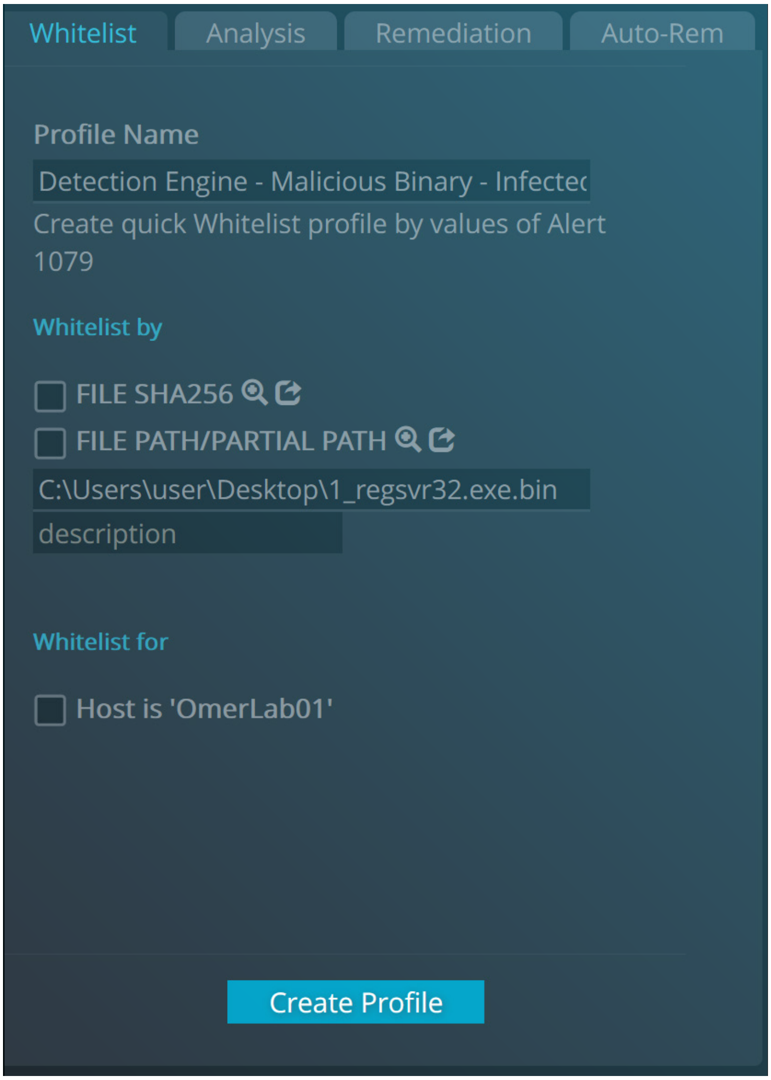
3. Critical Resource Protection

Cynet protects customers' users, networks, hosts (physical and virtual), files, process, cloud components, and configurations thanks to the platform's extensive view of their attack surface. It works by connecting different lightweight sensors to different resources – feeding data to a centralized aggregator.

Cynet's goal is to reduce the number of false positives, allowing customers to sharpen their focus on what's important.

Cynet developed two mechanisms:

- Dynamic Rules: Cynet rules are dynamic and can be modified in real-time by Cyent's CyOps team.
- Whitelisting Rules: Cynet customers can mark a component (like files, hosts, configurations, etc.) as whitelisted and not malicious.



Profile Name

Detection Engine - Malicious Binary - Infectec

Create quick Whitelist profile by values of Alert 1079

Whitelist by

□ FILE SHA256

□ FILE PATH/PARTIAL PATH

C:\Users\user\Desktop\1_regsvr32.exe.bin

description

Whitelist for

□ Host is 'OmerLab01'

Extended Threat Detection

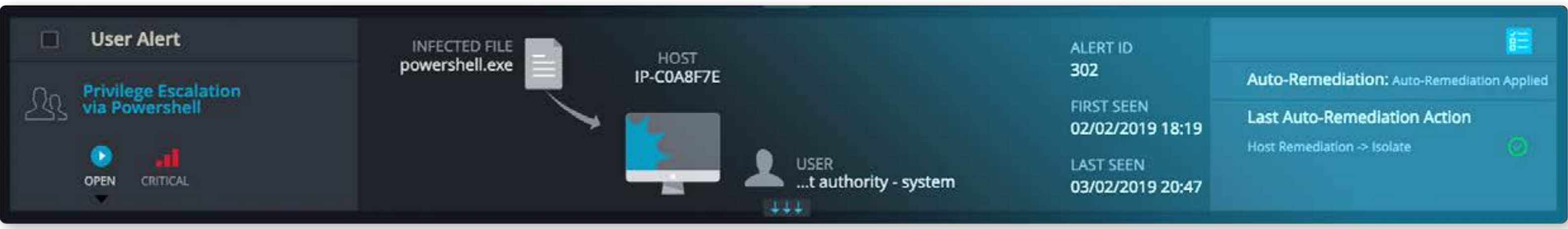
1. EDR

Analyzes process behavior to detect rogue processes and applications through various mechanisms, including:

- **SSDEEP Scan**: uses a compression algorithm that searches for similarities to known malware (aka Fuzzy fingerprints) commonly used for reusing existing tools without their detection via traditional signature-based solutions.
- **Memory Patterns**: analyzes a host's loaded memory for processes and searches for the following: patterns of activity, structure and behavior of data, data with suspicious strings and similarities to known malware, malware activities, processes that load suspicious or malicious DLLs to memory to gain access to sensitive operating system areas or be injected into other processes.
- **Advanced Detection Technology (ADT)**: heuristic tools to inspect operating systems for malicious behavior performed by file-based and fileless based malware and threats. This detects malicious activities in legitimate processes like PowerShell or cmd. ADT analyzes a command's structure, results and the connection between the command to the parent process that searches for malicious patterns like a WinWord file running a PowerShell command.
- **Driver Mode (kernel)**: gain visibility to kernel-level threats. This mechanism also prevents the Cynet Endpoint Protection Scanner (EPS) from being terminated. Protective mechanisms include anti-tampering: protecting Cynet processes from being terminated or manipulated, write protection to sensitive OS areas in the hard disk, proxy to critical system resources such as Lsass.

Alert Example 3: Privilege Escalation

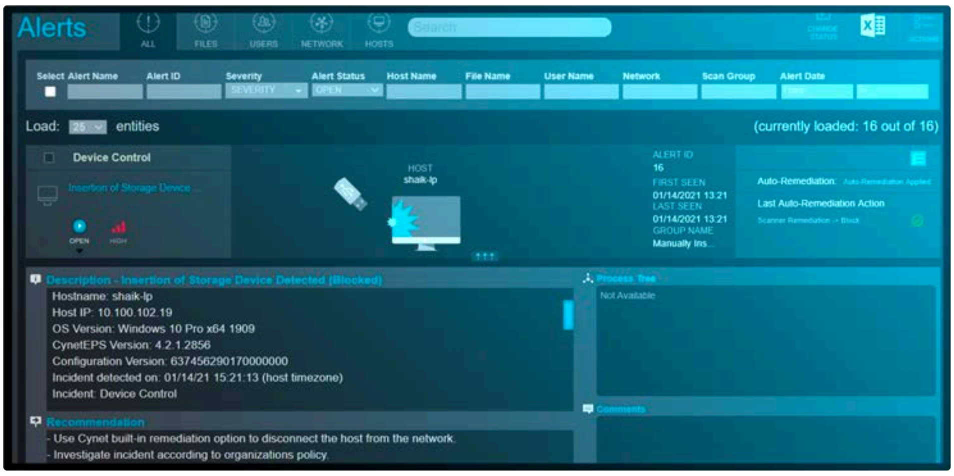
Cynet detects and blocks PowerShell, a legitimate admin process, from attempting to perform a user privilege escalation.



User Alert
Privilege Escalation via Powershell
OPEN CRITICAL
INFECTED FILE: powershell.exe
HOST: IP-C0A8F7E
USER: ...t authority - system
ALERT ID: 302
FIRST SEEN: 02/02/2019 18:19
LAST SEEN: 03/02/2019 20:47
Auto-Remediation: Auto-Remediation Applied
Last Auto-Remediation Action
Host Remediation -> Isolate

Alert Example 4: Exploitation Protection

Cynet detects and blocks a crafted Word document containing an exploit.



Select	Alert Name	Alert ID	Severity	Alert Status	Host Name	File Name	User Name	Network	Scan Group	Alert Date
□			SEVERITY	OPEN						

Load: 25 entities (currently loaded: 16 out of 16)

Device Control
Insertion of Storage Device ...
OPEN HIGH
HOST: shaik-lp
ALERT ID: 16
FIRST SEEN: 01/14/2021 13:21
LAST SEEN: 01/14/2021 13:21
GROUP NAME: Manually Ins...
Auto-Remediation: Auto-Remediation Applied
Last Auto-Remediation Action
Scanner Remediation -> Block

Description - Insertion of Storage Device Detected (Blocked)

Hostname: shaik-lp
Host IP: 10.100.102.19
OS Version: Windows 10 Pro x64 1909
CynetEPS Version: 4.2.1.2856
Configuration Version: 637456290170000000
Incident detected on: 01/14/21 15:21:13 (host timezone)
Incident: Device Control

Recommendation

- Use Cynet built-in remediation option to disconnect the host from the network.
- Investigate incident according to organizations policy.

Process Tree

Not Available

Comments

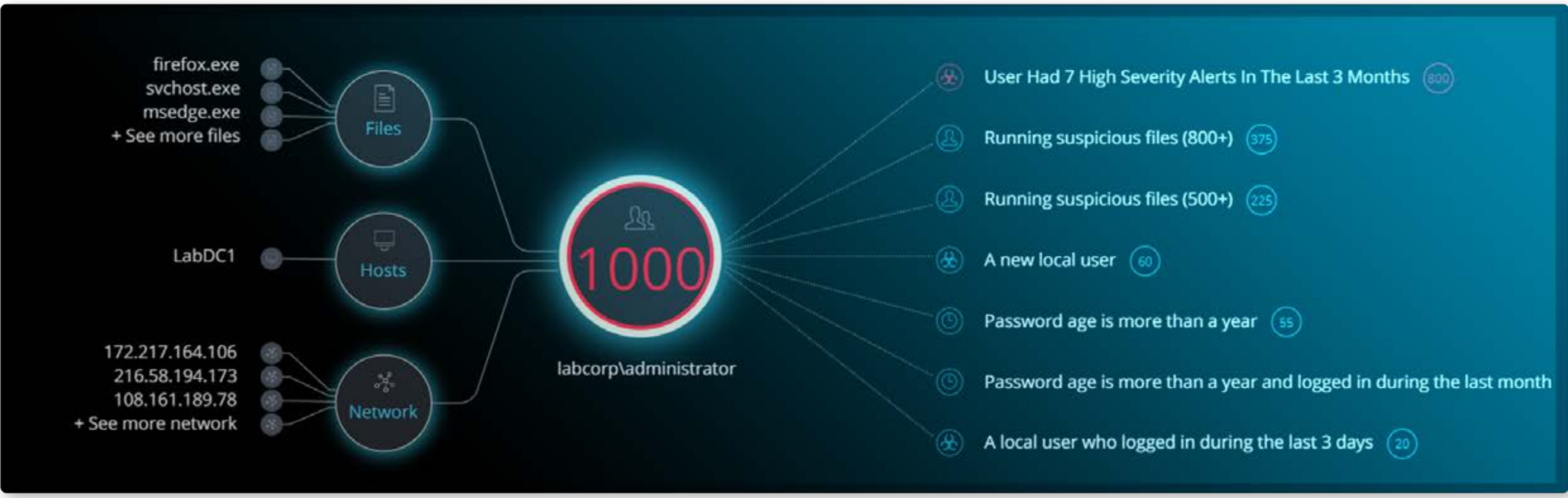
2. User Behavioral Analytics Rules (UBA Rules)

Learns the behavior of user and entities to alert on unusual activity, including:

- Real-time monitoring of all the interactions users initiate
- Hosts users log into, number of hosts, location, and frequency
- Internal and external network communication
- Data files users opened
- Executed processes

Forensics Example 5: User Behavior

Cynet's forensics displays highly suspicious user behavior by correlating various abnormal activities.



User Had 7 High Severity Alerts In The Last 3 Months 800

Running suspicious files (800+) 375

Running suspicious files (500+) 225

A new local user 60

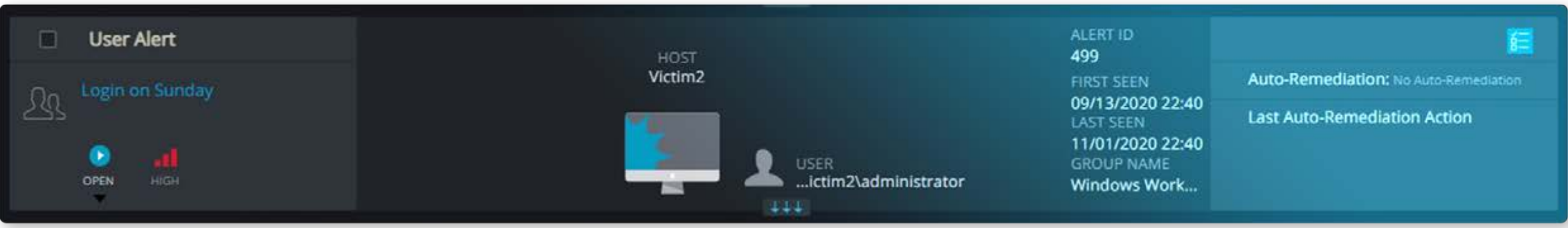
Password age is more than a year 55

Password age is more than a year and logged in during the last month

A local user who logged in during the last 3 days 20

Alert Example 6: Login on Sunday

Cynet's UEBA component detects abnormal weekend login activity.



Login on Sunday

HOST
Victim2

USER
...ictim2\administrator

ALERT ID
499

FIRST SEEN
09/13/2020 22:40

LAST SEEN
11/01/2020 22:40

GROUP NAME
Windows Work...

Auto-Remediation: No Auto-Remediation

Last Auto-Remediation Action

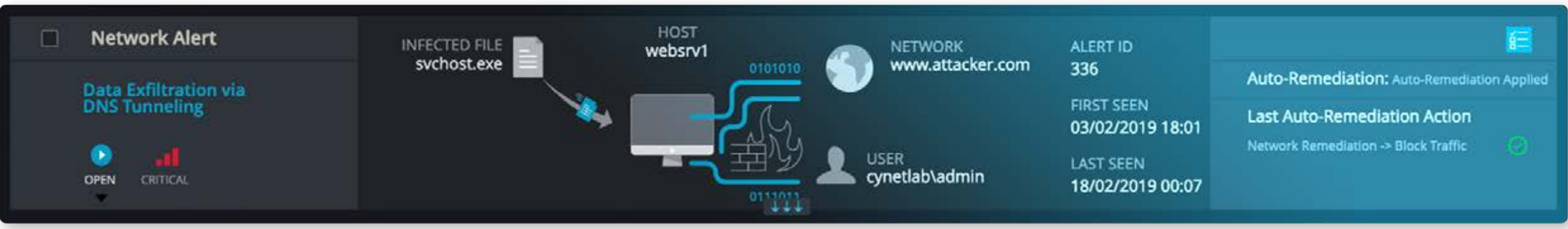
3. Network Detection & Response

Analyzes activities to detect attacks on the network, including:

- Network-based credential theft (ARP spoofing, DNS responder)
- Network-based lateral movement
- Malicious outbound communication (C2C, phishing)
- Network-based reconnaissance (scanning attacks)
- Network-based data exfiltration (tunneling via various protocols)

Alert Example 7: Data Exfiltration

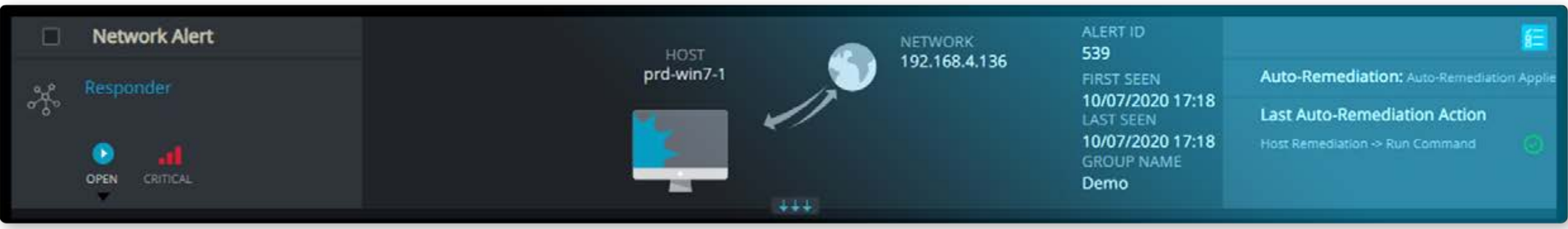
This alert detects an advanced stage in the attack's kill chain where the attacker has gained access to its target data and attempts to exfiltrate it by disguising the compromised data as legitimate DNS traffic.



Network Alert
Data Exfiltration via DNS Tunneling
OPEN CRITICAL
INFECTED FILE svchost.exe
HOST websrv1
NETWORK www.attacker.com
USER cynetlab\admin
ALERT ID 336
FIRST SEEN 03/02/2019 18:01
LAST SEEN 18/02/2019 00:07
Auto-Remediation: Auto-Remediation Applied
Last Auto-Remediation Action
Network Remediation -> Block Traffic

Alert Example 8: Responder malware

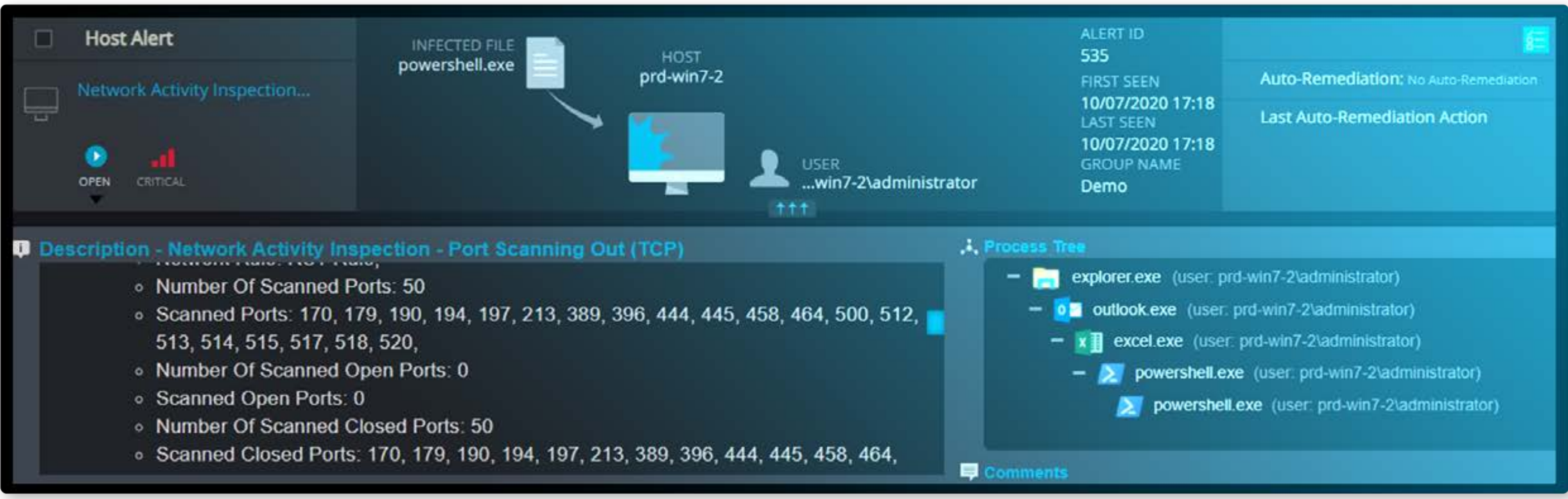
Cynet detects and blocks the Responder malware which exploits network protocols.



Network Alert
Responder
OPEN CRITICAL
HOST prd-win7-1
NETWORK 192.168.4.136
ALERT ID 539
FIRST SEEN 10/07/2020 17:18
LAST SEEN 10/07/2020 17:18
GROUP NAME Demo
Auto-Remediation: Auto-Remediation Applie
Last Auto-Remediation Action
Host Remediation -> Run Command

Alert Example 9: Port Scanning

Cynet detects that a host started to perform a port scan on the network.



Host Alert
Network Activity Inspection...
OPEN CRITICAL
INFECTED FILE powershell.exe
HOST prd-win7-2
USER ...win7-2\administrator
ALERT ID 535
FIRST SEEN 10/07/2020 17:18
LAST SEEN 10/07/2020 17:18
GROUP NAME Demo
Auto-Remediation: No Auto-Remediation
Last Auto-Remediation Action

Description - Network Activity Inspection - Port Scanning Out (TCP)

- Number Of Scanned Ports: 50
- Scanned Ports: 170, 179, 190, 194, 197, 213, 389, 396, 444, 445, 458, 464, 500, 512, 513, 514, 515, 517, 518, 520,
- Number Of Scanned Open Ports: 0
- Scanned Open Ports: 0
- Number Of Scanned Closed Ports: 50
- Scanned Closed Ports: 170, 179, 190, 194, 197, 213, 389, 396, 444, 445, 458, 464,

Process Tree

- explorer.exe (user: prd-win7-2\administrator)
  - outlook.exe (user: prd-win7-2\administrator)
    - excel.exe (user: prd-win7-2\administrator)
      - powershell.exe (user: prd-win7-2\administrator)
        - powershell.exe (user: prd-win7-2\administrator)

Comments

4. Deception

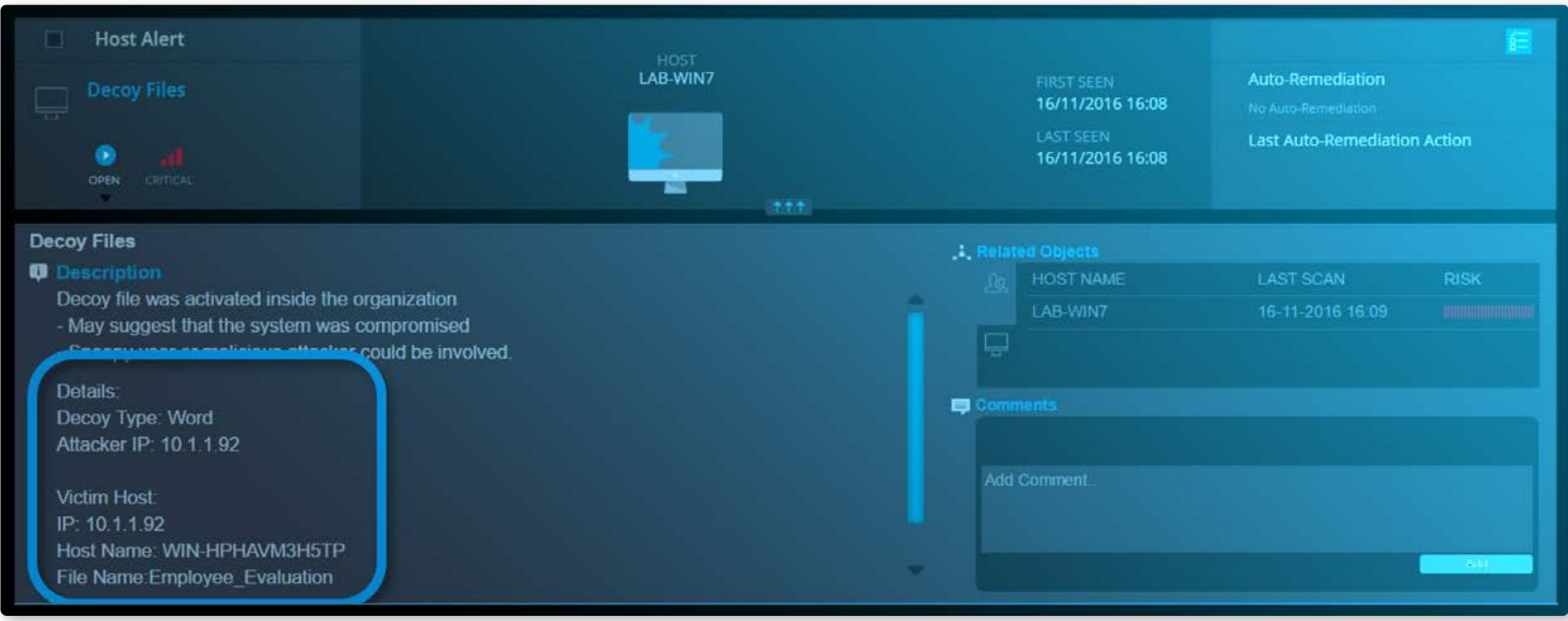
Using honeypot tactics, Cynet places decoys in the environment and monitors them to lure, detect, and alert on attempted attack incidents.

Alerts are generated on detection of:

- Ransomware decoys
- Suspicious files
- User decoys
- Network decoys

Alert Example 10: Deception (Files)

The attacker was lured into revealing their presence through a planted decoy Word file.



FIRST SEEN 16/11/2016 16:08
LAST SEEN 16/11/2016 16:08

Decoy Files

Description

Decoy file was activated inside the organization
- May suggest that the system was compromised
- Snoopy user or malicious attacker could be involved.

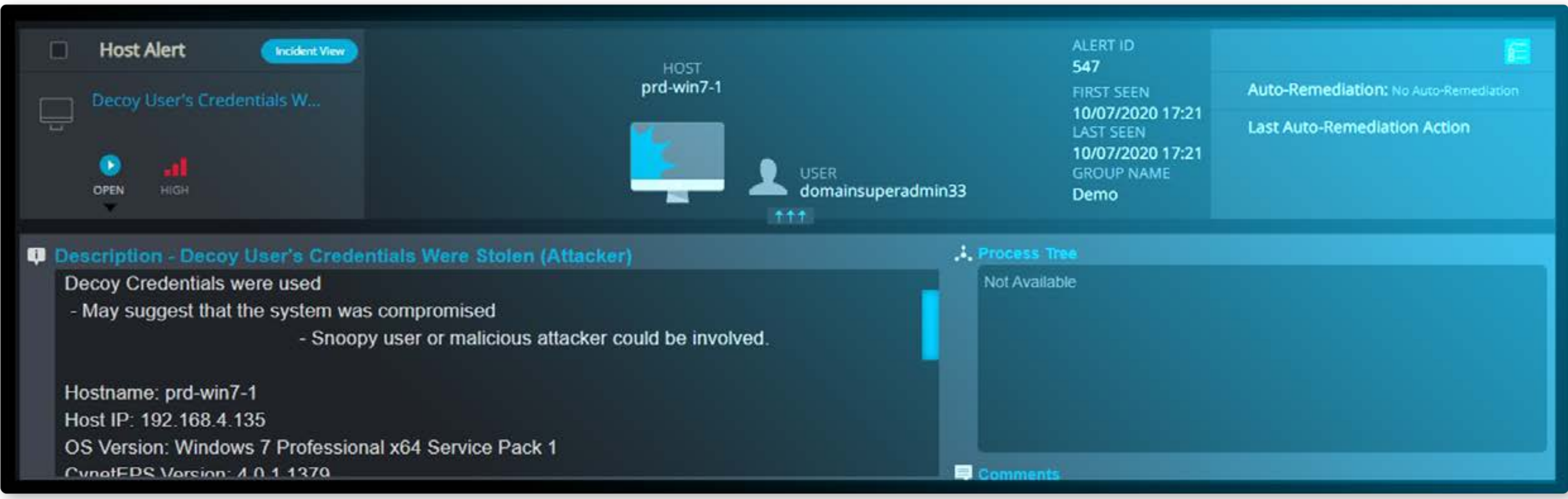
Details:
Decoy Type: Word
Attacker IP: 10.1.1.92

Victim Host:
IP: 10.1.1.92
Host Name: WIN-HPHAVM3H5TP
File Name:Employee_Evaluation

HOST NAME	LAST SCAN	RISK
LAB-WIN7	16-11-2016 16:09	

Alert Example 11: Deception (Users)

The attacker was lured into revealing their presence by attempting to authenticate as a decoy user.



Host Alert
Incident View
Decoy User's Credentials W...
OPEN
HIGH
HOST
prd-win7-1
Auto-Remediation: No Auto-Remediation
Last Auto-Remediation Action
Process Tree
Comments

USER domainsuperadmin33
ALERT ID 547
FIRST SEEN 10/07/2020 17:21
LAST SEEN 10/07/2020 17:21
GROUP NAME Demo

Description - Decoy User's Credentials Were Stolen (Attacker)

Decoy Credentials were used
- May suggest that the system was compromised
- Snoopy user or malicious attacker could be involved.

Hostname: prd-win7-1
Host IP: 192.168.4.135
OS Version: Windows 7 Professional x64 Service Pack 1
CynetEPS Version: 4.0.1.1379

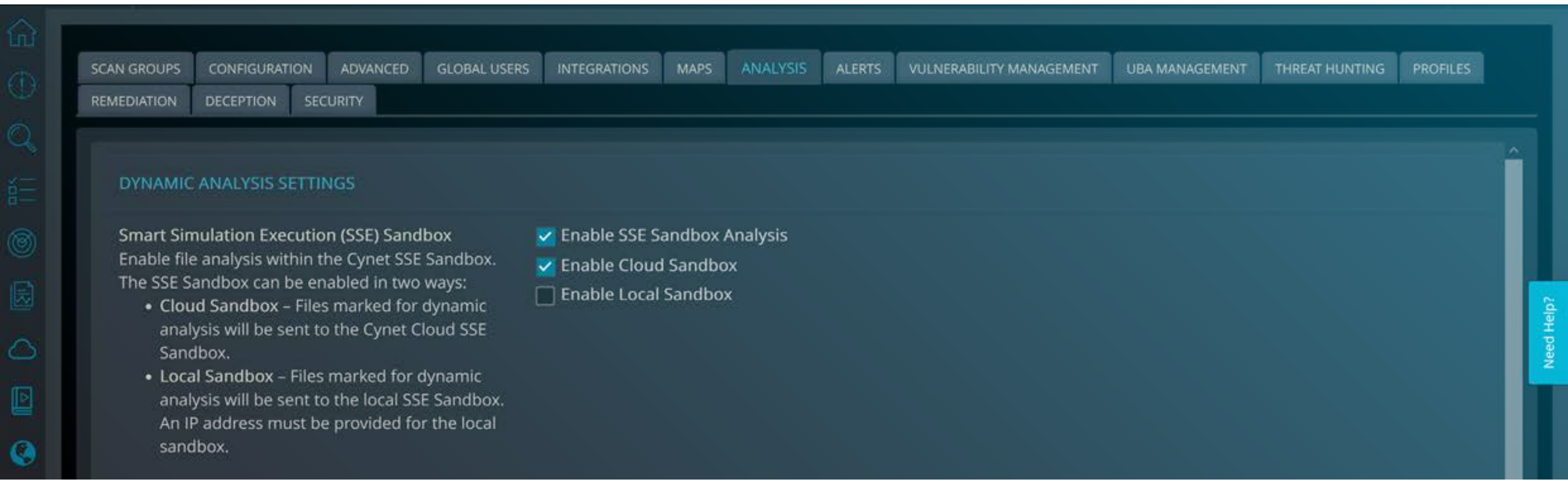
Not Available

5. Sandbox

Cynet's platform sends files for inspection via Smart Simulation Execution (SSE) Sandbox.

The SSE Sandbox can be enabled in two ways:

- **Cloud Sandbox**: files marked for dynamic analysis will be sent to the Cynet Cloud SSE Sandbox.
- **Local Sandbox**: files marked for dynamic analysis will be sent to the local SSE Sandbox. An IP address must be provided for the local sandbox.



DYNAMIC ANALYSIS SETTINGS

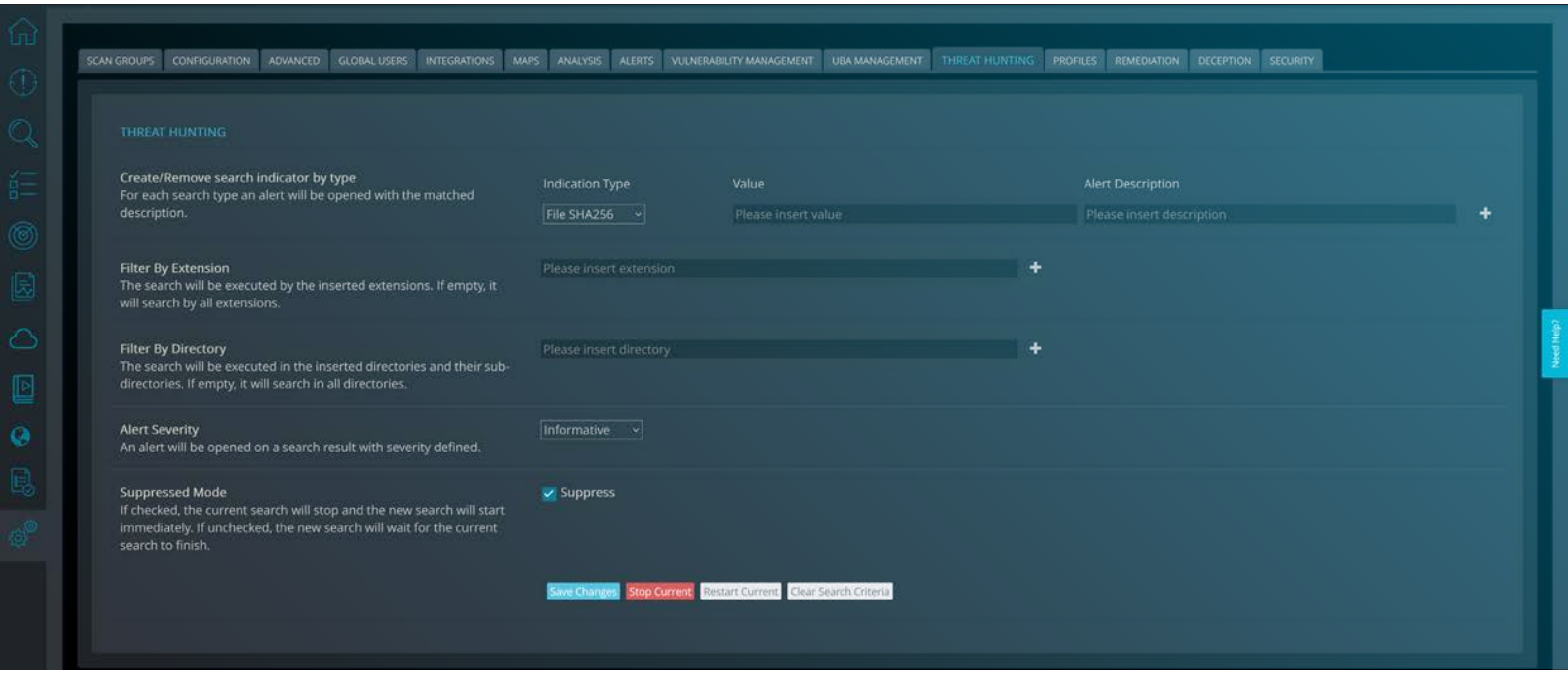
Smart Simulation Execution (SSE) Sandbox
Enable file analysis within the Cynet SSE Sandbox.
The SSE Sandbox can be enabled in two ways:

- Cloud Sandbox – Files marked for dynamic analysis will be sent to the Cynet Cloud SSE Sandbox.
- Local Sandbox – Files marked for dynamic analysis will be sent to the local SSE Sandbox. An IP address must be provided for the local sandbox.

☑ Enable SSE Sandbox Analysis
☑ Enable Cloud Sandbox
☐ Enable Local Sandbox

6. Threat Intelligence

Cyber threats are continuously evolving, which means that there needs to be an ongoing, dynamic mechanism that allows for creating and updating the threat map. Cynet's threat intelligence enables its customers to extend configure Create and update search indicators by SHA256, MD5, FileName, or Full File Path.



THREAT HUNTING

Create/Remove search indicator by type
For each search type an alert will be opened with the matched description.

Indication Type: File SHA256
Value: Please insert value
Alert Description: Please insert description

Filter By Extension
The search will be executed by the inserted extensions. If empty, it will search by all extensions.
Please insert extension

Filter By Directory
The search will be executed in the inserted directories and their sub-directories. If empty, it will search in all directories.
Please insert directory

Alert Severity
An alert will be opened on a search result with severity defined.
Informative

Suppressed Mode
If checked, the current search will stop and the new search will start immediately. If unchecked, the new search will wait for the current search to finish.
☑ Suppress

Cloud & SaaS Security

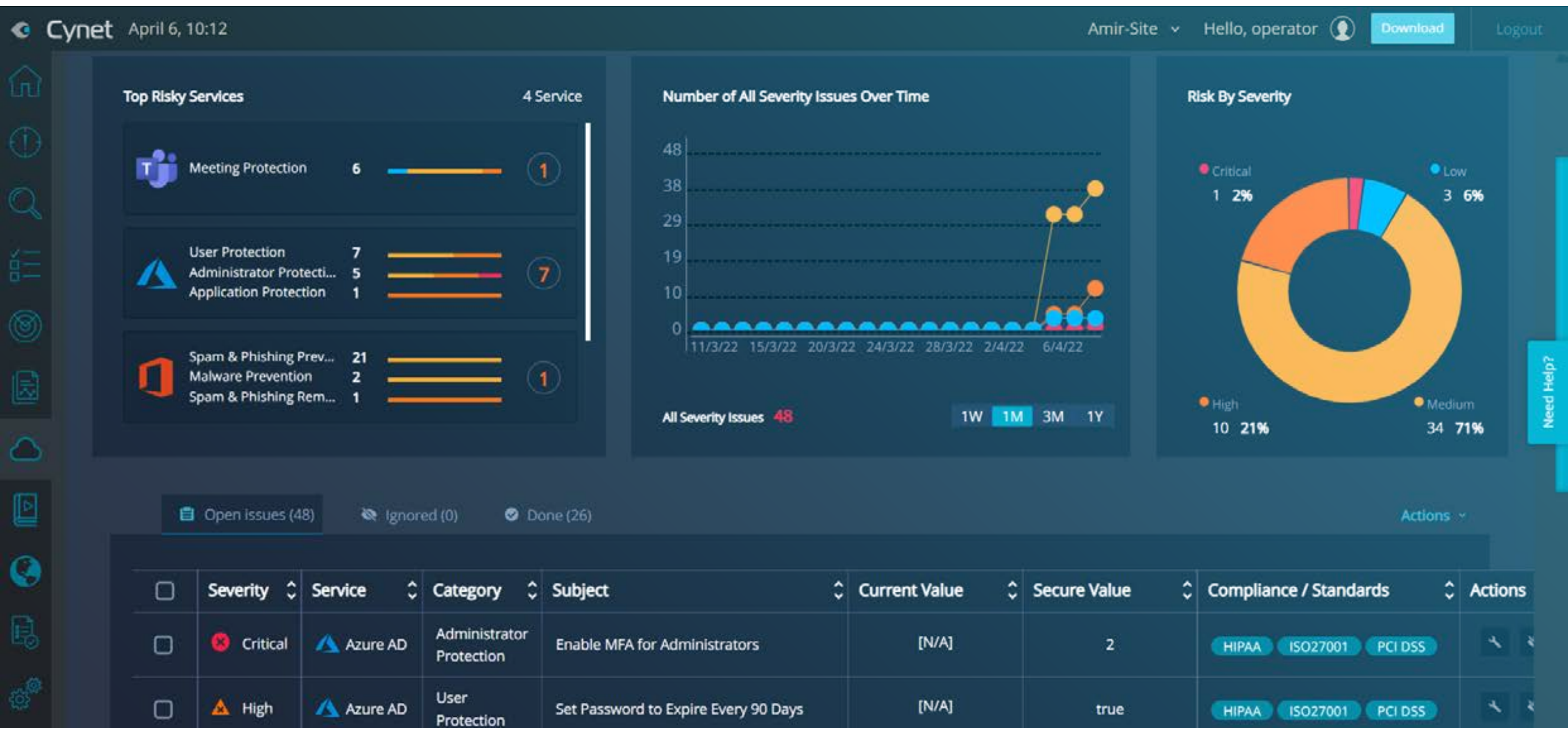
1. SaaS Security Posture Management (SSPM)

Cynet SSPM provides visibility into the security settings of all SaaS applications on a single platform, including:

- Insights into the configuration of the native SaaS security settings
- Suggestions to improve the configurations and reduce the risk
- One-click auto-remediation to correct configuration errors
- Comparison with the industry frameworks with automatic adjustments and reconfiguration

Automatically Discover SaaS Risks

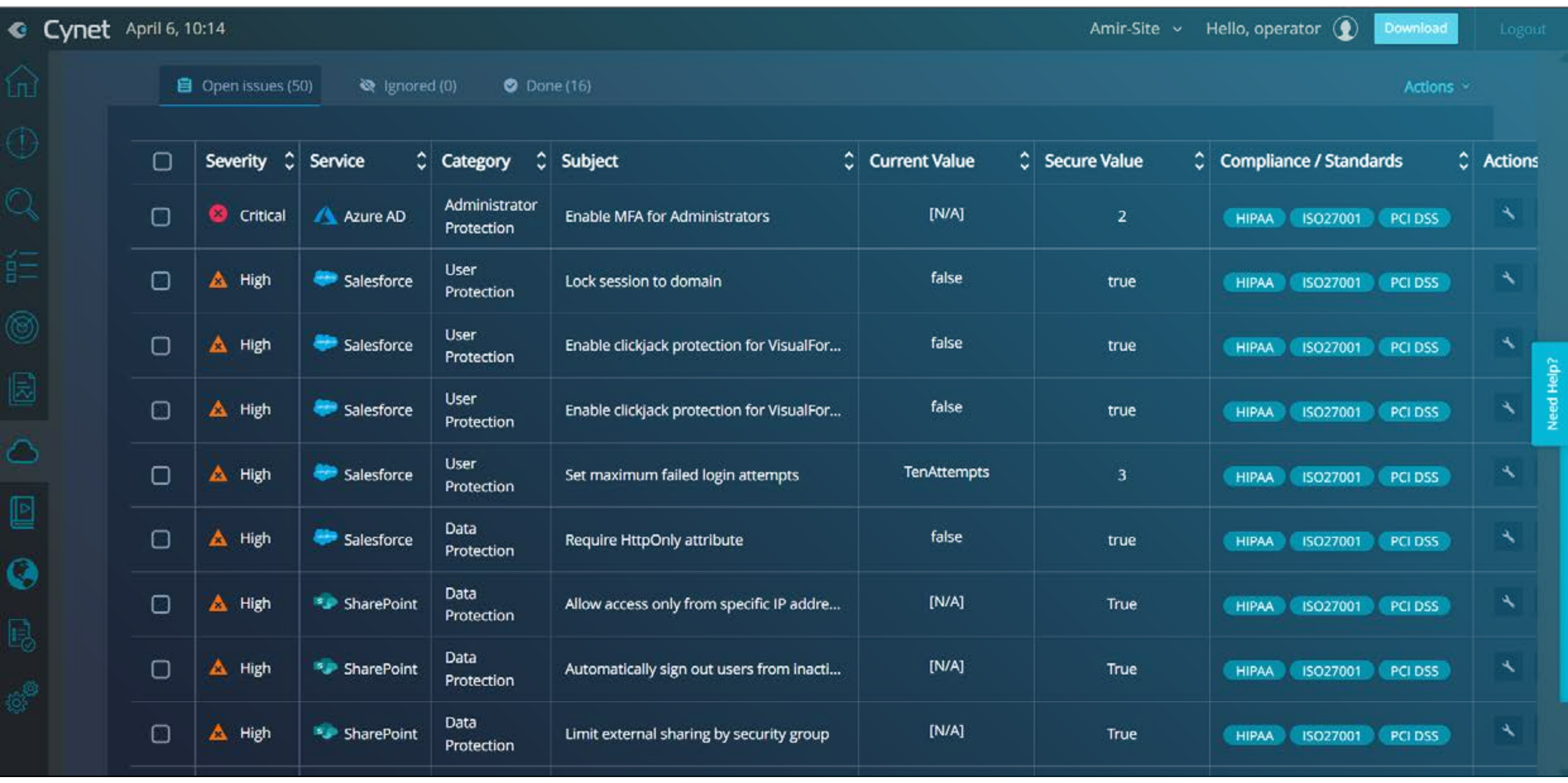
Automatically identify security risks across all your SaaS applications, prioritize risks by category, and track the status of all issues directly from your Cynet dashboard. Gain comprehensive SaaS security risk detection and remediation capabilities to your Cynet dashboard. Proactively monitor configuration settings across your SaaS applications and hunt for security posture issues without the need to access additional panes of glass. Cynet's intuitive user interface allows you to immediately identify and prioritize SaaS security posture issues.



☐	Severity	Service	Category	Subject	Current Value	Secure Value	Compliance / Standards	Actions
☐	Critical	Azure AD	Administrator Protection	Enable MFA for Administrators	[N/A]	2	HIPAA ISO27001 PCI DSS	
☐	High	Azure AD	User Protection	Set Password to Expire Every 90 Days	[N/A]	true	HIPAA ISO27001 PCI DSS	

Analyze and Fix Issue with a Single Click

Drill down to the exact details and insights for each identified risk, see recommended remediation actions, and fix issues with one click. Cynet removes the guesswork by suggesting best practice configuration settings and auto-remediation capabilities that allow you to quickly take action to correct issues before they become security events.



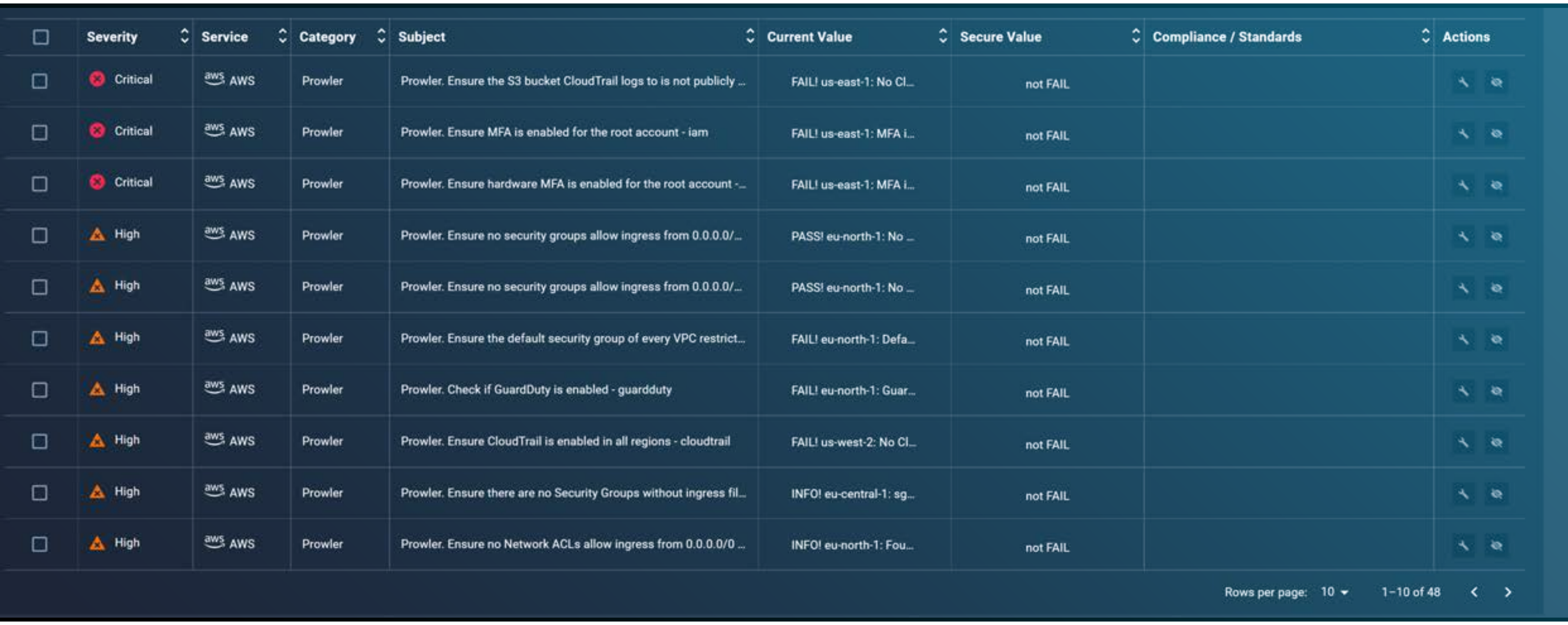
☐	Severity	Service	Category	Subject	Current Value	Secure Value	Compliance / Standards	Actions
☐	Critical	Azure AD	Administrator Protection	Enable MFA for Administrators	[N/A]	2	HIPAA ISO27001 PCI DSS	
☐	High	Salesforce	User Protection	Lock session to domain	false	true	HIPAA ISO27001 PCI DSS	
☐	High	Salesforce	User Protection	Enable clickjack protection for VisualFor...	false	true	HIPAA ISO27001 PCI DSS	
☐	High	Salesforce	User Protection	Enable clickjack protection for VisualFor...	false	true	HIPAA ISO27001 PCI DSS	
☐	High	Salesforce	User Protection	Set maximum failed login attempts	TenAttempts	3	HIPAA ISO27001 PCI DSS	
☐	High	Salesforce	Data Protection	Require HttpOnly attribute	false	true	HIPAA ISO27001 PCI DSS	
☐	High	SharePoint	Data Protection	Allow access only from specific IP addre...	[N/A]	True	HIPAA ISO27001 PCI DSS	
☐	High	SharePoint	Data Protection	Automatically sign out users from inacti...	[N/A]	True	HIPAA ISO27001 PCI DSS	
☐	High	SharePoint	Data Protection	Limit external sharing by security group	[N/A]	True	HIPAA ISO27001 PCI DSS	

2. CSPM

Cynet extends its SSPM offering with cloud security posture management (CSPM) for Amazon Web Services (AWS). It continuously monitors and remediates risk while checking for misconfigurations of cloud services.

Cynet CSPM includes:

- Scans AWS deployed IaaS configuration
  - Regions
  - VMs
  - Storage
  - DBs
  - Networks
  - Users
- Empowered by customizable policies which allows simple and easy configurations of rules.



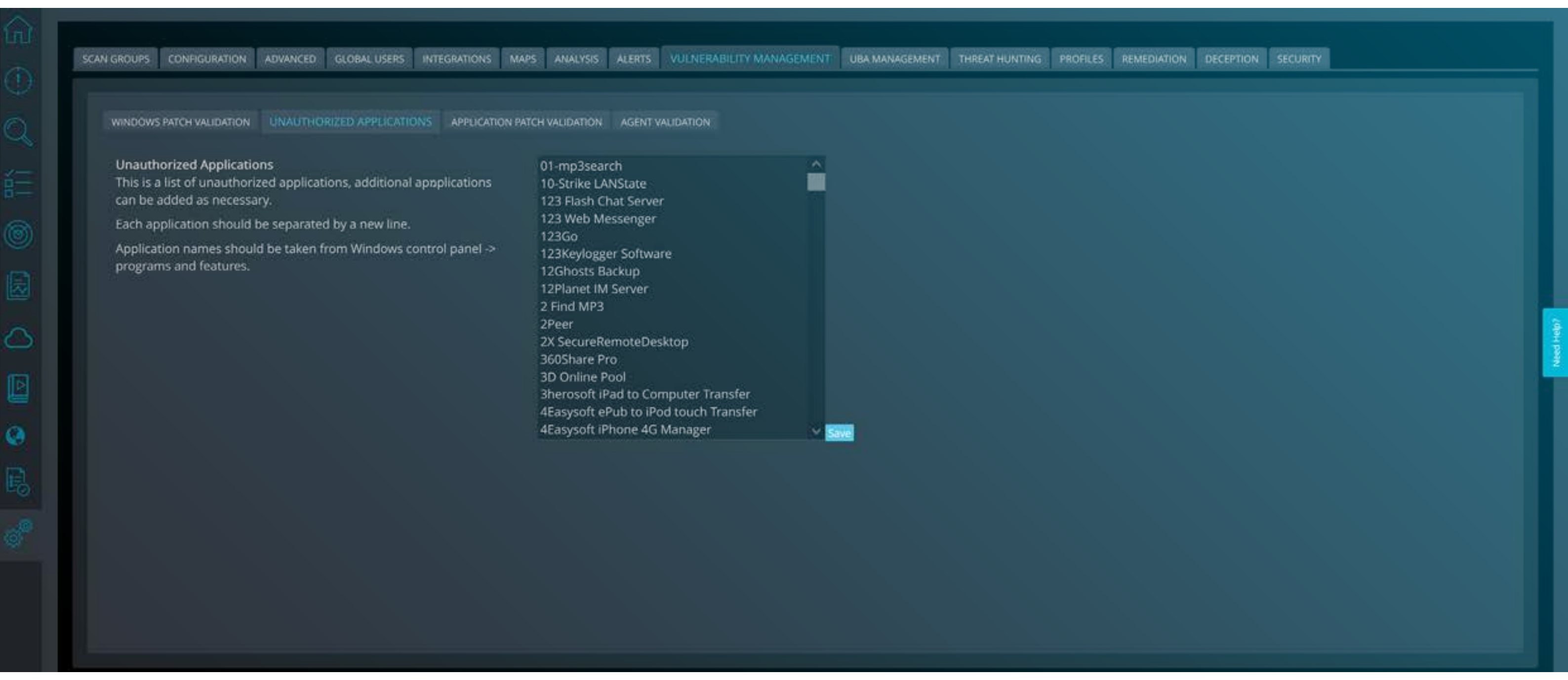
□	Severity	Service	Category	Subject	Current Value	Secure Value	Compliance / Standards	Actions
□	Critical	AWS	Prowler	Prowler. Ensure the S3 bucket CloudTrail logs to is not publicly ...	FAIL! us-east-1: No Cl...	not FAIL		
□	Critical	AWS	Prowler	Prowler. Ensure MFA is enabled for the root account - iam	FAIL! us-east-1: MFA i...	not FAIL		
□	Critical	AWS	Prowler	Prowler. Ensure hardware MFA is enabled for the root account -...	FAIL! us-east-1: MFA i...	not FAIL		
□	High	AWS	Prowler	Prowler. Ensure no security groups allow ingress from 0.0.0.0/...	PASS! eu-north-1: No ...	not FAIL		
□	High	AWS	Prowler	Prowler. Ensure no security groups allow ingress from 0.0.0.0/...	PASS! eu-north-1: No ...	not FAIL		
□	High	AWS	Prowler	Prowler. Ensure the default security group of every VPC restrict...	FAIL! eu-north-1: Defa...	not FAIL		
□	High	AWS	Prowler	Prowler. Check if GuardDuty is enabled - guardduty	FAIL! eu-north-1: Guar...	not FAIL		
□	High	AWS	Prowler	Prowler. Ensure CloudTrail is enabled in all regions - cloudtrail	FAIL! us-west-2: No Cl...	not FAIL		
□	High	AWS	Prowler	Prowler. Ensure there are no Security Groups without ingress fil...	INFO! eu-central-1: sg...	not FAIL		
□	High	AWS	Prowler	Prowler. Ensure no Network ACLs allow ingress from 0.0.0.0/0 ...	INFO! eu-north-1: Fou...	not FAIL		

IT & Security Operations

1. Vulnerability Management

Cynet collects host vulnerabilities and advanced system information and displays these to the user as actionable forensic indicators, such as:

- Unauthorized applications
- Agent validation



Unauthorized Applications
This is a list of unauthorized applications, additional apnplications can be added as necessary.

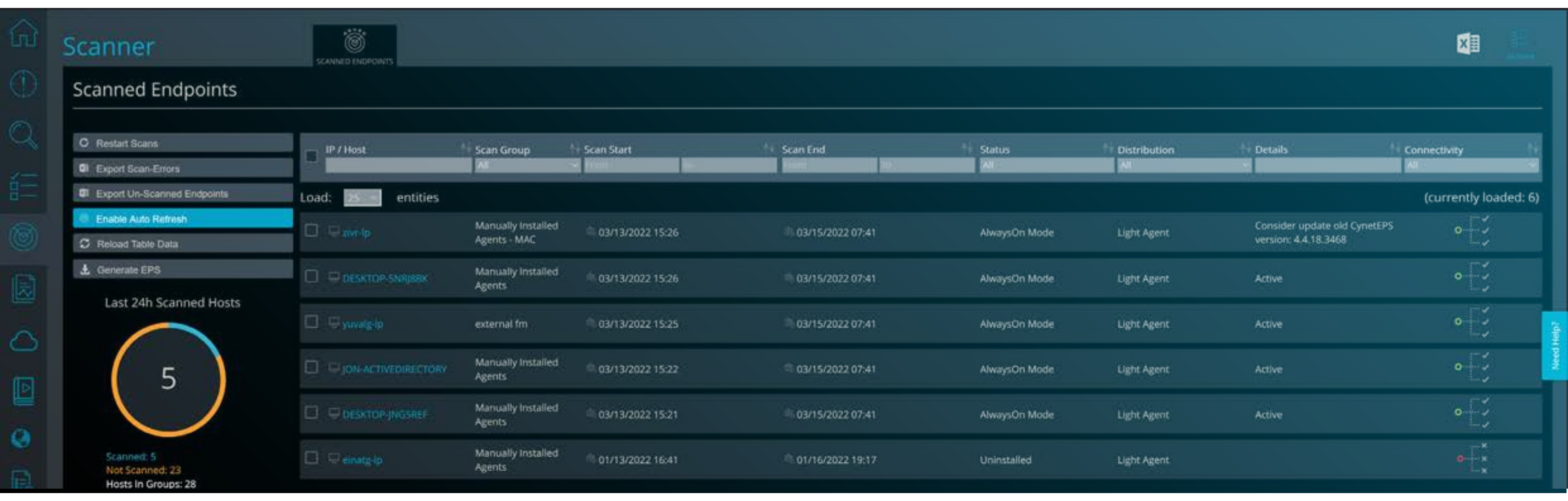
Each application should be separated by a new line.

Application names should be taken from Windows control panel -> programs and features.

```
01-mp3search
10-Strike LANState
123 Flash Chat Server
123 Web Messenger
123Go
123Keylogger Software
12Ghosts Backup
12Planet IM Server
2 Find MP3
2Peer
2X SecureRemoteDesktop
360Share Pro
3D Online Pool
3herosoft iPad to Computer Transfer
4Easysoft ePub to iPod touch Transfer
4Easysoft iPhone 4G Manager
```

2. Asset Inventory

You can review and manage connected assets – like on-prem or cloud application users, files, configurations, certificates – in Cynet's platform. Using this option allows Cynet users to review the asset's status and threat coverage as well as take actions against each asset.



Scanned Endpoints

Load: 25 entities (currently loaded: 6)

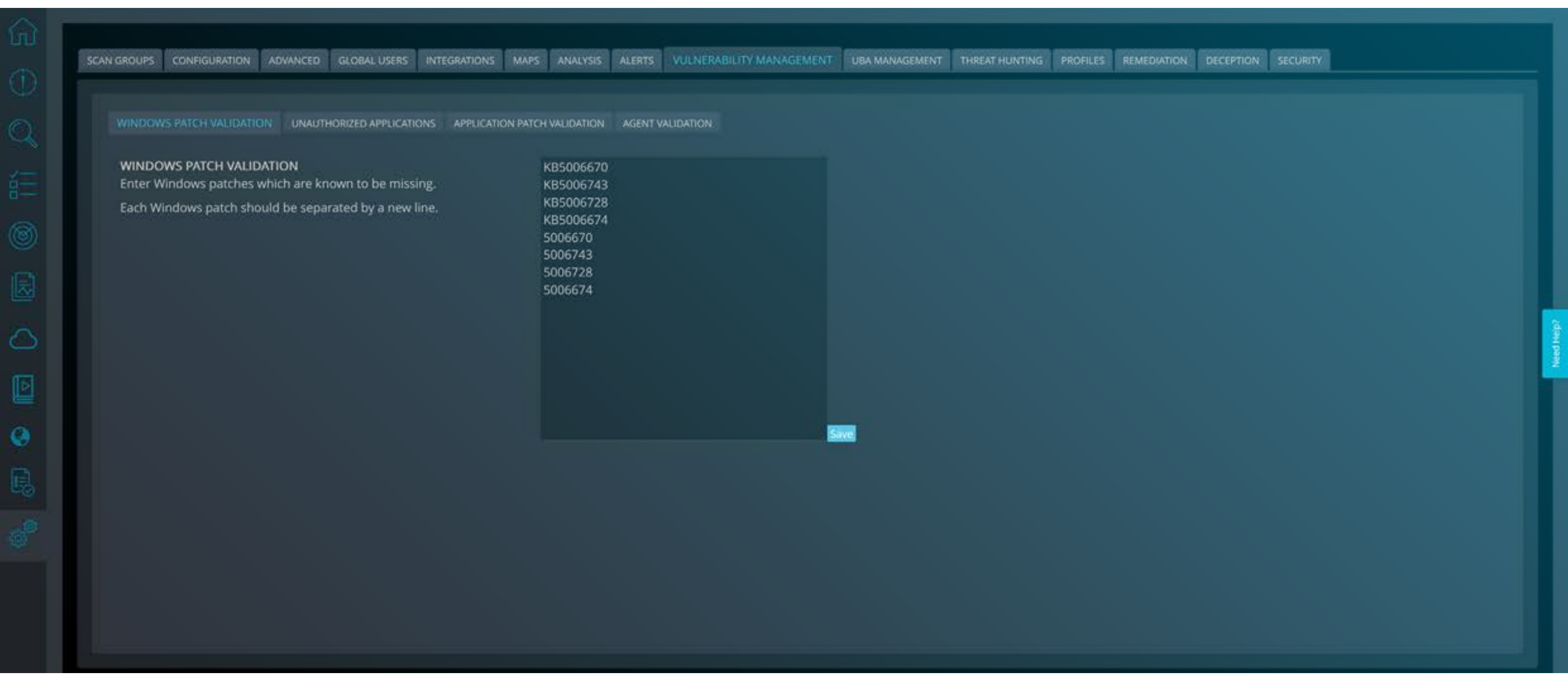
IP / Host	Scan Group	Scan Start	Scan End	Status	Distribution	Details	Connectivity
zivr-lp	Manually Installed Agents - MAC	03/13/2022 15:26	03/15/2022 07:41	AlwaysOn Mode	Light Agent	Consider update old CynetEPS version: 4.4.18.3468	
DESKTOP-SNRJ8BK	Manually Installed Agents	03/13/2022 15:26	03/15/2022 07:41	AlwaysOn Mode	Light Agent	Active	
yuvalg-lp	external fm	03/13/2022 15:25	03/15/2022 07:41	AlwaysOn Mode	Light Agent	Active	
JON-ACTIVEDIRECTORY	Manually Installed Agents	03/13/2022 15:22	03/15/2022 07:41	AlwaysOn Mode	Light Agent	Active	
DESKTOP-JNG5REF	Manually Installed Agents	03/13/2022 15:21	03/15/2022 07:41	AlwaysOn Mode	Light Agent	Active	
einatg-lp	Manually Installed Agents	01/13/2022 16:41	01/16/2022 19:17	Uninstalled	Light Agent		

Last 24h Scanned Hosts
5
Scanned: 5
Not Scanned: 23
Hosts In Groups: 28

3. IT Hygiene

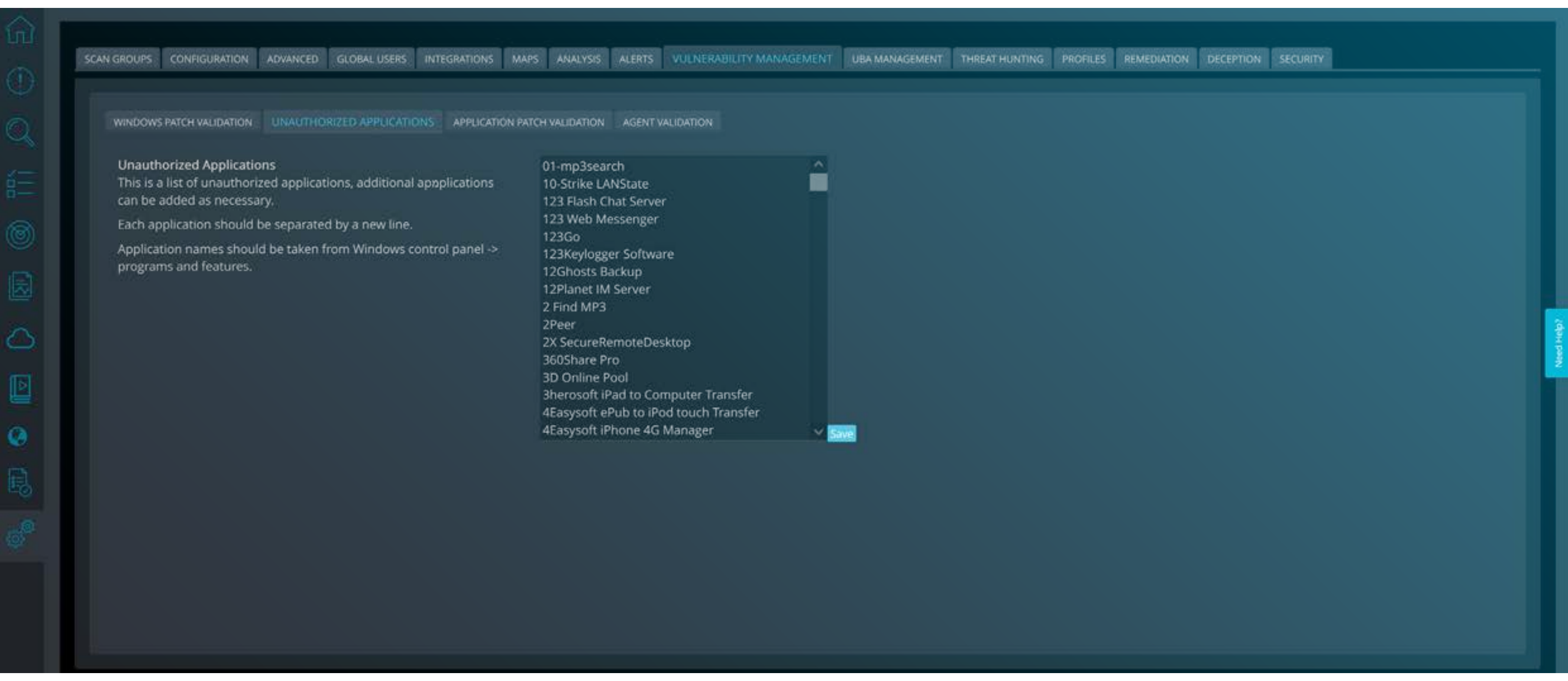
Cynet allows our customers to collect and monitor advanced system information, and displays these to the user as actionable forensic indicators, such as:

- Windows Patch validation
- Applications patch validation



WINDOWS PATCH VALIDATION
Enter Windows patches which are known to be missing.
Each Windows patch should be separated by a new line.

```
KB5006670
KB5006743
KB5006728
KB5006674
5006670
5006743
5006728
5006674
```



Unauthorized Applications
This is a list of unauthorized applications, additional apnplications can be added as necessary.

Each application should be separated by a new line.

Application names should be taken from Windows control panel -> programs and features.

```
01-mp3search
10-Strike LANState
123 Flash Chat Server
123 Web Messenger
123Go
123Keylogger Software
12Ghosts Backup
12Planet IM Server
2 Find MP3
2Peer
2X SecureRemoteDesktop
360Share Pro
3D Online Pool
3herosoft iPad to Computer Transfer
4Easysoft ePub to iPod touch Transfer
4Easysoft iPhone 4G Manager
```

Cynet Responder™: Automated Investigation & Response

Cynet fully automates the entire response workflow, removing manual efforts and ensuring important response details and actions are performed.

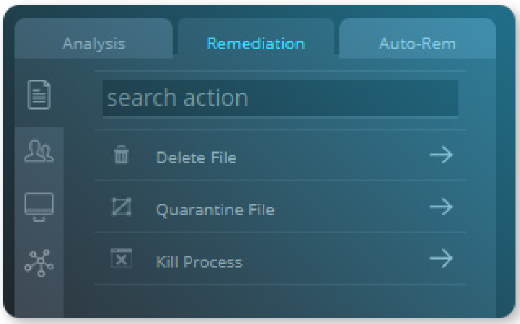
Alerts are logically grouped into incidents, reducing alert fatigue, and providing context of the threat. This includes:

- **Investigation:** Automated root cause and impact analysis
- **Findings:** Actionable conclusions on the attack's origin and its affected entities
- **Remediation:** Elimination of malicious presence, activity, and infrastructure across user, network, and endpoint attacks.

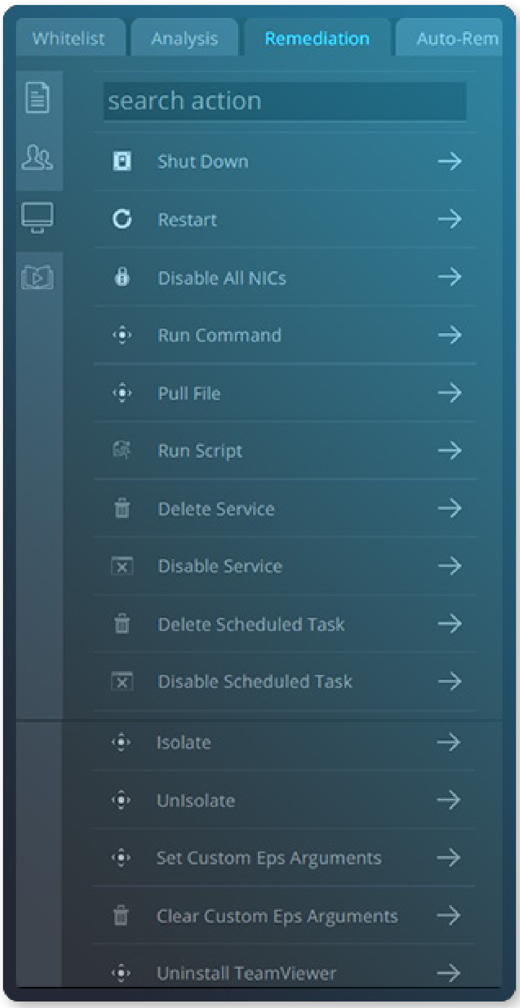
Preset Remediation Actions

Cynet provides the widest available set of remediation tools for infected hosts, malicious files, compromised user accounts, and attacker-controlled traffic.

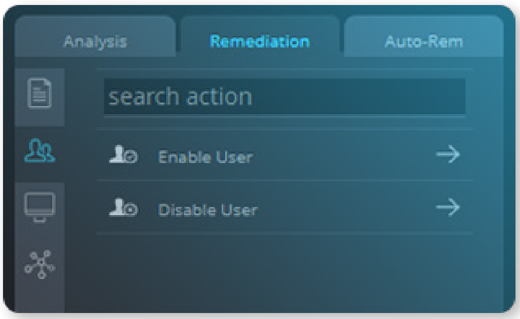
File



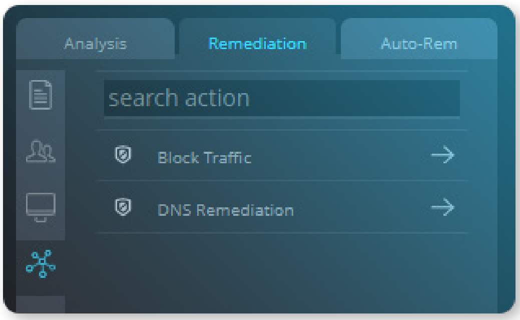
Host



User



Network

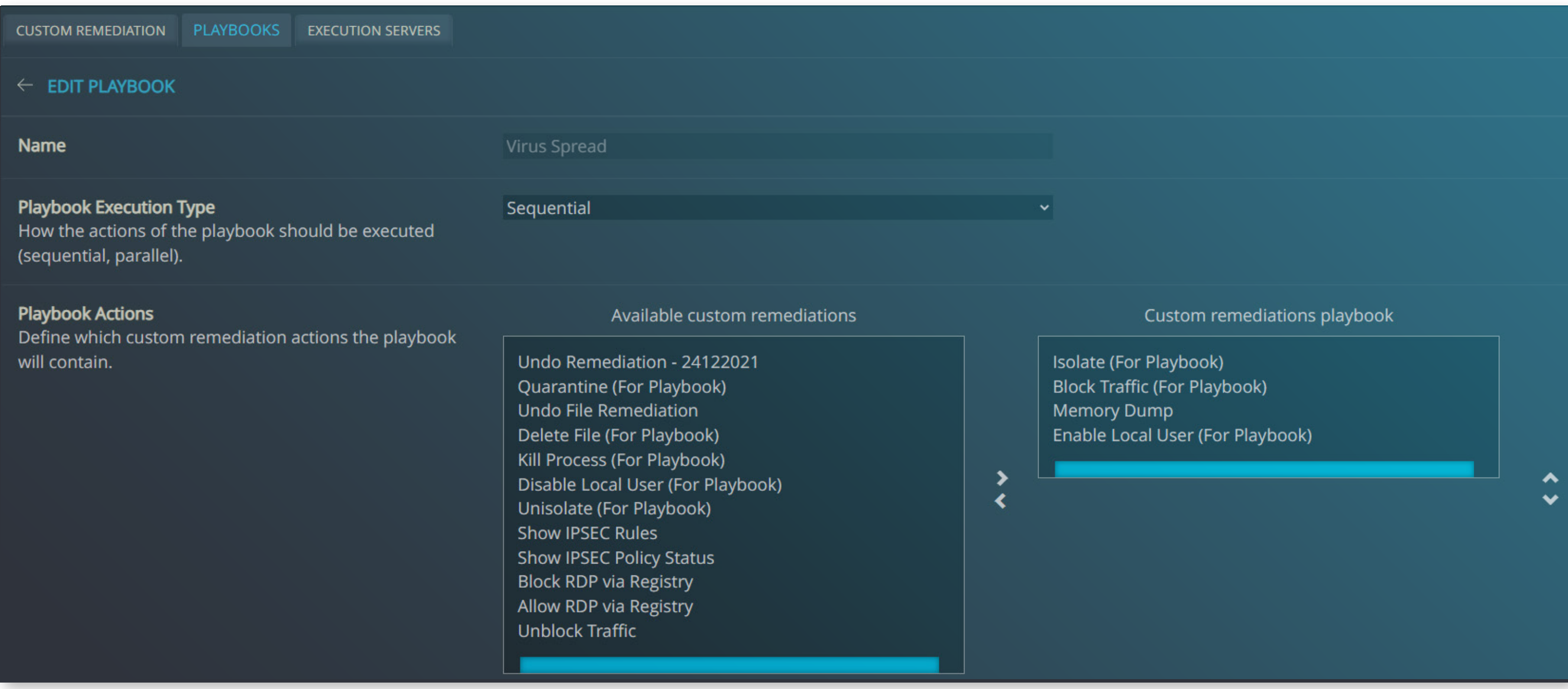


Remediation Playbooks

Playbooks chain together multiple associated remediation actions. This allows your security team to scale their alert-handling capacity by removing repetitive tasks and radically increases the share of attacks that are autonomously addressed and resolved by the Cynet 360 AutoXDR™ platform without need for human intervention.

Cynet 360 AutoXDR™ provides a wide number of remediation actions out of the box and supports the ability to create or edit your own playbook.

Playbook example 1: Virus Spread



Name: Virus Spread

Playbook Execution Type: Sequential
How the actions of the playbook should be executed (sequential, parallel).

Playbook Actions
Define which custom remediation actions the playbook will contain.

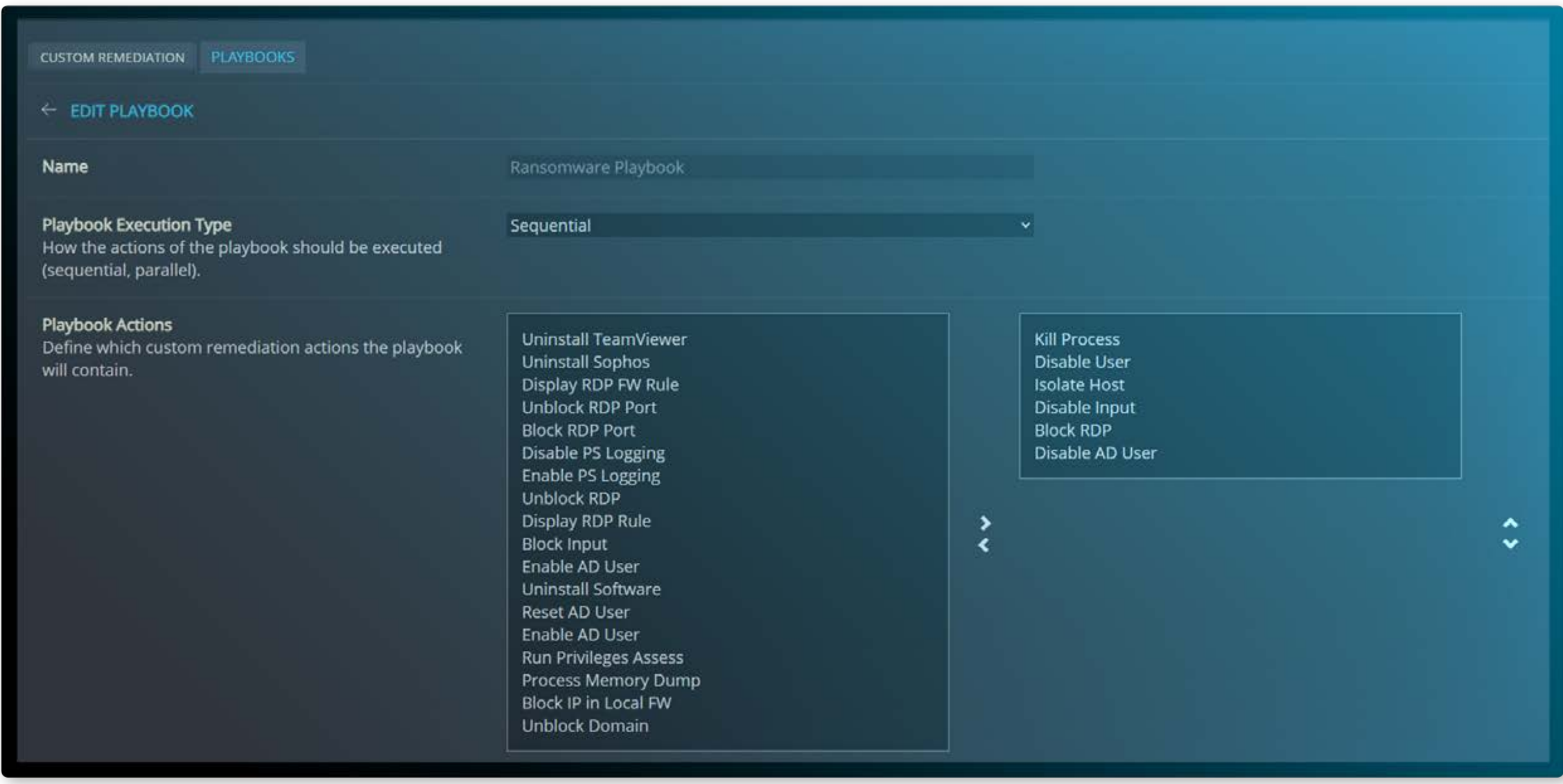
Available custom remediations:
- Undo Remediation - 24122021
- Quarantine (For Playbook)
- Undo File Remediation
- Delete File (For Playbook)
- Kill Process (For Playbook)
- Disable Local User (For Playbook)
- Unisolate (For Playbook)
- Show IPSEC Rules
- Show IPSEC Policy Status
- Block RDP via Registry
- Allow RDP via Registry
- Unblock Traffic

Custom remediations playbook:
- Isolate (For Playbook)
- Block Traffic (For Playbook)
- Memory Dump
- Enable Local User (For Playbook)

In this customized playbook, the displayed remediation actions are automatically run in parallel in order to disable the malware from jumping between machines.

Playbook example 2: Editing a Playbook

Editing your own playbook is easy – you can add or change the flow through a simple drag and drop menu.



Name: Ransomware Playbook

Playbook Execution Type: Sequential
How the actions of the playbook should be executed (sequential, parallel).

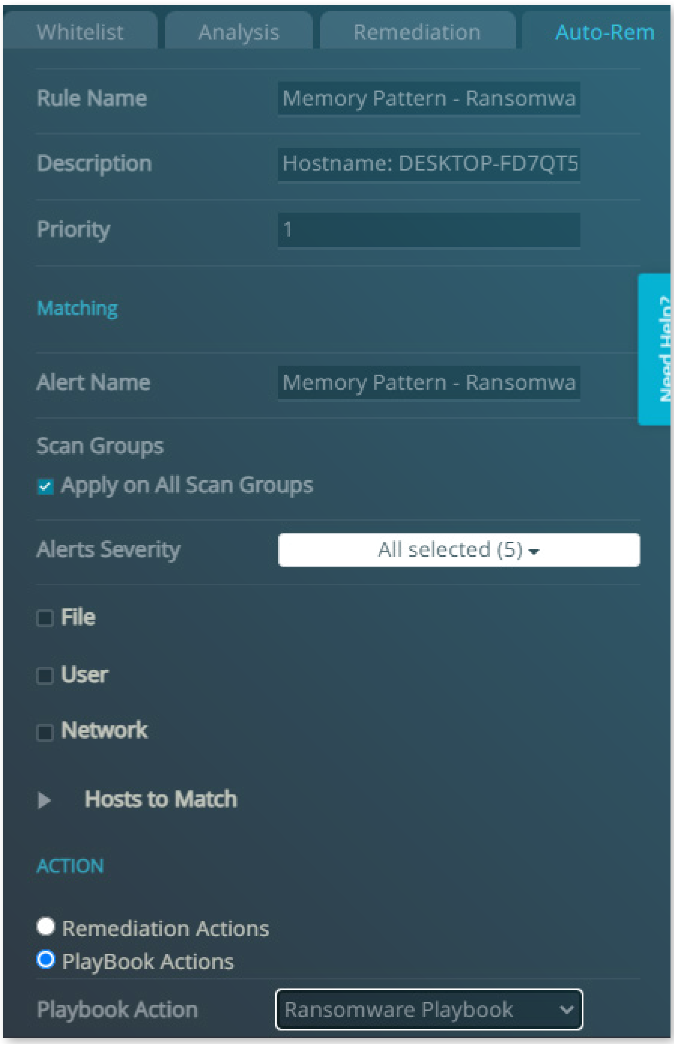
Playbook Actions
Define which custom remediation actions the playbook will contain.

- Uninstall TeamViewer
- Uninstall Sophos
- Display RDP FW Rule
- Unblock RDP Port
- Block RDP Port
- Disable PS Logging
- Enable PS Logging
- Unblock RDP
- Display RDP Rule
- Block Input
- Enable AD User
- Uninstall Software
- Reset AD User
- Enable AD User
- Run Privileges Assess
- Process Memory Dump
- Block IP in Local FW
- Unblock Domain

- Kill Process
- Disable User
- Isolate Host
- Disable Input
- Block RDP
- Disable AD User

Automated Remediation

Cynet 360 AutoXDR™ allows you to automatically run a built-in or customized playbook on a specific alert.



Rule Name: Memory Pattern - Ransomwa

Description: Hostname: DESKTOP-FD7QT5

Priority: 1

Matching

Alert Name: Memory Pattern - Ransomwa

Scan Groups

☑ Apply on All Scan Groups

Alerts Severity: All selected (5)

□ File

□ User

□ Network

▶ Hosts to Match

ACTION

○ Remediation Actions

● PlayBook Actions

Playbook Action: Ransomware Playbook

Incident Engine

Unique to Cynet, the Incident Engine provides automated incident response actions laid out on a visual timeline for immediate understanding of the attack – from root cause and scope of attack to resolution.

The Incident Engine starts by asking a series of questions to determine the root cause and scope of attack. When it has findings, it can take automated actions to remediate the threat. The visual timeline shows you all the necessary remediation actions that were taken to resolve the threat.

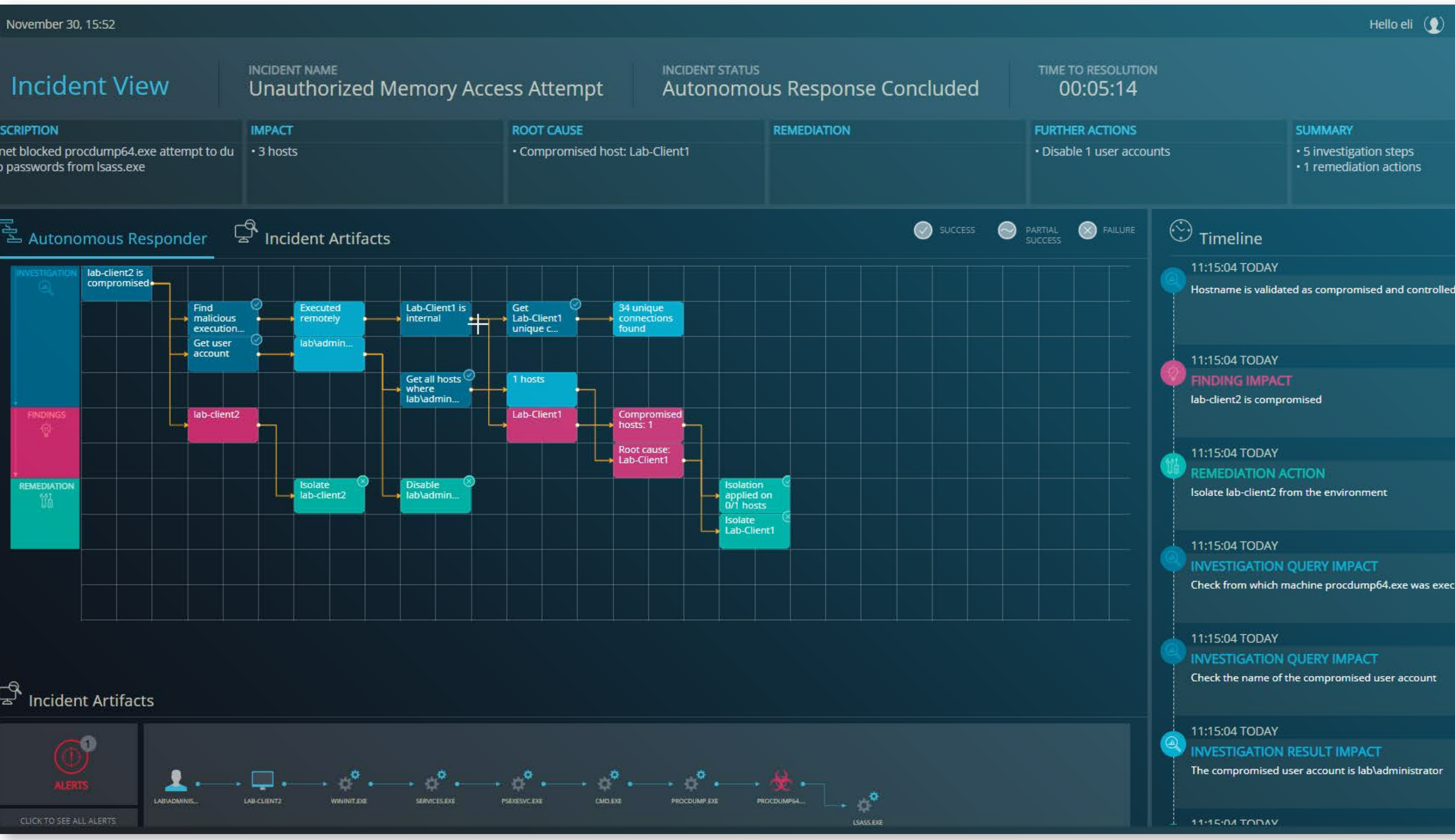
The Incident Engine saves you immense time and efforts. Complete investigation to resolution typically takes seconds to just a few minutes.

Incident Engine Example 1: Malicious Process Command

As part of its automated investigation, the Incident Engine reveals that the process was terminated early enough, preventing the execution of any malicious files. It then identifies that this malicious command was first executed by a Scheduled Task, a common utility leveraged by attackers to bypass security controls. Many attackers plant a Scheduled Task that may lay dormant for a while and then begin executing a malicious file. In this case, it's the wmic.exe file, which leads to the first finding - the root cause is the Scheduled Task.

The Incident Engine immediately takes action and removes the Scheduled Task from the host. It's important to note that if we were to rely only on the prevention level, that Scheduled Task may have continued to execute malicious files, maybe several files, hoping that one would not be detected. The Incident Engine, however, eliminated the root cause before it had the chance to happen.

As part of the investigation, the Incident Engine checks whether the malicious task made its way to other hosts and indeed finds this scheduled task on two other machines. The Incident Engine automatically deletes the scheduled task from them. Finally, the Incident Engine finds the first host to be infected - Yiftach-pc4. This machine communicated with the other two infected hosts so it is automatically isolated before any more damage can be done.



November 30, 15:52

Hello eli

Incident View

INCIDENT NAME
Unauthorized Memory Access Attempt

INCIDENT STATUS
Autonomous Response Concluded

TIME TO RESOLUTION
00:05:14

SCRIPTION
net blocked procdump64.exe attempt to du
p passwords from lsass.exe

IMPACT
- 3 hosts

ROOT CAUSE
- Compromised host: Lab-Client1

REMEDIATION

FURTHER ACTIONS
- Disable 1 user accounts

SUMMARY
- 5 investigation steps
- 1 remediation actions

Timeline

11:15:04 TODAY
Hostname is validated as compromised and controlled

11:15:04 TODAY
FINDING IMPACT
lab-client2 is compromised

11:15:04 TODAY
REMEDIATION ACTION
Isolate lab-client2 from the environment

11:15:04 TODAY
INVESTIGATION QUERY IMPACT
Check from which machine procdump64.exe was exec

11:15:04 TODAY
INVESTIGATION QUERY IMPACT
Check the name of the compromised user account

11:15:04 TODAY
INVESTIGATION RESULT IMPACT
The compromised user account is lab\administrator

11:15:04 TODAY

Cynet Correlator™: Log Management and Event Correlation

Cynet Correlator™ collects and correlates alert and activity data into actionable incidents, providing SIEM-like capabilities.

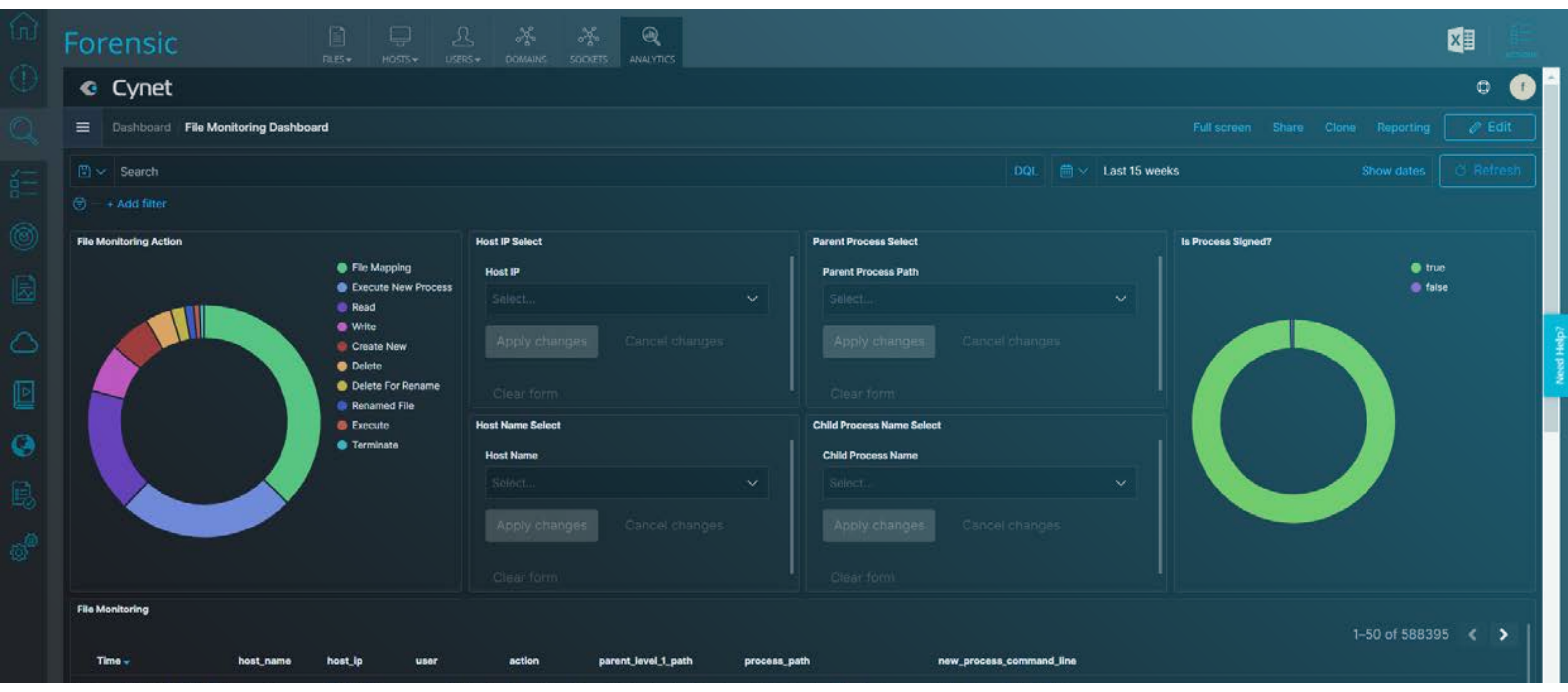
1. Centralized Log Management (CLM)

Cynet Centralized Log Management (CLM) automatically collects the highest-priority log data needed to quickly and accurately uncover threats across your environment.

- Identify threats and anomalies with intuitive analysis and visualization tools
- Simplify forensic analysis to investigate and uncover hidden attack components
- Run custom reports to help assess and demonstrate compliance with industry standards
- Leverage powerful search queries and filters for detailed and thorough analysis icon
- Retain log data in Cynet CLM to help meet compliance requirements icon

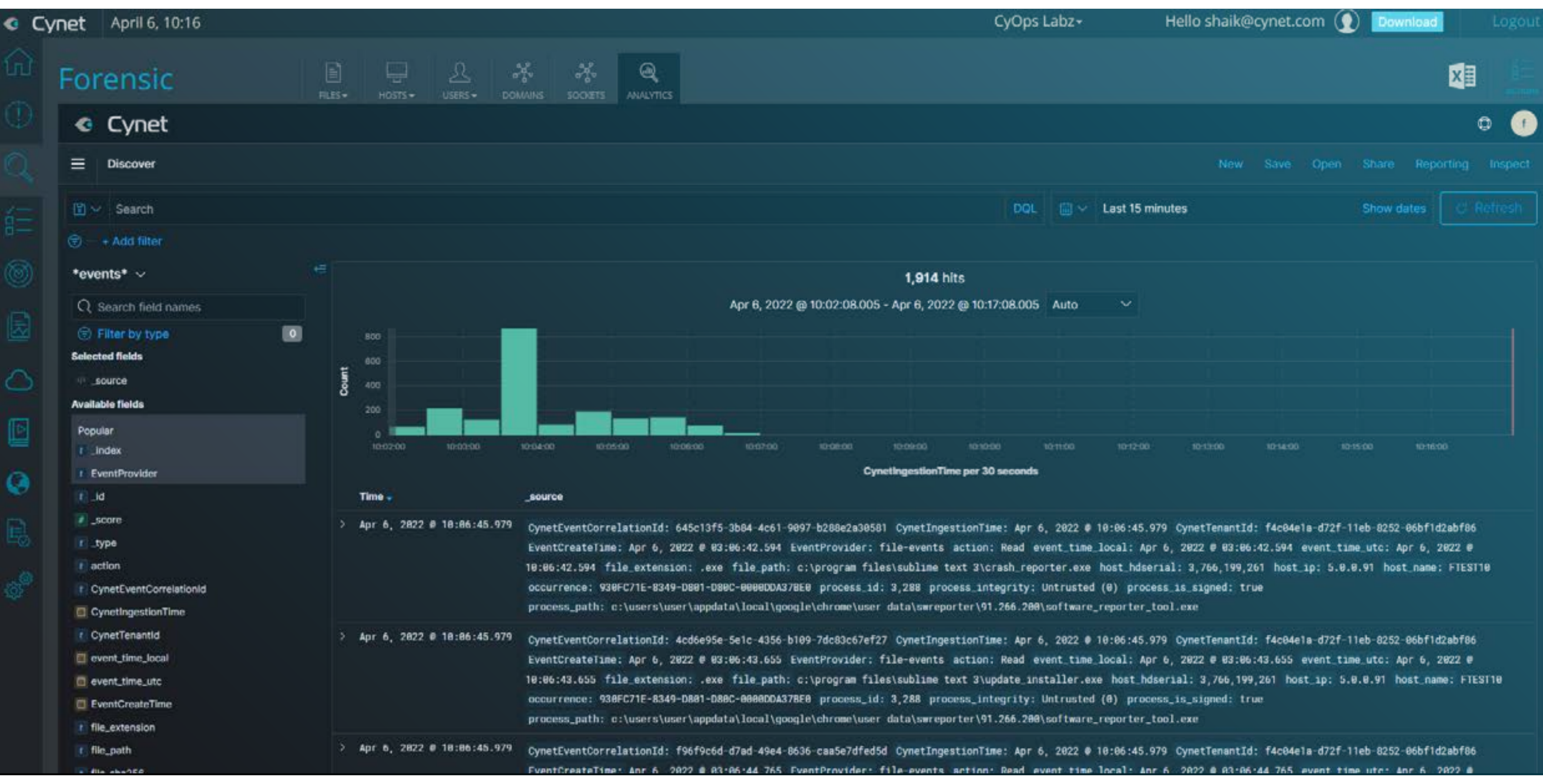
Visually analyze log data with intuitive charts and dashboards

Easily create charts and dashboards to gain insights from your log data. Advanced charts allow you to immediately see anomalies and trends so you can pinpoint and resolve issues quickly.



Analyze log data using an intuitive, consistent user interface

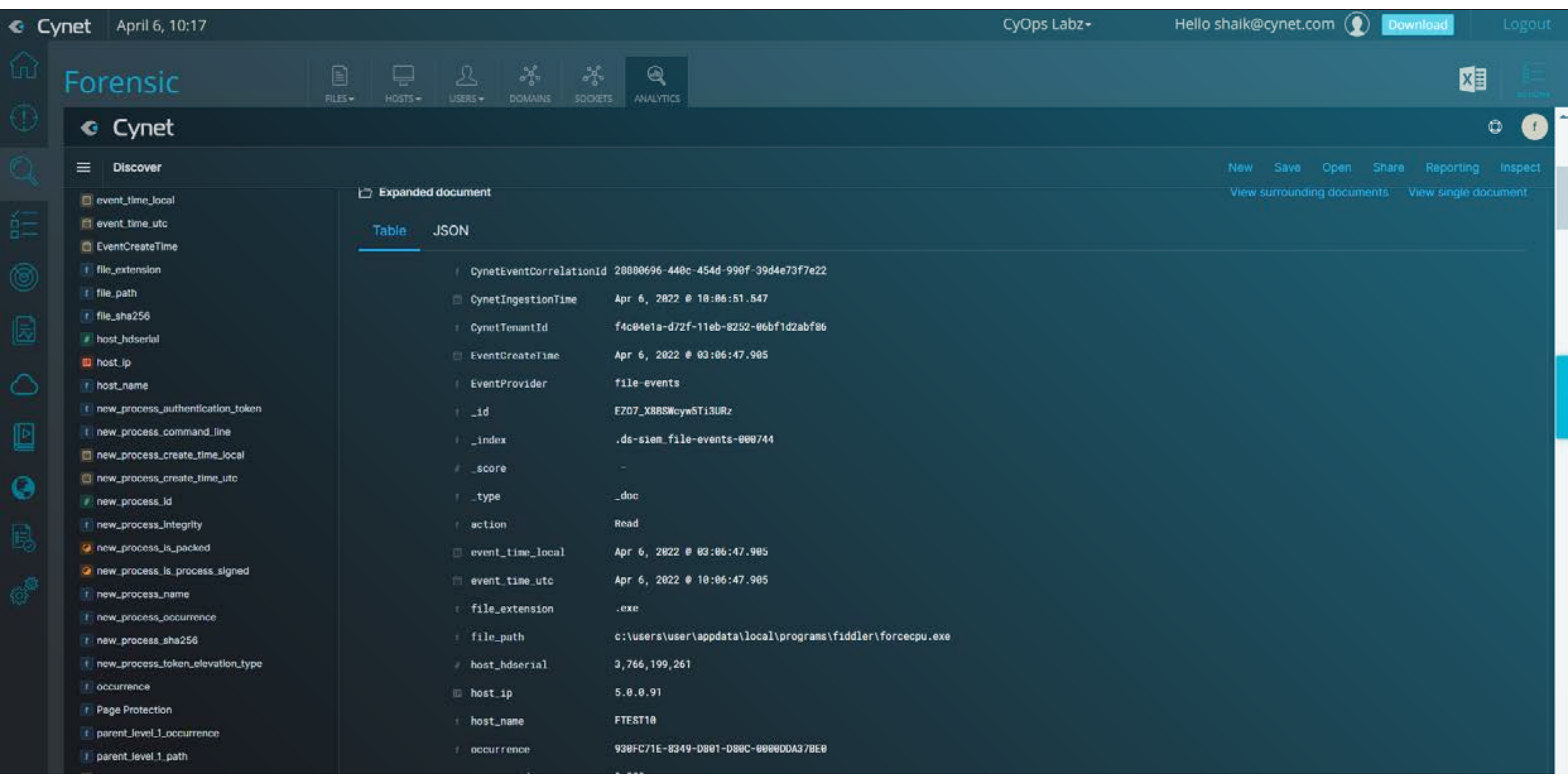
View, sort, query, filter, and correlate events from firewalls, Active Directory (AD), endpoints and more through a single dashboard so you can connect the dots to uncover stealthy threats. Eliminate the time required to sift through multiple siloed logs and to manually collect and correlate evidence. Having all necessary log data in a single pane of glass provides the access and visibility you need without overlooking critical data.



```
Apr 6, 2022 @ 10:06:45.979   CynetEventCorrelationId: 645c13f5-3b84-4c61-9097-b288e2a30581 CynetIngestionTime: Apr 6, 2022 @ 10:06:45.979 CynetTenantId: f4c04e1a-d72f-11eb-8252-06bf1d2abf06 EventCreateTime: Apr 6, 2022 @ 03:06:42.594 EventProvider: file-events action: Read event_time_local: Apr 6, 2022 @ 03:06:42.594 event_time_utc: Apr 6, 2022 @ 10:06:42.594 file_extension: .exe file_path: c:\program files\sublime text 3\crash_reporter.exe host_hdserial: 3,766,199,261 host_ip: 5.0.0.91 host_name: FTEST10 occurrence: 930FC71E-8349-D801-D80C-0000DDA37BE0 process_id: 3,288 process_integrity: Untrusted (0) process_is_signed: true process_path: c:\users\user\appdata\local\google\chrome\user data\swreporter\91.266.200\software_reporter_tool.exe
Apr 6, 2022 @ 10:06:45.979   CynetEventCorrelationId: 4cd6e95e-5e1c-4356-b109-7dc83c67ef27 CynetIngestionTime: Apr 6, 2022 @ 10:06:45.979 CynetTenantId: f4c04e1a-d72f-11eb-8252-06bf1d2abf06 EventCreateTime: Apr 6, 2022 @ 03:06:43.655 EventProvider: file-events action: Read event_time_local: Apr 6, 2022 @ 03:06:43.655 event_time_utc: Apr 6, 2022 @ 10:06:43.655 file_extension: .exe file_path: c:\program files\sublime text 3\update_installer.exe host_hdserial: 3,766,199,261 host_ip: 5.0.0.91 host_name: FTEST10 occurrence: 930FC71E-8349-D801-D80C-0000DDA37BE0 process_id: 3,288 process_integrity: Untrusted (0) process_is_signed: true process_path: c:\users\user\appdata\local\google\chrome\user data\swreporter\91.266.200\software_reporter_tool.exe
Apr 6, 2022 @ 10:06:45.979   CynetEventCorrelationId: f96f9c6d-d7ad-49e4-8636-caa5e7dfed5d CynetIngestionTime: Apr 6, 2022 @ 10:06:45.979 CynetTenantId: f4c04e1a-d72f-11eb-8252-06bf1d2abf06 EventCreateTime: Apr 6, 2022 @ 03:06:44.765 EventProvider: file-events action: Read event_time_local: Apr 6, 2022 @ 03:06:44.765 event_time_utc: Apr 6, 2022 @
```

Deep dive into log data details with a single click

With your critical log data integrated into Cynet CLM, you can see detailed information for every log event with a single click. No need to move between multiple log sources and interfaces with Cynet CLM. Quickly jump to the log data you need for your investigation, all within the Cynet console.



```
CynetEventCorrelationId   28880696-440c-454d-990f-39d4e73f7e22
CynetIngestionTime        Apr 6, 2022 @ 10:06:51.547
CynetTenantId             f4c04e1a-d72f-11eb-8252-06bf1d2abf06
EventCreateTime           Apr 6, 2022 @ 03:06:47.905
EventProvider             file-events
_id                       EZO7_X8BSWcyw5Ti3URz
_index                    .ds-siem_file-events-000744
_score                    -
_type                     _doc
action                    Read
event_time_local          Apr 6, 2022 @ 03:06:47.905
event_time_utc            Apr 6, 2022 @ 10:06:47.905
file_extension            .exe
file_path                 c:\users\user\appdata\local\programs\fiddler\forcecpu.exe
host_hdserial             3,766,199,261
host_ip                   5.0.0.91
host_name                 FTEST10
occurrence                930FC71E-8349-D801-D80C-0000DDA37BE0
```

CyOps: 24/7 Managed Detection and Response (MDR) Team

Cynet complements its autonomous breach protection technology with integrated security services at no additional cost. CyOps is a 24/7 team of threat analysts and security researchers that leverage their expertise and Cynet's vast threat intelligence feeds to provide various services to Cynet's customers, in respect to each customer's specific needs and security preferences.

Alert Monitoring

The CyOps team continuously monitors your environment – every hour of every day throughout the year. The team manages events, alerts, customer inquiries, and incidents. The team also provides alert analysis and correlation to other Cynet 360 AutoXDR™ alerted events.

The CyOps team will proactively contact you when certain alerts or events are detected along with specific actions that should be taken.

Threat Hunting

CyOps continually searches for new emerging threats in order to implement Indicators of Compromise (IoCs) and patterns into Cynet 360 AutoXDR™ mechanisms. These proactive actions enable Cynet 36 AutoXDR™ 0 to collect, analyze, and alert for events while giving the forensics feature its ability to assess an entity's risk level.

Remote Incident Response (IR)

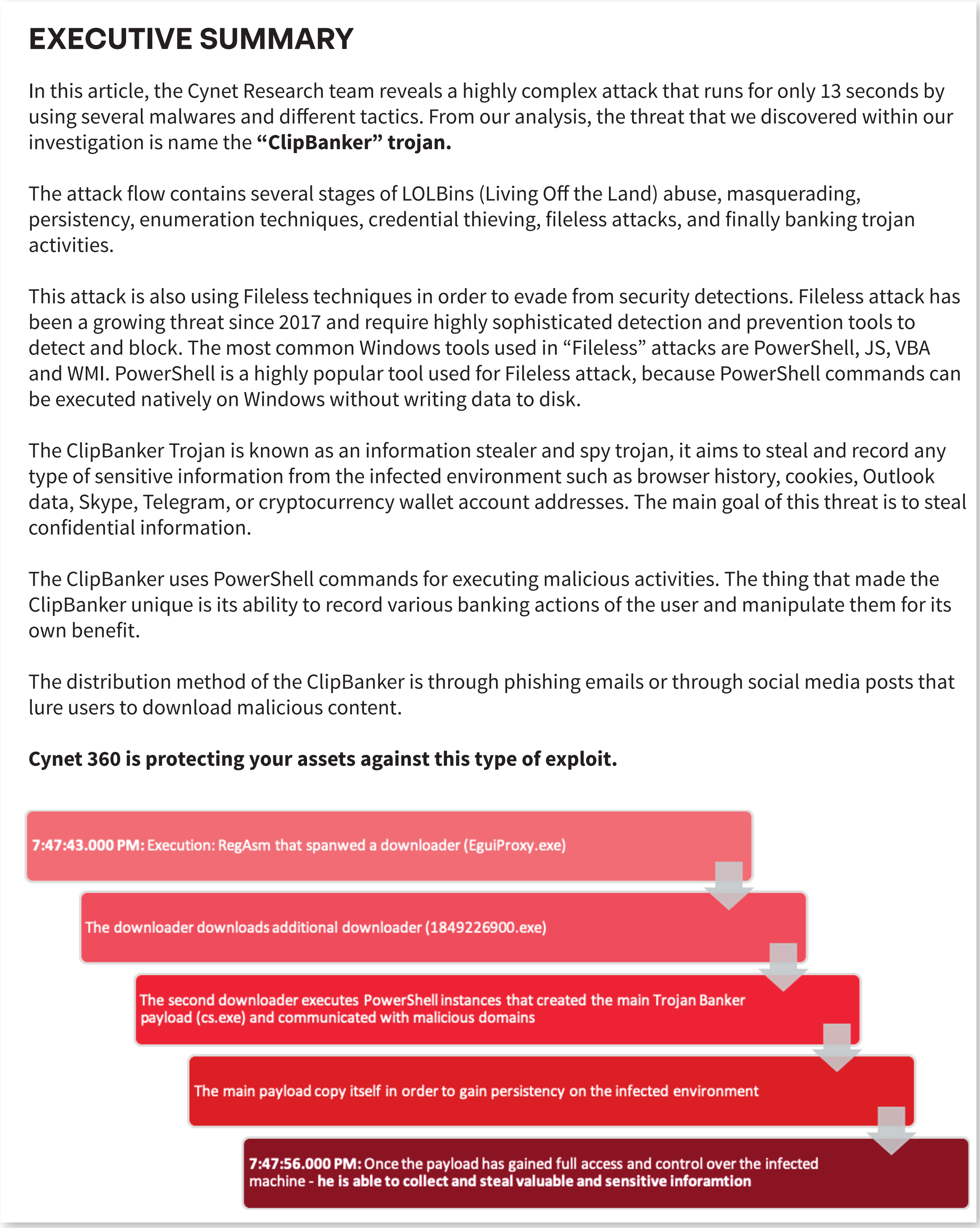
The CyOps IR experts work in close partnership with the affected company to resolve incidents as fast as possible. Their process includes creating customized policies within the Cynet 360 AutoXDR™ platform to scope and analyze the threat as well as providing recommendations and mitigations on the endpoint and across the IT and security environment.

Attack Reports

The CyOps teams generates comprehensive reports in response to client questions.

Attack Reports Example 1: 13 Seconds Attack

The Cynet Threat Research Report contains an executive level summary, analysis description including involved processes, and associated indicators of compromise, on the "13 Seconds Attack" where malware compromises a single host within 13 seconds.



EXECUTIVE SUMMARY

In this article, the Cynet Research team reveals a highly complex attack that runs for only 13 seconds by using several malwares and different tactics. From our analysis, the threat that we discovered within our investigation is name the **"ClipBanker" trojan.**

The attack flow contains several stages of LOLBins (Living Off the Land) abuse, masquerading, persistency, enumeration techniques, credential thieving, fileless attacks, and finally banking trojan activities.

This attack is also using Fileless techniques in order to evade from security detections. Fileless attack has been a growing threat since 2017 and require highly sophisticated detection and prevention tools to detect and block. The most common Windows tools used in "Fileless" attacks are PowerShell, JS, VBA and WMI. PowerShell is a highly popular tool used for Fileless attack, because PowerShell commands can be executed natively on Windows without writing data to disk.

The ClipBanker Trojan is known as an information stealer and spy trojan, it aims to steal and record any type of sensitive information from the infected environment such as browser history, cookies, Outlook data, Skype, Telegram, or cryptocurrency wallet account addresses. The main goal of this threat is to steal confidential information.

The ClipBanker uses PowerShell commands for executing malicious activities. The thing that made the ClipBanker unique is its ability to record various banking actions of the user and manipulate them for its own benefit.

The distribution method of the ClipBanker is through phishing emails or through social media posts that lure users to download malicious content.

Cynet 360 is protecting your assets against this type of exploit.

7:47:43.000 PM: Execution: RegAsm that spanwed a downloader (EguiProxy.exe)

The downloader downloads additional downloader (1849226900.exe)

The second downloader executes PowerShell instances that created the main Trojan Banker payload (cs.exe) and communicated with malicious domains

The main payload copy itself in order to gain persistency on the infected environment

7:47:56.000 PM: Once the payload has gained full access and control over the infected machine - **he is able to collect and steal valuable and sensitive inforamtion**

Advanced CyOps Services

Monthly Threat Intelligence Report

A detailed report on the highest-severity threats detected by Cynet360 agents deployed across our client environments around the globe. The comprehensive report includes a summary of trends and highlights, as well as activities and best practices recommendations to enhance your cyber-awareness.

CyOps Dedicated Analyst

An experienced CyOps analyst assigned to personally oversee your account and services and be your single point of contact for Cynet. Beyond the 24/7 proactive monitoring you automatically receive from the CyOps team, the dedicated analyst is focused on your environment and needs.

Advanced Incident Response Service Retainer

An umbrella of advanced response capabilities that extend beyond the environment protected by the Cynet AutoXDR™ platform. With the Cynet Advanced IR Retainer, the Cynet IR team is prepared to hit the ground running 24/7 in the event of a breach anywhere in your environment to quickly eliminate threats and get your business back on track.

Third Party Integrations

Integrating Cynet with your existing security technologies and related infrastructure is easy. Cynet Integration engineers can develop integrations for most technologies with the Cynet 360 AutoXDR™ platform using common scripting languages and a RESTful API, including technologies such as SIEM, ticketing, case management, firewall, and much more.

OS SUPPORT

WINDOWS (32/64 BIT)

- Windows XP SP3 and above
- Windows Vista SP1 and above
- Windows 7 SP1 and above
- Windows 8 & 8.1
- Windows 10
- Windows 11
- Windows Embedded/Industrial/IoT
- Windows Server 2003 SP2
- Windows Server 2008 / R2
- Windows Server 2012 / R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

LINUX (32/64 BIT)

- Red Hat 7+
- Fedora 23+
- Ubuntu 16.04+
- CentOS 6.9+
- SUSE 12.0+
- Debian 9.0+
- Oracle Enterprise Linux 7.6+
- Amazon Linux 1 & 2
- AlmaLinux 8.5+

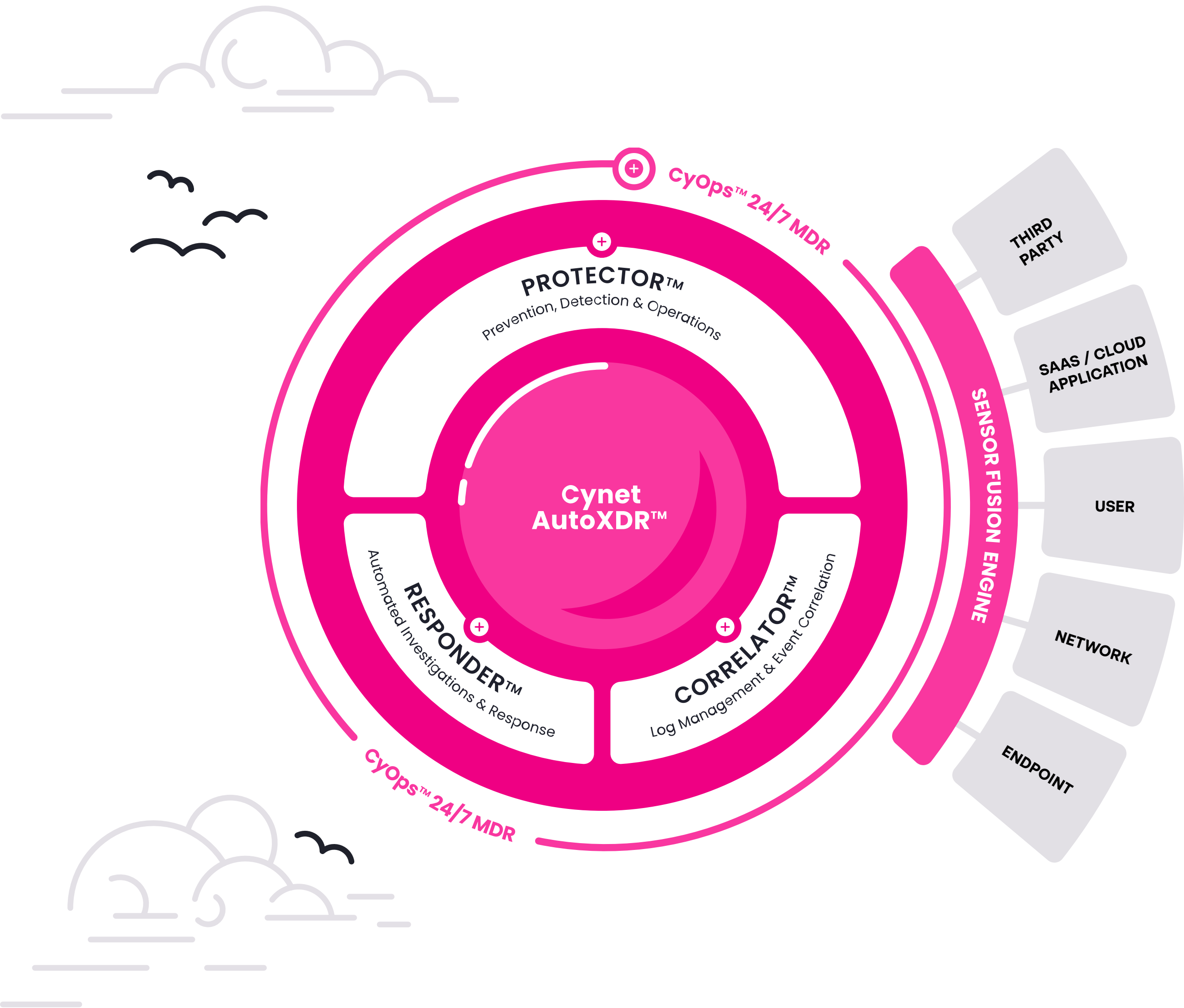
MAC (64 BIT)

- macOS High Sierra
- macOS Mojave
- macOS Catalina
- macOS Big Sur
- macOS Monterey
- macOS Ventura
- (Apple Silicon M1 & M2)

ABOUT US

Cynet's end-to-end, natively automated XDR platform, backed by a 24/7 MDR service was purpose-built to enable lean IT security teams to achieve comprehensive and effective protection regardless of their resources, team size, or skills.

Cynet delivers the prevention and detection capabilities of EPP, EDR, NDR, Deception, UBA rules, and CSPM, together with alert and activity correlation and extensive response automation capabilities.



Our vision is to enable security teams to put their cybersecurity on autopilot and focus their limited resources on managing security rather than operating it.

Bring sanity back to cybersecurity with a fresh approach that makes protecting your organization easy and stress-less.