

CYNET 360 - PROTEZIONE AUTONOMA CONTRO LE COMPROMISSIONI

XDR E AUTOMAZIONE DELLA RISPOSTA IN UN'UNICA
PIATTAFORMA SUPPORTATA DA SERVIZI 24*7 (MDR)
SEMPRE ATTIVI

Introduzione

Diversi strati di difesa sono costosi e complessi da gestire per le squadre di sicurezza di piccole dimensioni. Per far fronte a un numero crescente di minacce avanzate, sono costretti ad adottare numerose tecnologie per prevenire future violazioni.

Di conseguenza, devono confrontarsi con una serie di problemi:

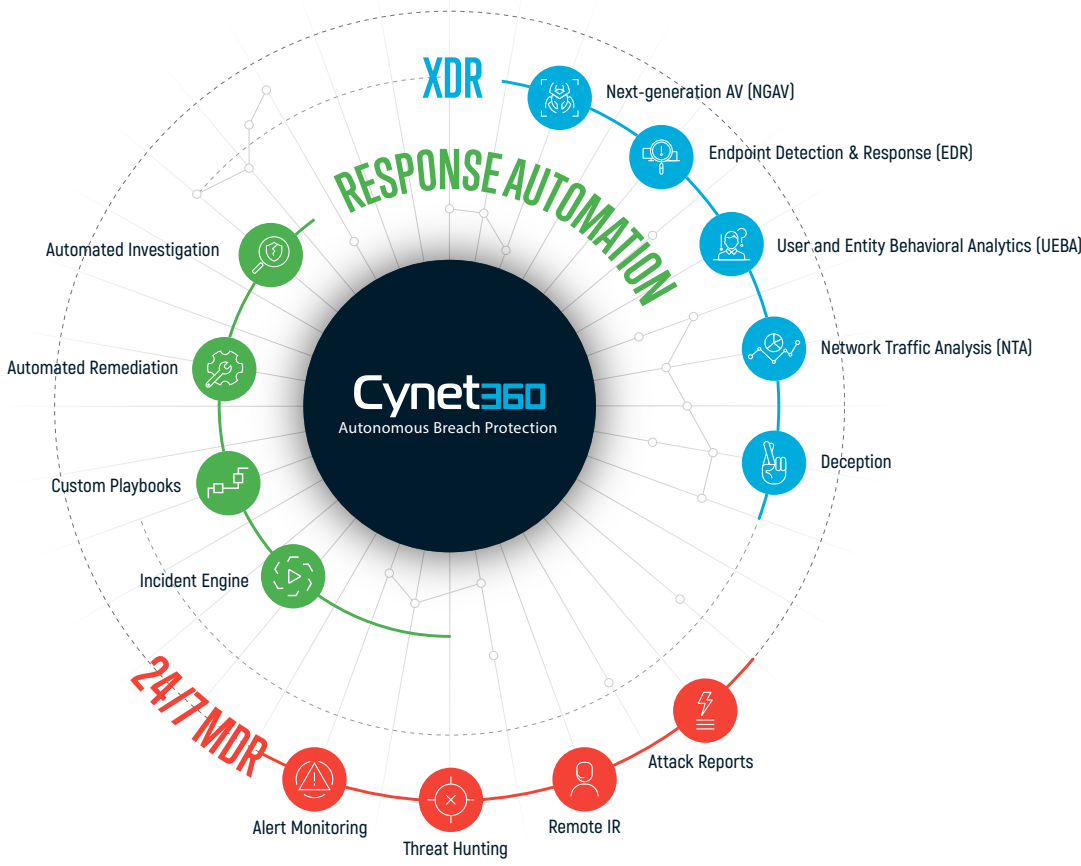
- **Distribuzione:** è complesso integrare prodotti diversi non predisposti per la loro interoperazione.
- **Stack di sicurezza inefficiente e inefficace:** tecnologie non sinergiche comportano sia sovrapposizioni che punti ciechi.
- **Flussi di lavoro manuali:** le tecnologie di protezione contro compromissioni e violazioni dei dati richiedono uno sforzo operativo manuale che, per definizione, non permette di scalare e gestire un numero significativo di allarmi operation that, by definition, cannot scale to the volume of generated alerts.
- **Insieme di competenze specifiche:** mancano le conoscenze necessarie a operare e mantenere queste tecnologie in modo efficiente. Di conseguenza, la sicurezza IT rimane fuori dalla portata della maggior parte delle organizzazioni.

Gli stack di sicurezza sono un tormento per la maggior parte dei gruppi di sicurezza. Il motivo per cui si aggiungono tecnologie è proteggere l'organizzazione. Tuttavia, sovrapporre tecnologie non integrate porta a una gestione inefficiente delle stesse e alla conseguente mancanza di una protezione adeguata.



Piattaforma Cynet 360 per la protezione autonoma dalle violazioni

Cynet combina nativamente tre funzionalità in un'unica soluzione unificata: capacità estese di rilevamento e risposta (XDR), automazione della risposta e servizi di rilevamento e risposta gestiti (MDR) 24 ore su 24, 7 giorni su 7. Con Cynet 360, anche i gruppi di sicurezza più piccoli avranno a disposizione una soluzione efficace contro minacce complesse.



La soluzione XDR di Cynet fornisce un'unica piattaforma per prevenire, rilevare, diagnosticare e correggere una vasta gamma di vettori d'attacco. La visibilità su endpoint, rete e attività degli utenti, potenziata della Deception Technology (tecnologia dell'inganno), fornisce la più ampia e profonda protezione contro ogni tipo di minaccia.

Cynet 360 implementa una diagnostica automatizzata di tutti gli avvisi riguardanti gli endpoint, gli utenti o la rete che consente di rivelarne la causa e la portata, applicando le misure correttive necessarie per eliminare completamente la minaccia.

Incident View

INCIDENT NAME
Unauthorized Memory Access Attempt

INCIDENT STATUS
Autonomous Response Concluded

TIME TO RESOLUTION
00:05:14

DESCRIPTION	IMPACT	ROOT CAUSE	REMEDIATION	FURTHER ACTIONS	SUMMARY
Cynet blocked procdump.exe attempt to dump passwords from lsass.exe	• 3 hosts	• Compromised host: Lab-Client1		• Disable 1 user accounts	• 5 investigation steps • 1 remediation actions

Autonomous Responder

Incident Artifacts

INVESTIGATION

lab-client2 is compromised

Find malicious execution...

Get user account

lab-client2

Executed remotely

lab\admin...

Lab-Client1 is internal

Get Lab-Client1 unique c...

34 unique connections found

Get all hosts where lab\admin...

1 hosts

Lab-client1

Compromised hosts: 1

Root cause: Lab-Client1

Isolation applied on all hosts

Isolate Lab-Client1

Isolate lab-client2

Disable lab\admin...

REMEDIATION

via UI

Timeline

11:15:04 30/10/2020
Hostname is validated as compromised and controlled by attacker

11:15:04 30/10/2020
FINDING IMPACT
lab-client2 is compromised

11:15:04 30/10/2020
REMEDIATION ACTION
Isolate lab-client2 from the environment

11:15:04 30/10/2020
INVESTIGATION QUERY IMPACT
Check from which machine procdump.exe was executed

11:15:04 30/10/2020
INVESTIGATION QUERY IMPACT
Check the name of the compromised user account

11:15:04 30/10/2020
INVESTIGATION RESULT IMPACT
The compromised user account is lab\administrator

11:15:04 30/10/2020
REMEDIATION ACTION
Disable compromised user account lab\administrator on lab-client2

11:15:04 30/10/2020
INVESTIGATION QUERY IMPACT
Check if lab\administrator has logged in to additional hosts

Incident Artifacts

ALERTS

CLICK TO SEE ALL ALERTS

LABADMIN...

LAB-CLIENT2

WININIT.EXE

SERVICES.EXE

PSXSVC.EXE

CMD.EXE

PROCDUMP.EXE

LSASS.EXE

Cynet fornisce, inoltre, un'ampia gamma di azioni di correzione automatizzate e altamente personalizzabili per gestire le minacce secondo le proprie preferenze.

Per di più, Cynet mette a disposizione un gruppo di esperti di Cybersecurity – disponibile 24 ore su 24, 7 giorni su 7 e incluso nella piattaforma Cynet 360 – per potenziare e guidare la squadra del cliente.

ULTERIORI INFORMAZIONI

XDR - Soluzioni estese di prevenzione e risposta

La soluzione XDR di Cynet combina in modo nativo diverse funzionalità preconfigurate di prevenzione e rilevamento, fornendo così un'impeccabile protezione multi-livello agli operatori, che risparmiano tempo e fatica nell'acquisto, nell'integrazione e nella gestione di soluzioni eterogenee.

Visualizzazione degli avvisi in Cynet 360

La piattaforma consente di ottenere una visione immediata dello stato delle minacce in tutto l'ambiente.



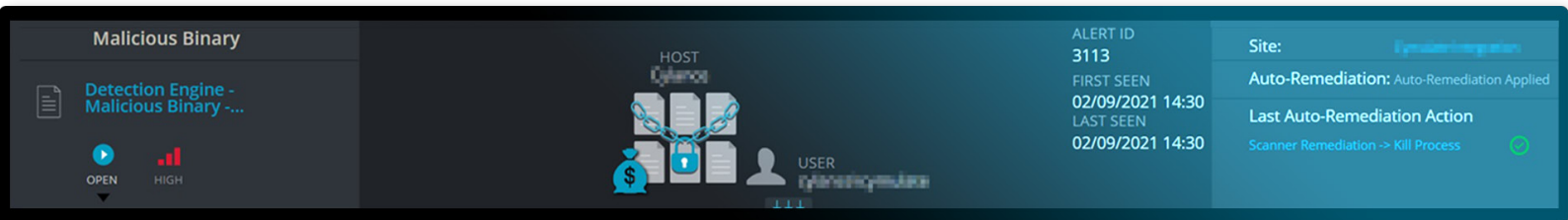
Antivirus di ultima generazione (NGAV)

Esegue la scansione di file attivi e inattivi per proteggerli da malware noti.

- Protezione da malware basata sull'intelligenza artificiale (IA)
- Protezione da malware derivante dall'analisi statica basata sull'intelligenza artificiale
- Protezione da exploit basata sul comportamento
- Protezione dall'esecuzione di script, macro e minacce fileless basata sul comportamento

Esempio di avviso 1: Avviso di file binario dannoso

La protezione da malware basata sull'IA di Cynet blocca l'esecuzione di un file con codice binario dannoso.



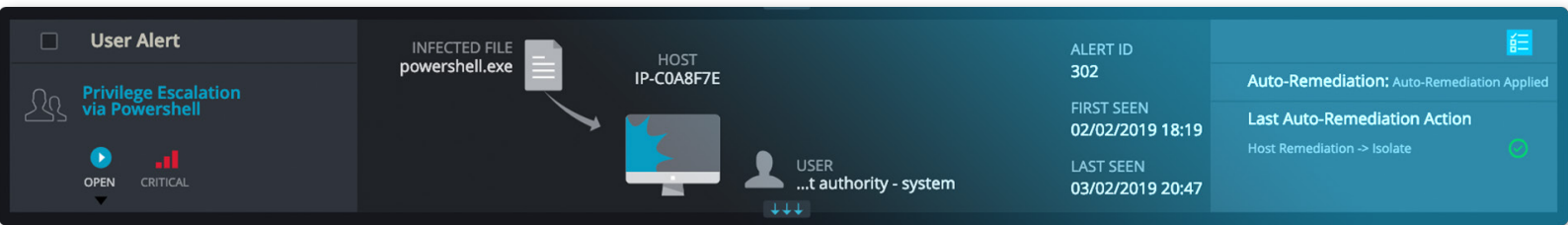
EDR

Analizza il comportamento per rilevare i processi e le applicazioni non autorizzati attraverso vari meccanismi, tra cui:

- Scansione SSDEEP: utilizza un algoritmo di compressione che ricerca analogie con malware conosciuti (si parla anche di fuzzy fingerprints). Una tecnica che rileva il riutilizzo degli strumenti esistenti solitamente trasparente alle soluzioni tradizionali basate su firma.
- Banchi di memoria (Memory Patterns): analizza la memoria caricata da un host per rilevare processi: cerca schemi di attività, struttura e comportamento, dati con stringhe sospette e analogie con malware noti, attività e processi che caricano in memoria DLL pericolose per accedere ad aree sensibili del sistema operativo o per intercettare altri processi.
- Tecnologia avanzata di rilevamento (ADT – Advanced Detection Technology): insieme di strumenti euristici per ispezionare i sistemi operativi alla ricerca di comportamenti dannosi eseguiti da malware e minacce basate su file o senza file. Questi strumenti rilevano le attività malevoli nei processi di sistema come PowerShell o cmd. ADT analizza la struttura di un comando, i risultati e la connessione tra il comando e il processo padre alla ricerca di comportamenti dannosi come l'esecuzione di un comando PowerShell da parte, per esempio, di un file WinWord.
- Modalità driver (kernel): consente di acquisire visibilità sulle minacce a livello di kernel. Questo meccanismo impedisce, inoltre, che Cynet Endpoint Protection Scanner (EPS) venga terminato. I meccanismi di difesa includono sistemi antimanomissione, compresa la protezione dei processi Cynet dall'interruzione o dalla manipolazione, la protezione da scrittura in aree sensibili del sistema operativo e l'accesso a risorse critiche di sistema come LSASS.

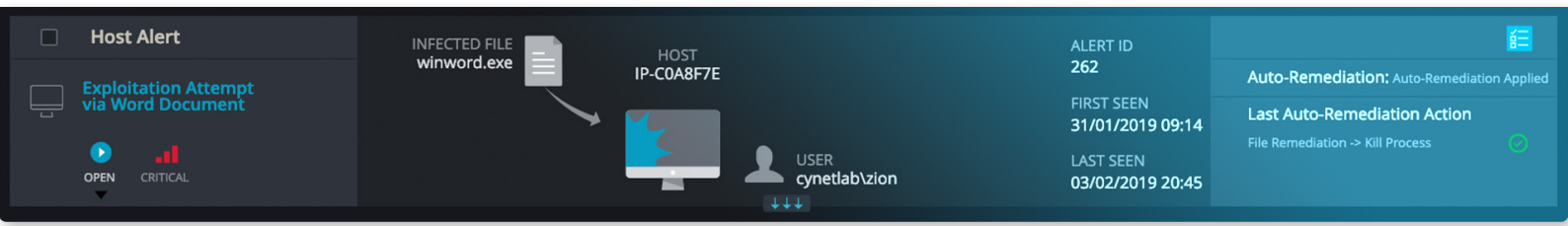
Esempio di avviso 2: Escalation dei privilegi

Cynet rileva PowerShell, un processo amministrativo legittimo, e gli impedisce di eseguire un'escalation dei privilegi utente.



Esempio di avviso 3: Protezione da exploit

Cynet rileva e blocca un documento Word predisposto per eseguire un exploit.



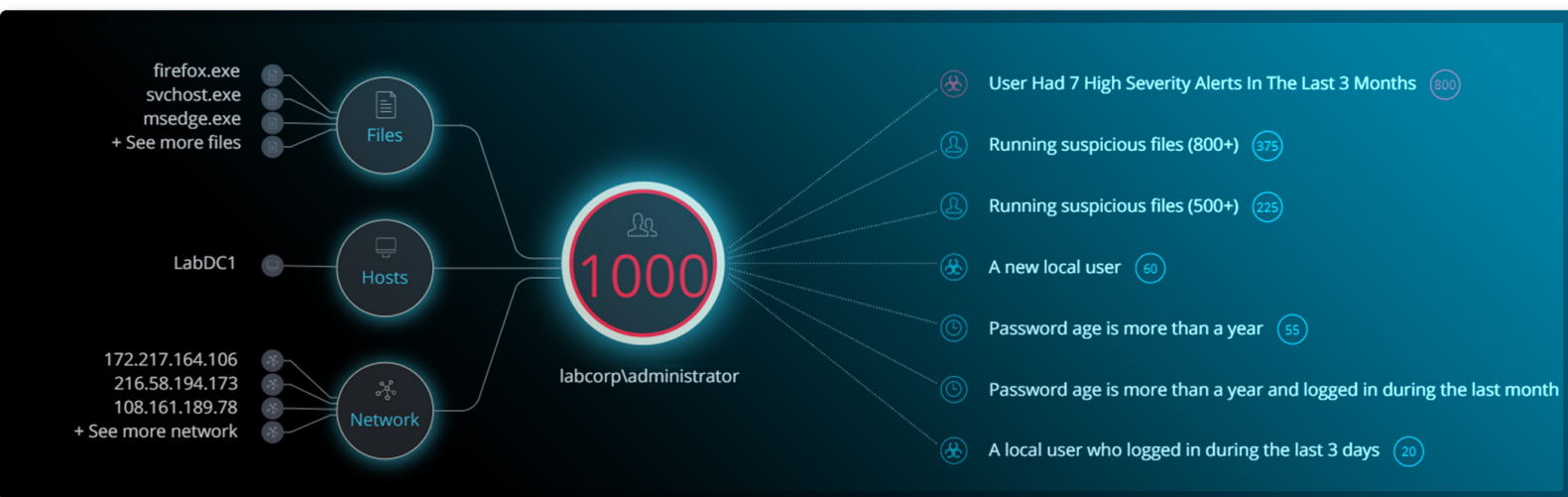
Analisi del comportamento degli utenti e delle entità (UEBA)

Apprende il comportamento degli utenti e delle entità e avvisa in caso di attività anomale. Questa funzione include:

- Monitoraggio in tempo reale di tutte le interazioni avviate dagli utenti
- Host a cui accedono gli utenti, numero di postazioni, posizione e frequenza
- Comunicazione di rete interna ed esterna
- File aperti dagli utenti
- Processi eseguiti

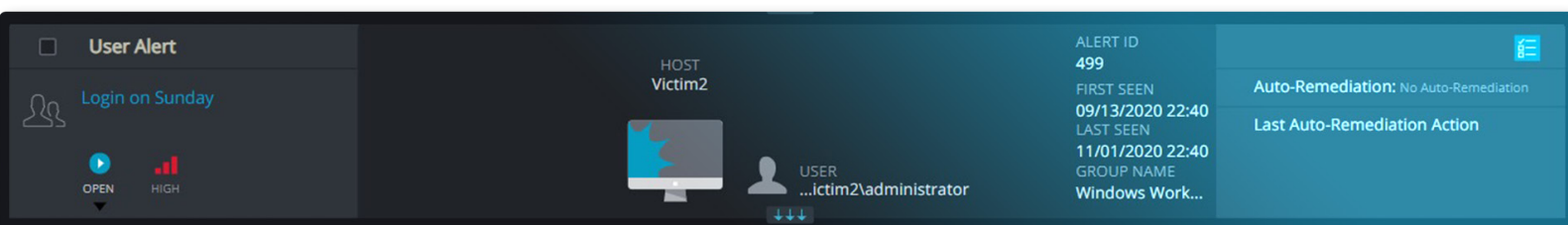
Esempio di analisi forense 4: Comportamento dell'utente

L'analisi forense di Cynet mostra un comportamento utente altamente sospetto correlando varie attività anomale.



Esempio di avviso 5: Accesso di domenica

Il componente UEBA di Cynet rileva attività anomale di accesso durante il fine settimana.



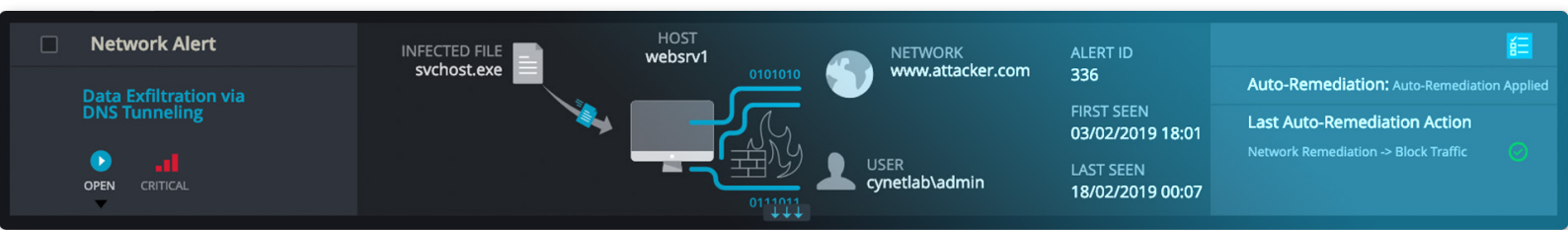
Analisi del traffico di rete

Analizza le attività per rilevare gli attacchi alla rete, tra cui:

- Furto di credenziali basato sulla rete (ARP spoofing, DNS responder)
- Movimento laterale sulla rete
- Comunicazioni in uscita dannose (C2C, phishing)
- Ricognizione della rete (scansione delle porte)
- Esfiltrazione di dati (tunneling tramite vari protocolli)

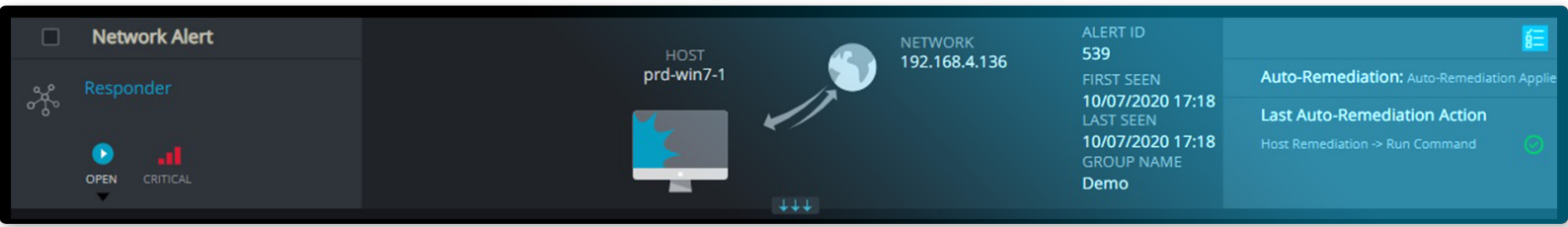
Esempio di avviso 6: Esfiltrazione di dati

Questo avviso rileva una fase avanzata all'interno della kill chain di attacco, in cui l'attaccante ha ottenuto l'accesso ai dati e tenta di esfiltrarli mascherandoli come traffico DNS legittimo.



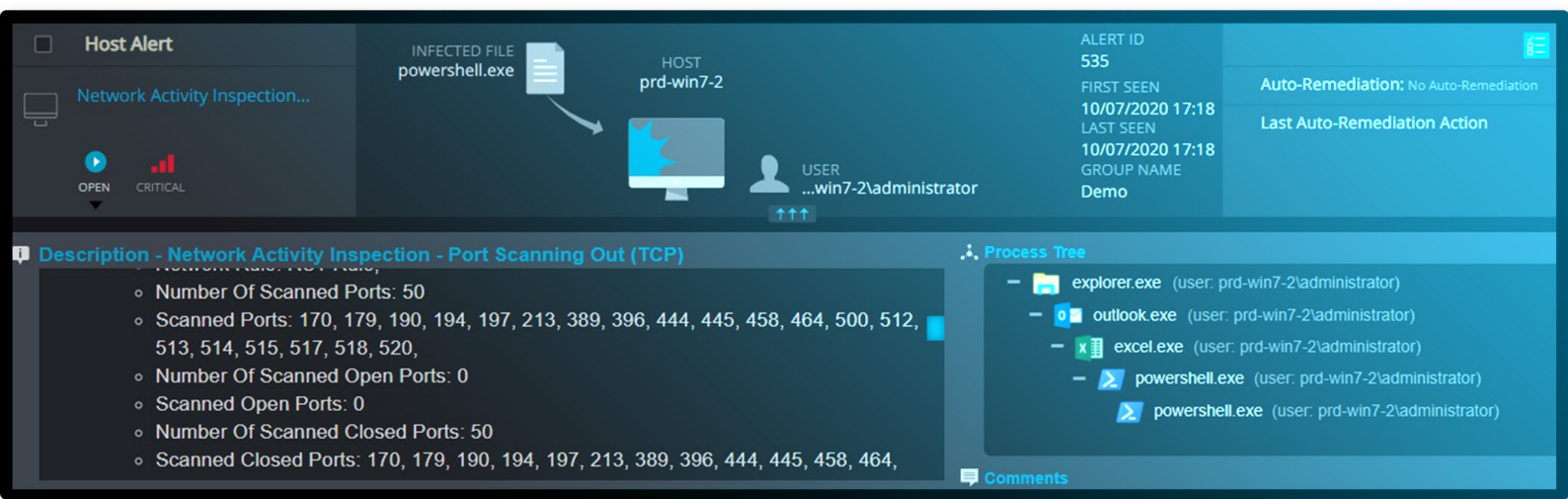
Esempio di avviso 7: Responder

Cynet rileva e blocca malware di tipo Responder che sfrutta alcuni protocolli di rete.



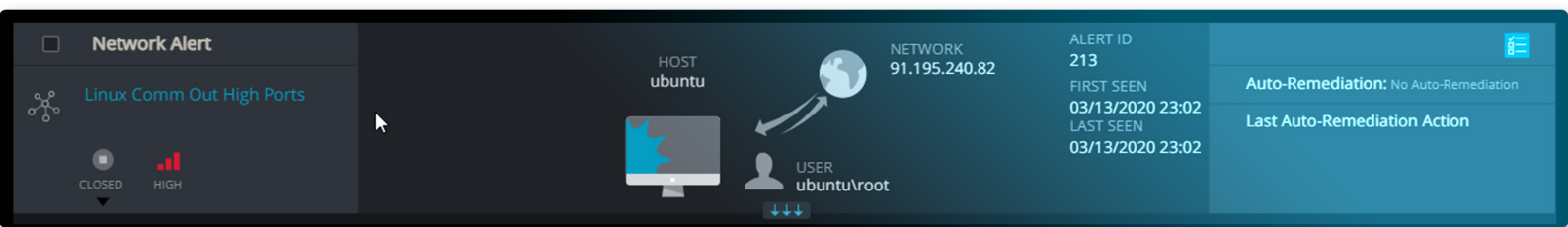
Esempio di avviso 8: Scansione delle porte

Cynet ha rilevato che un host ha iniziato a eseguire una scansione di una porta sulla rete.



Esempio di avviso 9: Comunicazione in uscita da porte di rete in un intervallo alto

Una macchina basata su Linux ha eseguito attività sospette come root utilizzando porte di intervallo elevato.



Deception (inganno)

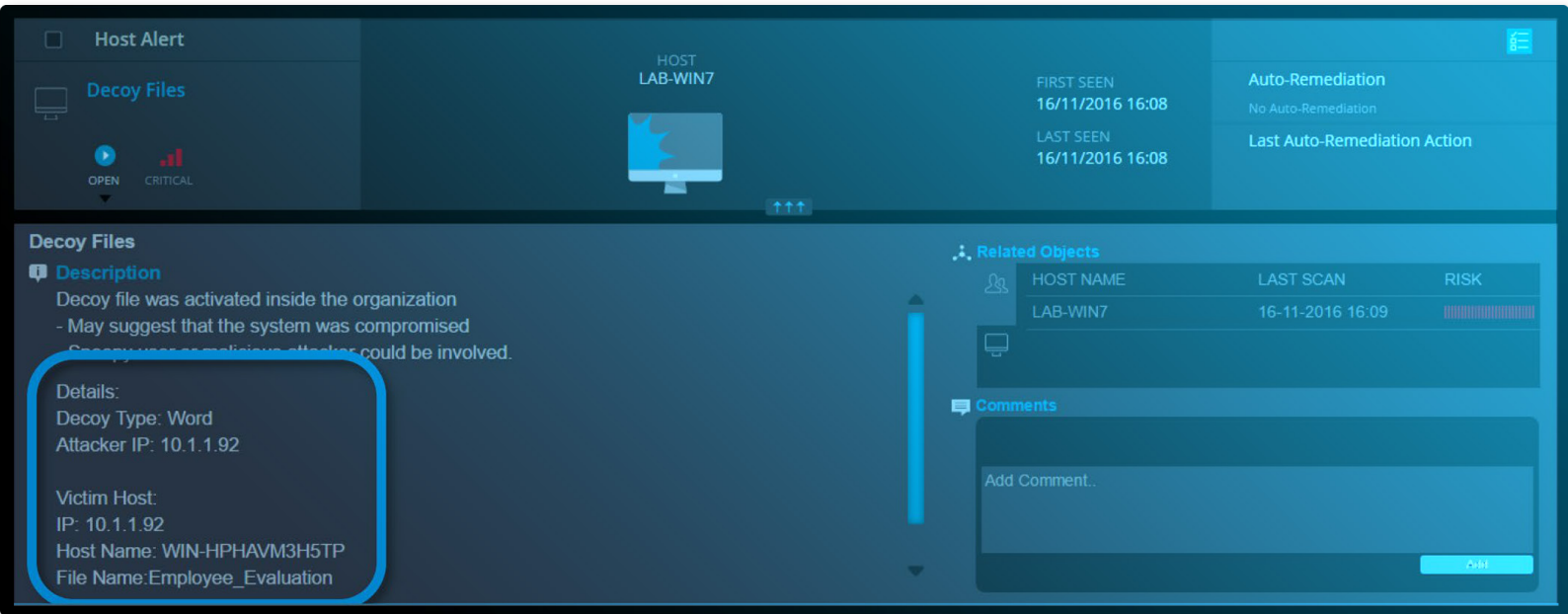
Utilizzando tattiche di tipo honeypot, Cynet colloca speciali esche nell'ambiente e le monitora per attirare, rilevare e notificare i tentativi di attacco.

Gli avvisi vengono generati nel momento in cui vengono attivate alcune esche:

- Ransomware
- File sospetti
- Utenti
- Reti

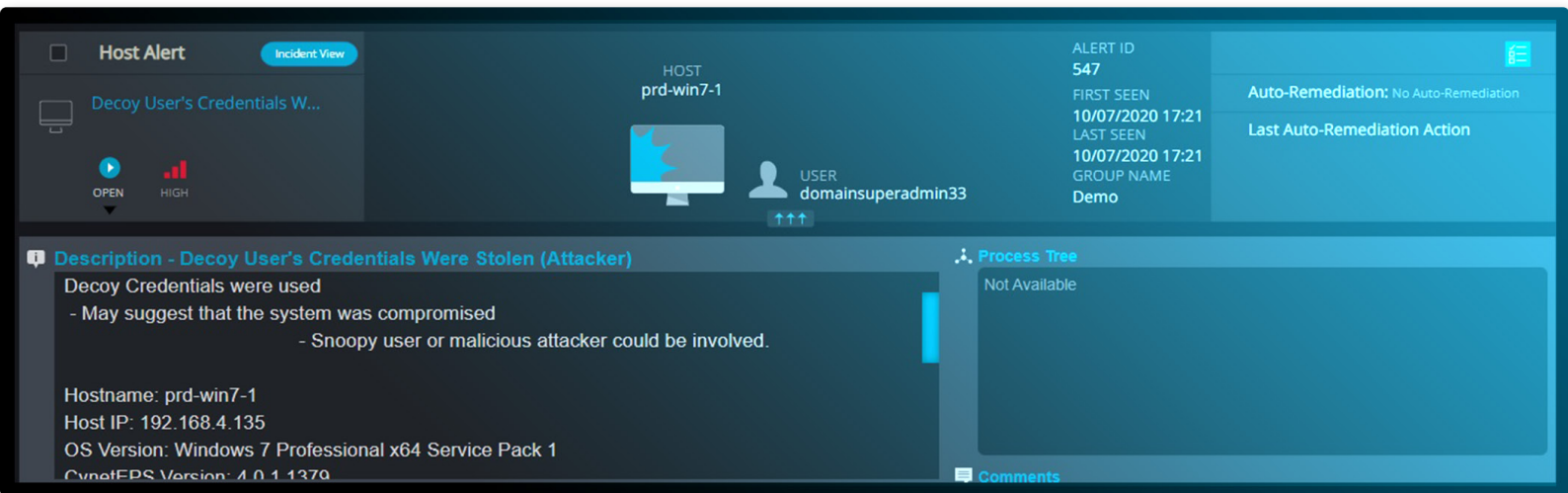
Esempio di avviso 10: Deception (file)

L'attaccante è stato indotto a rivelare la propria presenza attraverso un file di Word piazzato intenzionalmente come esca.



Esempio di avviso 11: Deception (utenti)

L'attaccante è stato indotto a rivelare la propria presenza tentando di autenticarsi come utente esca.



Controllo del dispositivo

Rilevamento e blocco di dispositivi esterni collegati all'endpoint (ad esempio, un dispositivo USB o una scheda SD).

Esempio di avviso 12: Avviso di un dispositivo di archiviazione collegato

Rilevamento e blocco di un dispositivo di archiviazione collegato che non rispetta le politiche di sicurezza.

The screenshot displays the Cynet 360 Alerts interface. At the top, there's a navigation bar with icons for ALL, FILES, USERS, NETWORK, and HOSTS, along with a search bar and buttons for CHANGE STATUS and ACTIONS. Below this is a table header for alerts with columns: Select Alert Name, Alert ID, Severity, Alert Status, Host Name, File Name, User Name, Network, Scan Group, and Alert Date. The table shows one alert with ID 16, Severity HIGH, and Status OPEN. The host name is shaik-lp. The alert description is 'Insertion of Storage Device Detected (Blocked)'. The interface also shows a 'Device Control' section with a USB icon and a 'Process Tree' section which is currently 'Not Available'. A 'Recommendation' section at the bottom provides instructions on how to handle the incident.

Alerts

ALL FILES USERS NETWORK HOSTS Search CHANGE STATUS ACTIONS

Select Alert Name	Alert ID	Severity	Alert Status	Host Name	File Name	User Name	Network	Scan Group	Alert Date
☐	16	SEVERITY	OPEN	shaik-lp					From To

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

Device Control

Insertion of Storage Device ...

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

Process Tree

Not Available

Recommendation

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

Comments

Automazione della risposta

Cynet automatizza completamente l'intero flusso delle attività in caso di allerta, eliminando gli sforzi manuali e garantendo l'esecuzione di importanti azioni e misure di risposta.

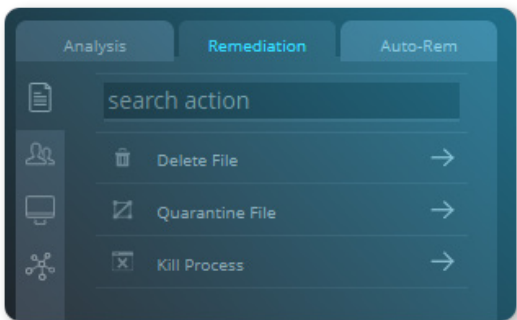
Le allerte sono raggruppate in incidenti in modo logico, riducendone la difficoltà di gestione e fornendo il contesto della minaccia. Le azioni comprendono:

- **Diagnostica.** Analisi automatizzata della causa e dell'impatto
- **Risultati.** Informazioni sull'origine dell'attacco e sulle entità interessate
- **Correzione.** Eliminazione della presenza, delle attività e dei manufatti di tutti gli attacchi contro gli utenti, la rete e gli endpoint.

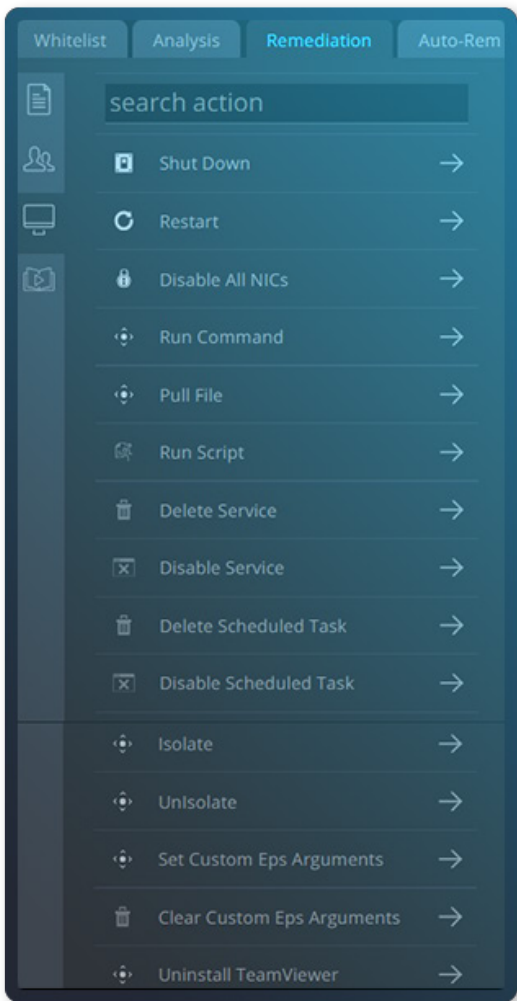
Azioni di correzione preimpostate

Cynet fornisce la più ampia gamma di strumenti di correzione disponibili per host infetti, file dannosi, account utente compromessi e traffico controllato da un utente malintenzionato.

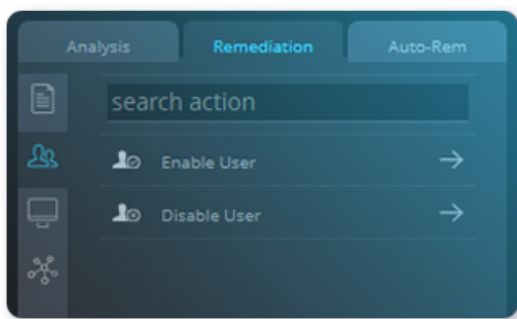
File



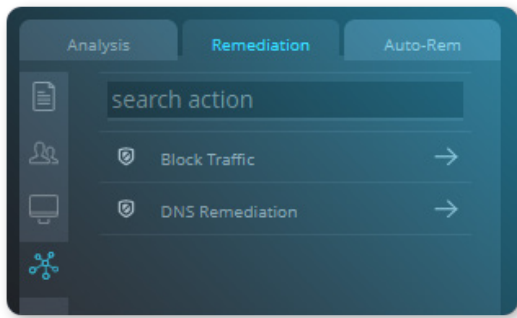
Host



Utente



Rete

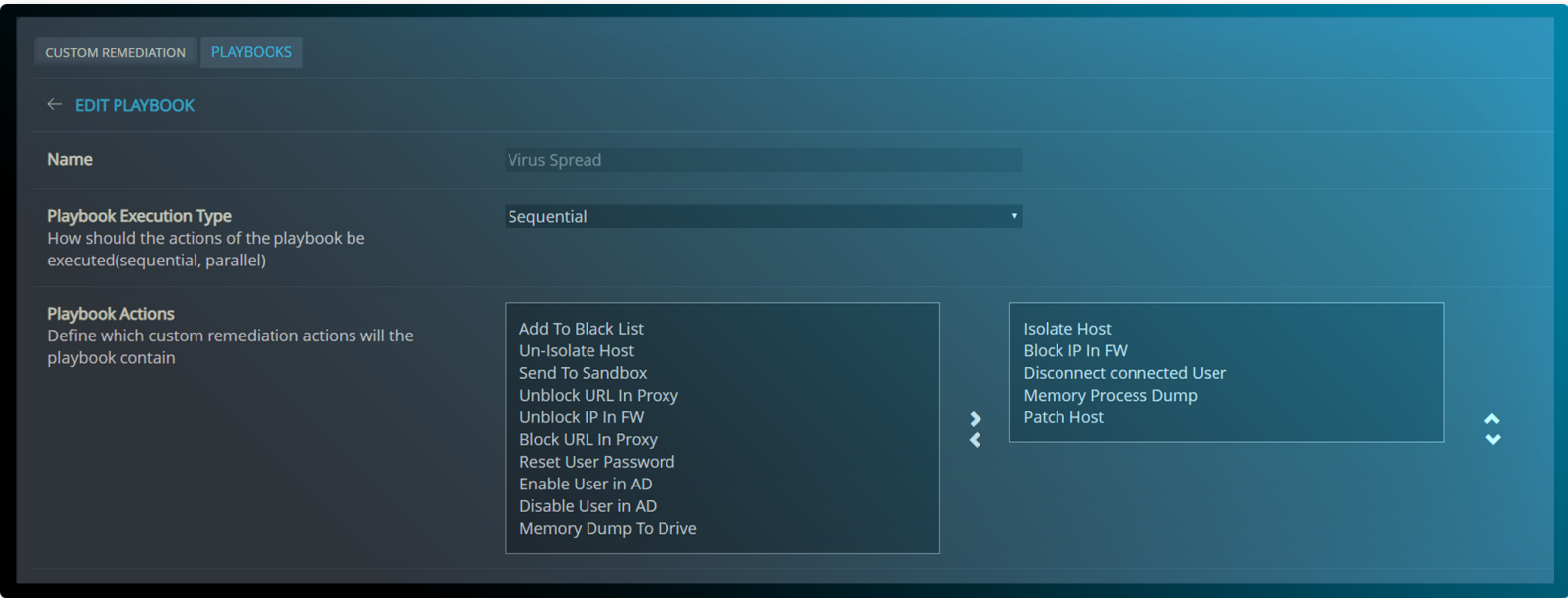


Playbook di correzione (remediation)

I playbook concatenano molteplici azioni di correzione. Questo consente alle squadre di sicurezza di scalare la propria capacità di gestione delle allerte eliminando le attività ripetitive e aumentando considerevolmente il numero di attacchi gestiti e risolti autonomamente da Cynet 360 senza necessità di intervento umano.

Cynet 360 fornisce un'ampia gamma di azioni correttive e supporta la possibilità di creare o modificare i propri playbook.

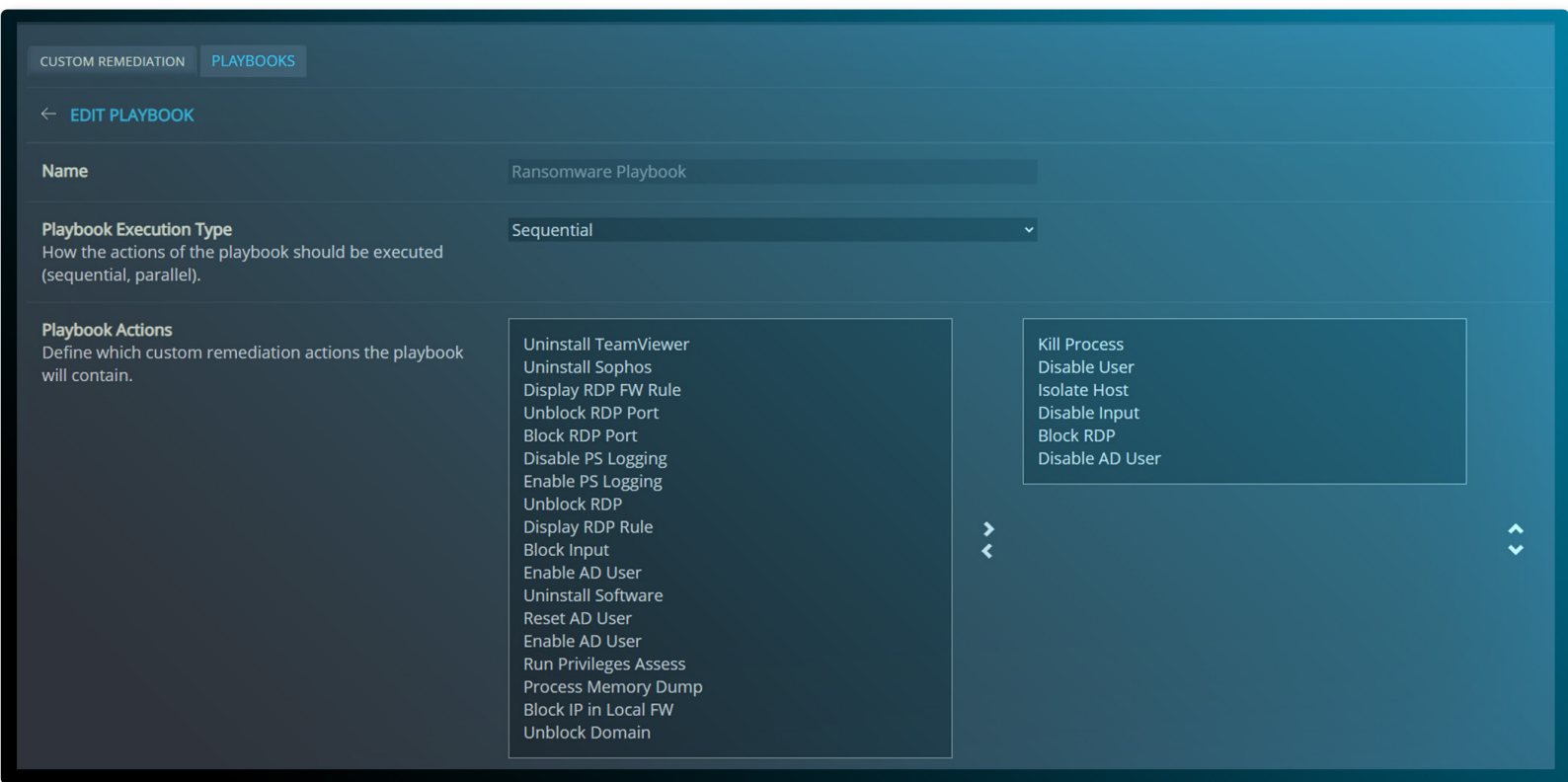
Esempio di playbook 1: Diffusione di virus



In questo playbook personalizzato, le azioni di correzione visualizzate vengono eseguite automaticamente, in parallelo, per impedire al malware di propagarsi da un computer all'altro.

Esempio di playbook 2: Modifica di un playbook

Modificare il playbook è semplice: è possibile aggiungere o modificare il flusso attraverso un semplice menù di trascinamento.



Correzione automatica

Cynet 360 consente di eseguire automaticamente un playbook integrato o personalizzato su un avviso specifico.

The screenshot shows the 'Remediation' tab in the Cynet 360 interface. It contains the following fields and options:

- Rule Name:** Attempt To Terminate Cyn
- Description:** Hostname: shaik-lpHost IP
- Priority:** 1
- Matching:**
 - Alert Name:** Attempt To Terminate Cyn
 - Hosts Groups:** ☒ Apply on All Hosts Groups
 - Alerts Severity:** All selected (5)
- File:** ☒
 - Hash:** 0AF6B3F8628E38B1551EC
 - File Name:** taskmgr.exe
- User:** ☐
- Network:** ☐
- Hosts to Match:** (expandable section)
- ACTION:**
 - ☒ Remediation Actions
 - ☐ PlayBook Actions
 - Remediation Type:** File Remediation
 - Action:** Quarantine File
- Save** button

Motore di risposta agli incidenti

Funzionalità esclusiva di Cynet, il motore di risposta agli incidenti mostra le azioni di risposta automatiche disposte visivamente in sequenza cronologica per una comprensione immediata dell'attacco, dalla causa principale e dalla portata fino alla sua risoluzione.

Il motore inizia formulando una serie di domande per determinare la causa principale e la portata dell'attacco. Ottenute le risposte, è in grado di adottare misure automatizzate per rispondere alla minaccia e risolverla. La cronologia visiva mostra tutte le azioni correttive che sono state adottate per rimuovere la minaccia stessa.

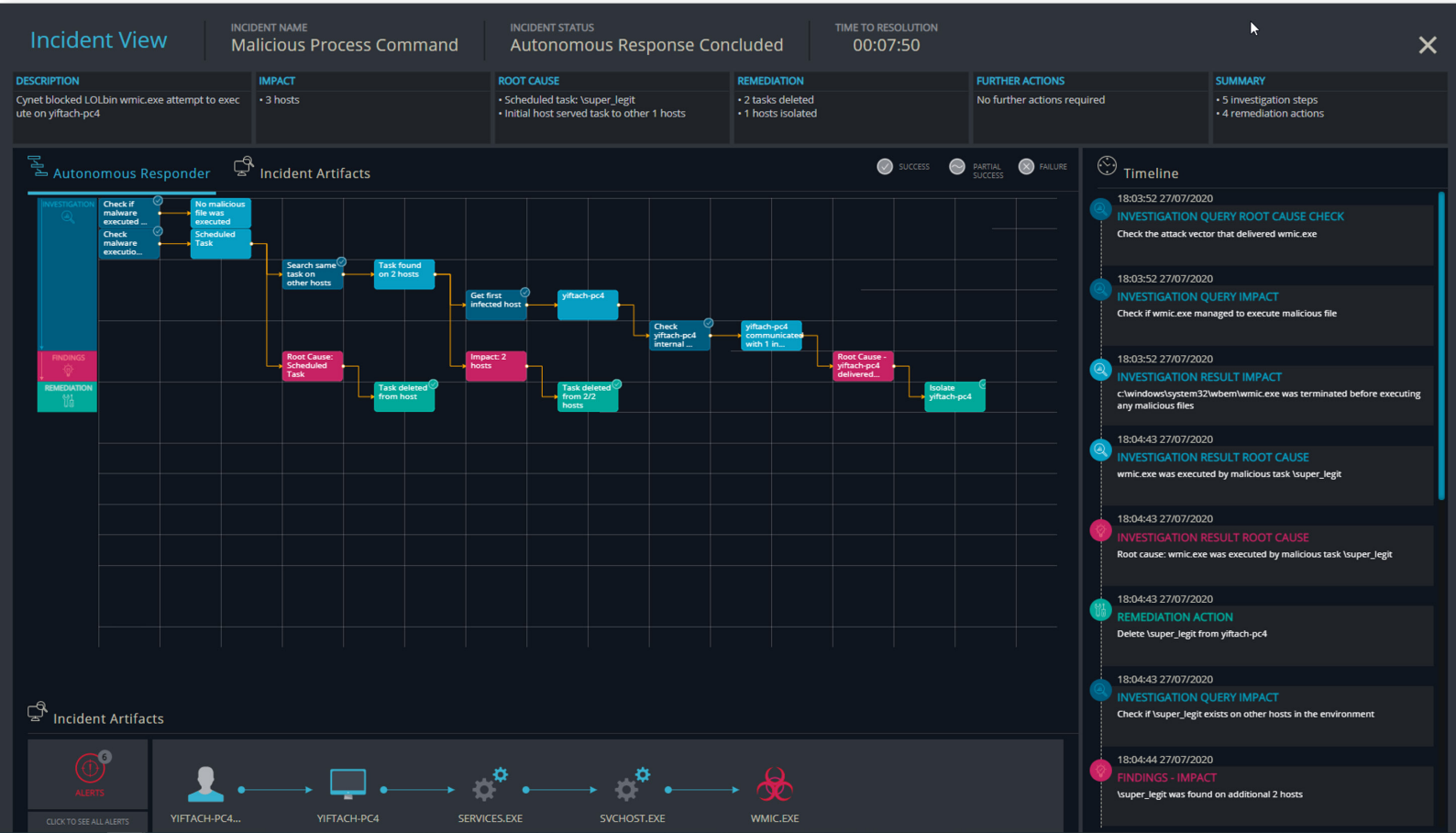
Il motore di risposta agli incidenti consente un immenso risparmio di tempo e energie. Il processo che va da un'analisi completa alla risoluzione dell'incidente richiede generalmente pochi secondi o pochi minuti.

Esempio di motore di risposta agli incidenti 1: Comando di processo dannoso

Come parte dell'indagine automatizzata, il motore di risposta agli incidenti rivela che il processo è stato terminato con sufficiente tempestività, impedendo l'esecuzione di file dannosi. Identifica, quindi, che il comando dannoso è stato eseguito per la prima volta da un'attività pianificata, sfruttata dagli attaccanti per aggirare alcuni controlli di sicurezza. Molti attaccanti installano un'attività pianificata che può rimanere inattiva anche per molto tempo, per poi iniziare a eseguire un file dannoso. In questo caso, si tratta del file wmic.exe, che porta al primo rilevamento: la causa principale è l'attività pianificata.

Il motore di risposta agli incidenti interviene immediatamente e rimuove dall'host l'attività pianificata. È importante notare che, se ci affidassimo solo al livello di prevenzione, l'attività pianificata potrebbe aver continuato a eseguire file dannosi, anche diversi, sperando che almeno uno non venisse rilevato. Il motore, tuttavia, ha eliminato la causa principale prima che si manifestassero le conseguenze.

Nell'ambito dell'indagine, il motore di risposta agli incidenti verifica se l'attività dannosa si è propagata ad altri host, difatti rileva questa attività pianificata su altri due computer. Il motore elimina automaticamente l'attività pianificata dalle due macchine. Infine, il motore identifica il primo host ad essere stato infettato: Vittima-pc4. Questa macchina ha comunicato con gli altri due host infetti, e dunque viene automaticamente isolato per scongiurare qualsiasi altro danno.



CyOps: squadra dedicata ai servizi gestiti di rilevamento e risposta in 24/7 (MDR - Managed Detect and Response)

Cynet completa la sua tecnologia di protezione autonoma contro le violazioni con servizi di sicurezza integrati senza costi aggiuntivi. CyOps è un gruppo di analisti di minacce e ricercatori di sicurezza che sfruttano le loro competenze e i numerosi feed di intelligence di Cynet per fornire servizi pregiati, rispettando le esigenze specifiche e le preferenze di sicurezza di ciascun cliente.



Monitoraggio degli avvisi

La squadra di CyOps monitora costantemente le telemetrie del cliente, ogni ora, ogni giorno, per tutto l'anno. La squadra gestisce eventi, avvisi, richieste dei clienti e incidenti; fornisce anche un'analisi degli avvisi e delle correlazioni con altri eventi segnalati da Cynet 360.

La squadra di CyOps contatterà il cliente nel caso in cui venissero rilevati determinati avvisi o eventi che richiedano azioni specifiche.

Threat Hunting

Gli analisti di CyOps ricercano continuamente le nuove minacce emergenti per creare indicatori di compromissione (IoC) e schemi ricorrenti nei meccanismi di Cynet 360. Queste azioni proattive consentono a Cynet 360 di raccogliere, analizzare e segnalare eventi, fornendo, al contempo, attraverso sofisticate funzionalità forensi, la capacità di valutare il livello di rischio di un'entità.

Risposta agli incidenti (IR) da remoto

Gli esperti di IR del gruppo di CyOps lavorano in stretta collaborazione con l'azienda interessata per risolvere gli incidenti il più rapidamente possibile. La procedura seguita comprende la creazione di politiche personalizzate all'interno di Cynet 360 per analizzare la minaccia e determinarne la portata, oltre a fornire raccomandazioni e mitigazioni sull'endpoint, nonché per tutto l'ambiente IT e relativa sicurezza.

Report sugli attacchi

Le squadre di CyOps generano report completi in risposta alle domande dei clienti.

Report di attacco, esempio 1: Attacco di 13 secondi

Il rapporto Cynet sulla ricerca della minaccia (Cynet Threat Research Report) offre una sintesi operativa e una descrizione dell'analisi – compresi i processi coinvolti e gli indicatori di compromissione associati – del cosiddetto “attacco di 13 secondi” in cui il malware compromette un singolo host nel giro di 13 secondi.

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.

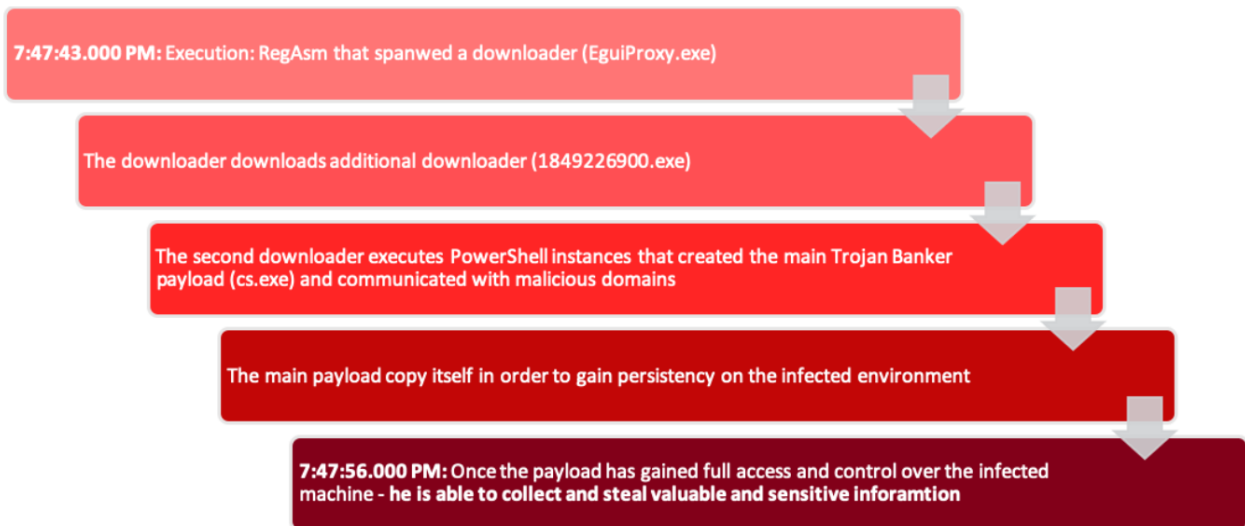
This attack is also using Fileless techniques in order to evade from security detections. Fileless attack has been a growing threat since 2017 and require highly sophisticated detection and prevention tools to detect and block. The most common Windows tools used in “Fileless” attacks are PowerShell, 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.

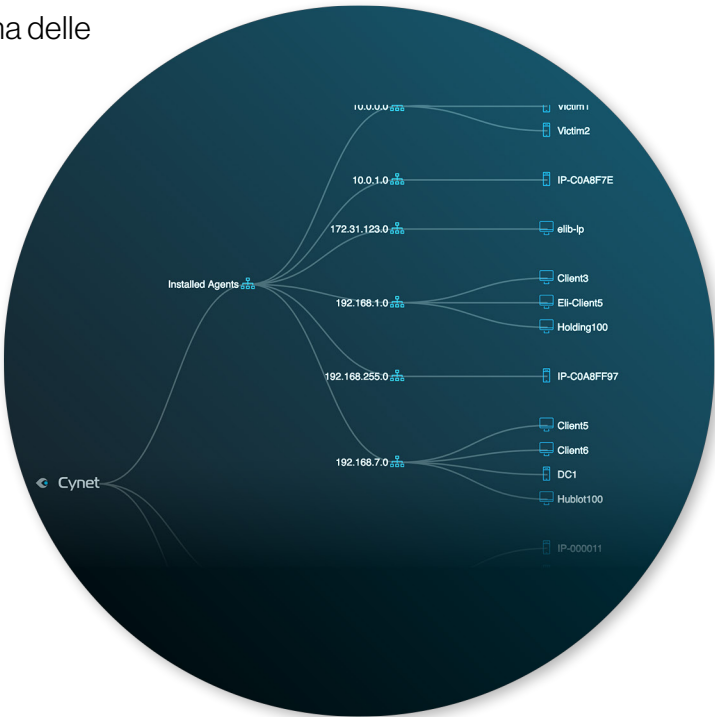
Cynet 360 is protecting your assets against this type of exploit.



Distribuzione

Il server di Cynet può essere distribuito in una delle seguenti modalità:

- **On-premise**
- **SaaS**
- **Ibrida:** adatto ad ambienti distribuiti in tutto il mondo, con server locali in ogni sito che inviano dati a un server centralizzato basato su cloud



L'agente Cynet è un file leggero con occupazione minima della memoria.

Cynet supporta vari metodi di distribuzione dell'agente quali RMM, MSI, Group Policy GPO, SCCM, incluso lo stesso dispatcher di Cynet, con la possibilità di distribuire fino a 5000 host in meno di un'ora.

SISTEMI OPERATIVI SUPPORTATI:



WINDOWS (32/64 BIT)

- [Windows XP SP3](#)
- [Windows Vista](#)
- [Windows 7](#)
- [Windows 8 and 8.1](#)
- [Windows 10](#)
- [Windows Server 2003 SP2](#)
- [Windows Server 2008 / 2008 R2](#)
- [Windows Server 2012 / 2012 R2](#)
- [Windows Server 2016](#)
- [Windows Server 2019](#)



LINUX (32/64 BIT)

- [Red Hat 6.4+](#)
- [Fedora 21+](#)
- [Ubuntu 14.04+](#)
- [CentOS 6.7+](#)
- [SUSE 12.0+](#)
- [Debian 6.0+](#)



MAC (64 BIT)

- [OS X Mavericks](#)
- [OS X Yosemite](#)
- [OS X El Capitan](#)
- [MacOS Sierra](#)
- [MacOS High Sierra](#)
- [MacOS Mojave](#)
- [MacOS Catalina](#)

Informazioni su Cynet

Cynet 360 è la prima piattaforma al mondo di protezione autonoma contro le violazioni che integra in modo nativo le funzionalità XDR di prevenzione e rilevamento degli attacchi a danno degli utenti, della rete e degli endpoint, con un motore di risposta agli incidenti che automatizza completamente le azioni di indagine e risoluzione, supportato da un servizio MDR di primordine operativo 24 ore su 24, 7 giorni su 7. La protezione dalle violazioni è completamente automatizzata e ora alla portata di qualsiasi organizzazione, indipendentemente dalle dimensioni e dal livello di competenza del gruppo che ha in carico la sicurezza. Per ulteriori informazioni, visitare il sito: <https://www.cynet.com>