FALCON 302

LEARNER GUIDE

VERSION 02.2024

CROWDSTRIKE

CROWDSTRIKE
UNIVERSITY

TABLE OF CONTENTS

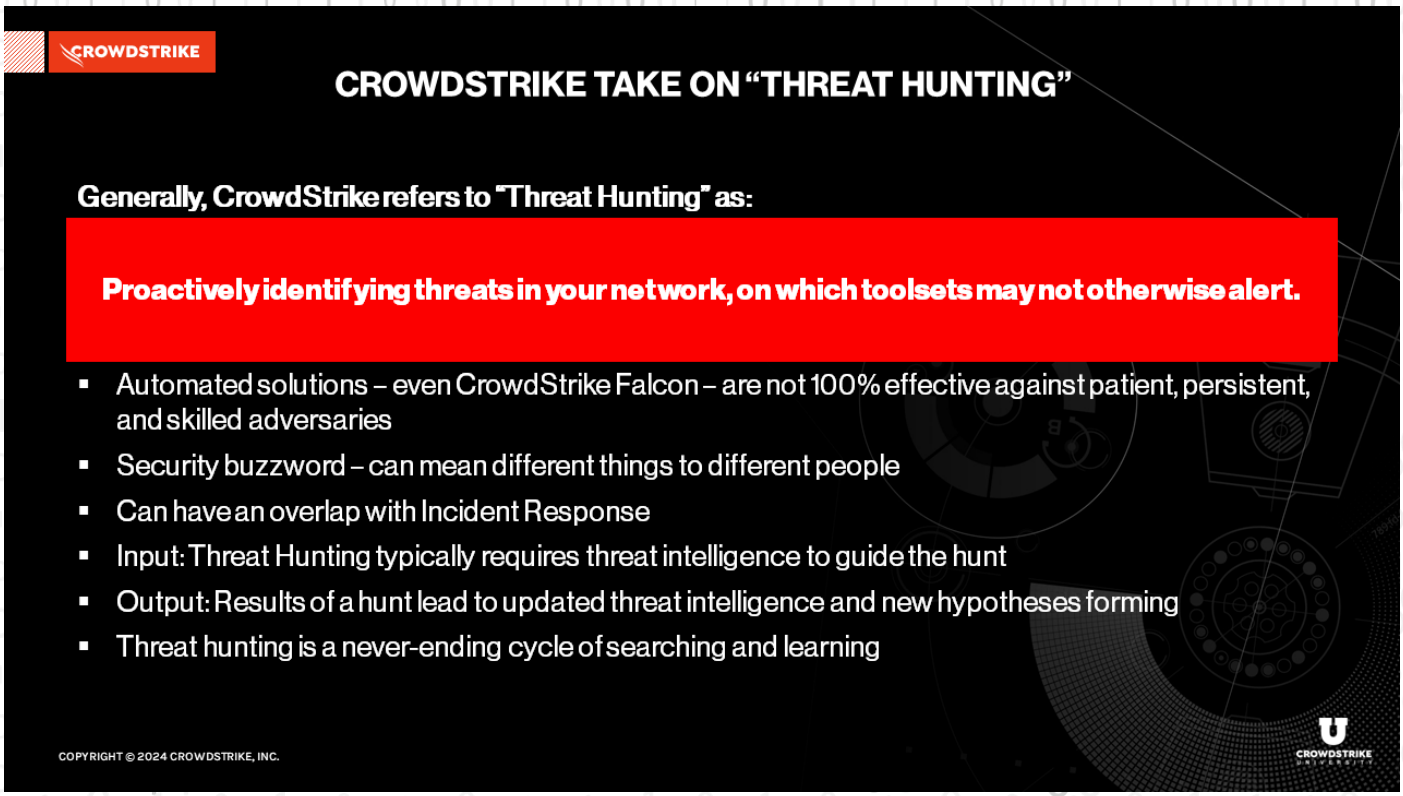
3	Overview
4	Threat Hunting Steps
7	Triggers and Pivots
16	Threat Sources
17	Intel 101
19	Resolution Tip
20	Threat Hunt Maturity Assessment
21	CrowdStrike S.E.A.R.C.H.
22	S.E.A.R.C.H. Tips
29	Hunting Methods
35	Visualizations
36	Advanced Hunting in EDR Data
40	Intelligence Models
42	MITRE ATT&CK
45	Morphological Analysis
47	ATT&CK Navigator
50	Threat Hunt Automation
53	Hunting Resources

CROWDSTRIKE

OVERVIEW

What is threat hunting?	Threat hunting is a discipline where skilled defenders hunt actively for the faintest signs of advanced attacks. It augments automated detection techniques such as machine learning and behavioral analytics with human experience and intuition, to see and stop advanced, stealthy attacks.
Benefits	Done properly, threat hunting leverages human experience to see and stop advanced attacks that might otherwise linger unseen for days, weeks, or months. It shortens dwell time, and is key to reliably stopping breaches.

CROWDSTRIKE TAKE ON THREAT HUNTING



THREAT HUNTING STEPS

The process of proactive cyber threat hunting typically involves three steps: a trigger, an investigation and a resolution.

1. Trigger	Point threat hunters to a specific area of the network for investigation when potential malicious activity is detected.
2. Investigation	Threat hunters use EDR technology to deep dive into potential malicious compromise of a system.
3. Resolution	Communicating malicious activity intelligence to operations and security teams so they can respond to the incident and mitigate threats.

REACTIVE VS. PROACTIVE HUNTING

Reactive Hunting

After threat detection

- When you have notification of a detection or that there is already an anomaly in your network
- Can come from a sensor or routine analysis of logs, netflow, etc
- Can come from a third party notification

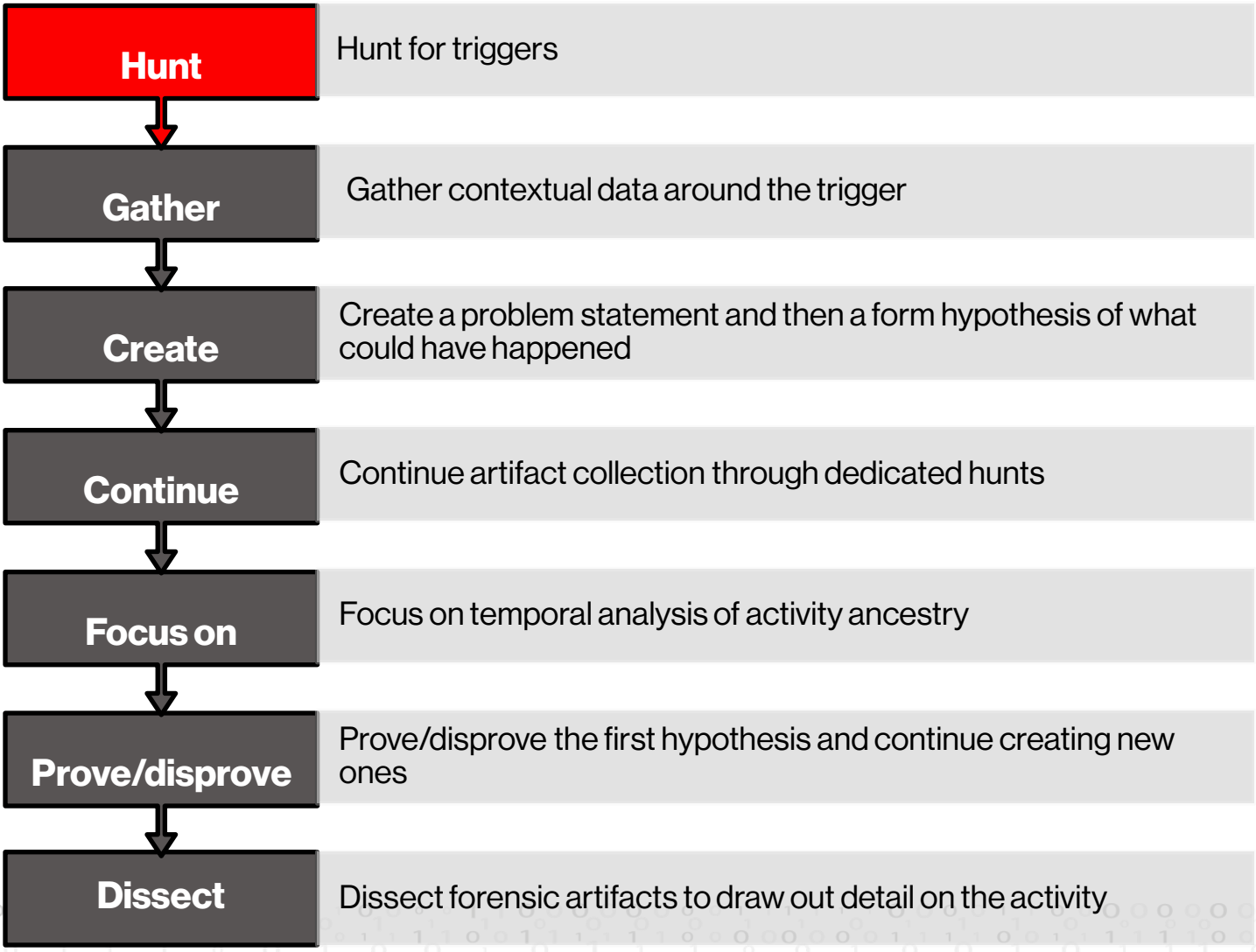
Proactive Hunting

Before threat detection

- No known attacks or compromises
- Searching for "just in case" scenarios and zero-day exploits
- Something you found in the news or intel but no indication it happened to you

CROWDSTRIKE THREAT HUNTING

Tips for Hunting with Falcon



CROWDSTRIKE THREAT HUNTING

The following sections of the Falcon platform pertain to a threat hunter.

SENSORS
Host sensors with on-board machine learning

VULNERABILITY MANAGEMENT
Check for vulnerabilities that prove/disprove your hypotheses

ENDPOINT SECURITY
Visualization of correlated events that cause detections

INVESTIGATE Raw data access and visual tools to sort and correlate data

EXPOSURE MANAGEMENT
Find unpatched and unapproved apps; examine account usage

CLOUD-BASED DATA STORE
Threat Graph and associated CrowdStrike data stores

REAL-TIME RESPONSE
Remote into any machine with an agent to extract artifacts

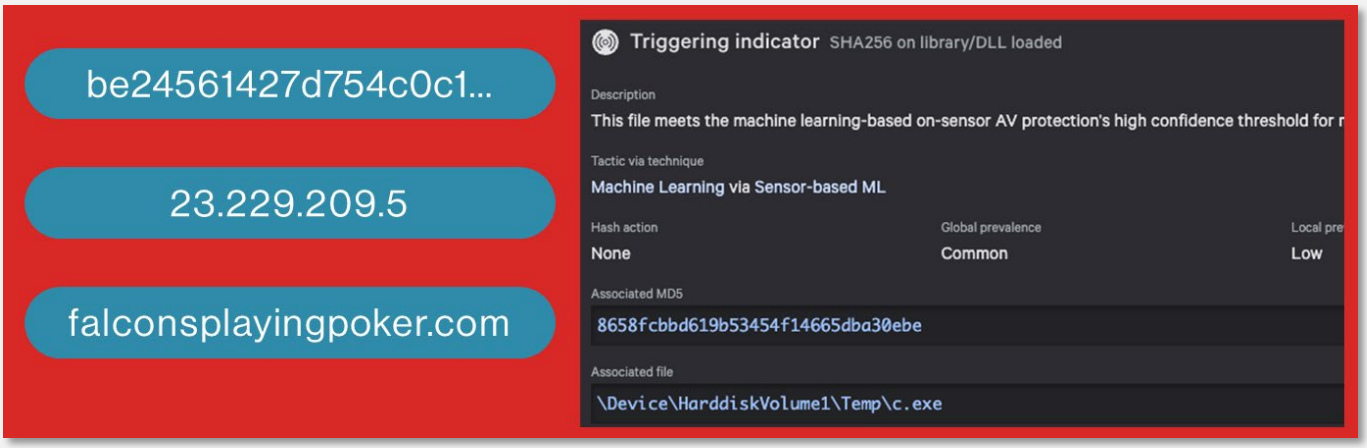
FALCON FORENSICS
Deploy a collector for fine-grained forensic analysis

CROWDSTRIKE THREAT INTELLIGENCE
Provide intelligence context to all the above

TRIGGERS AND PIVOTS

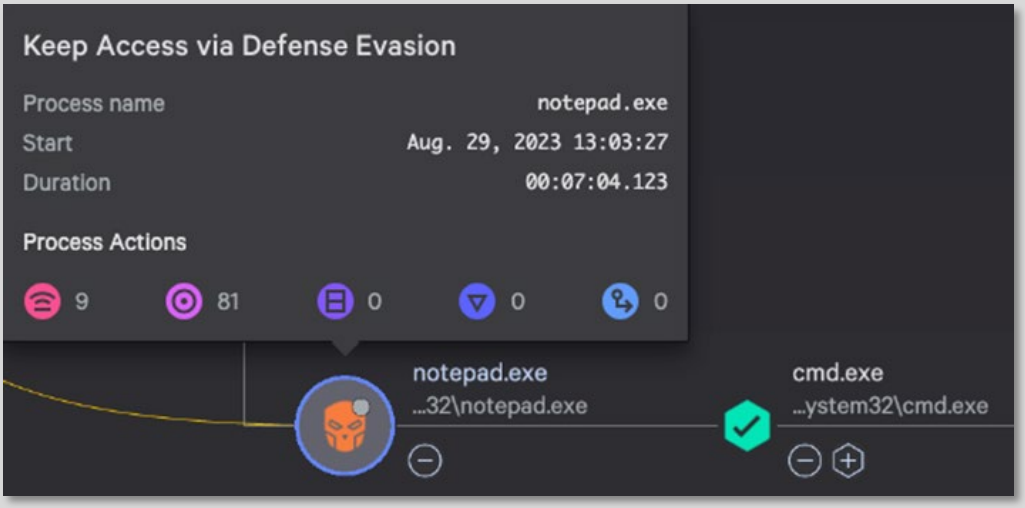
INDICATORS (IOCs)

- Hashes
- IP addresses
- Domain names



BEHAVIORS (IOAs)

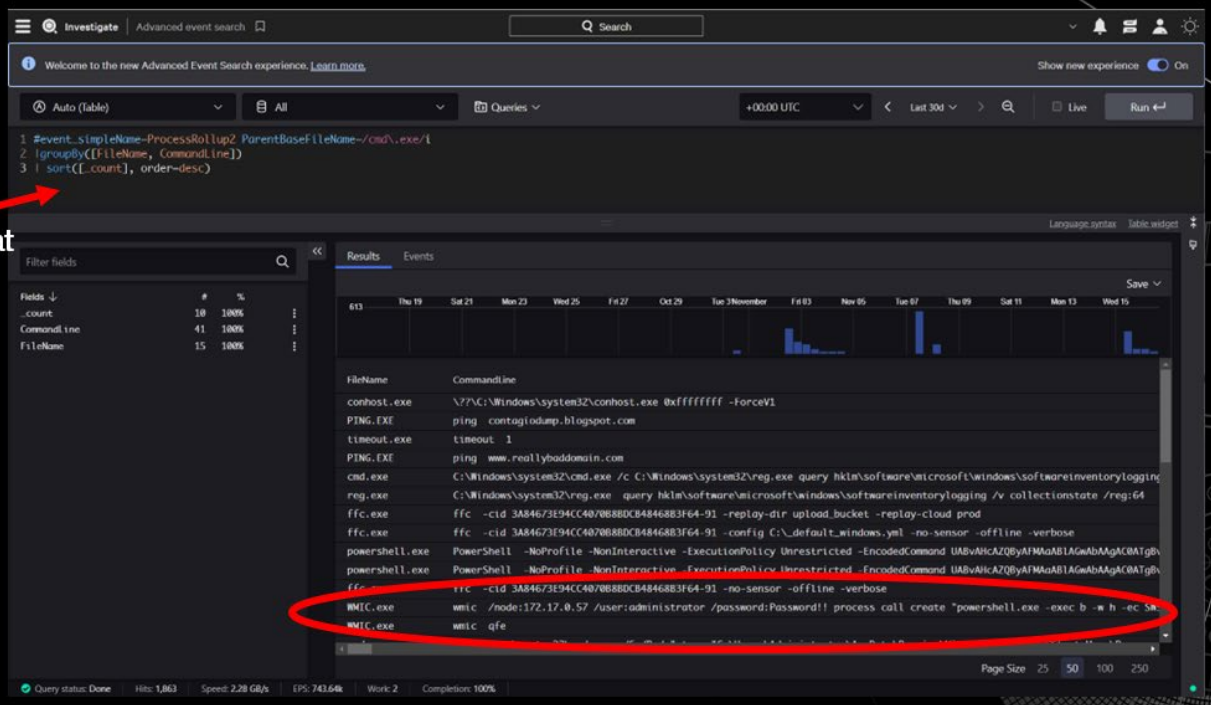
- Executables running from Temp directories
- Abnormal parent/child relationships
- Non-network processes making connections



FALCON TRIGGERS

FALCON TRIGGERS - INVESTIGATE (EVENT SEARCH)

Routine threat hunt query

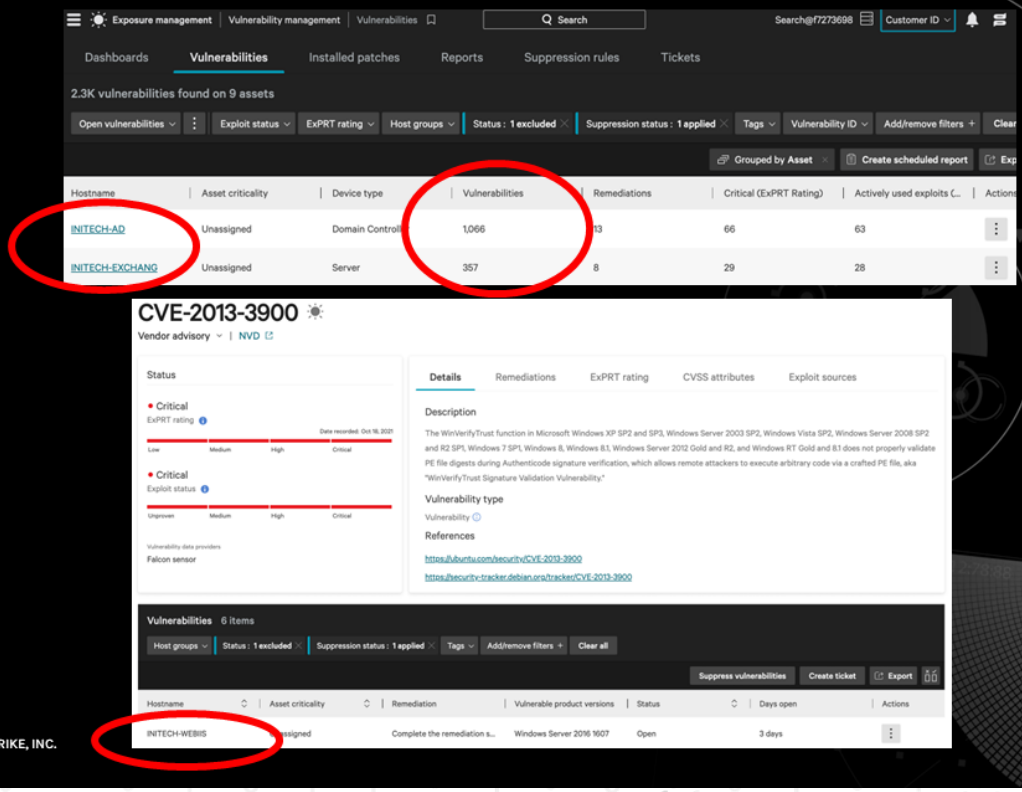


FALCON TRIGGERS - RAW DATA

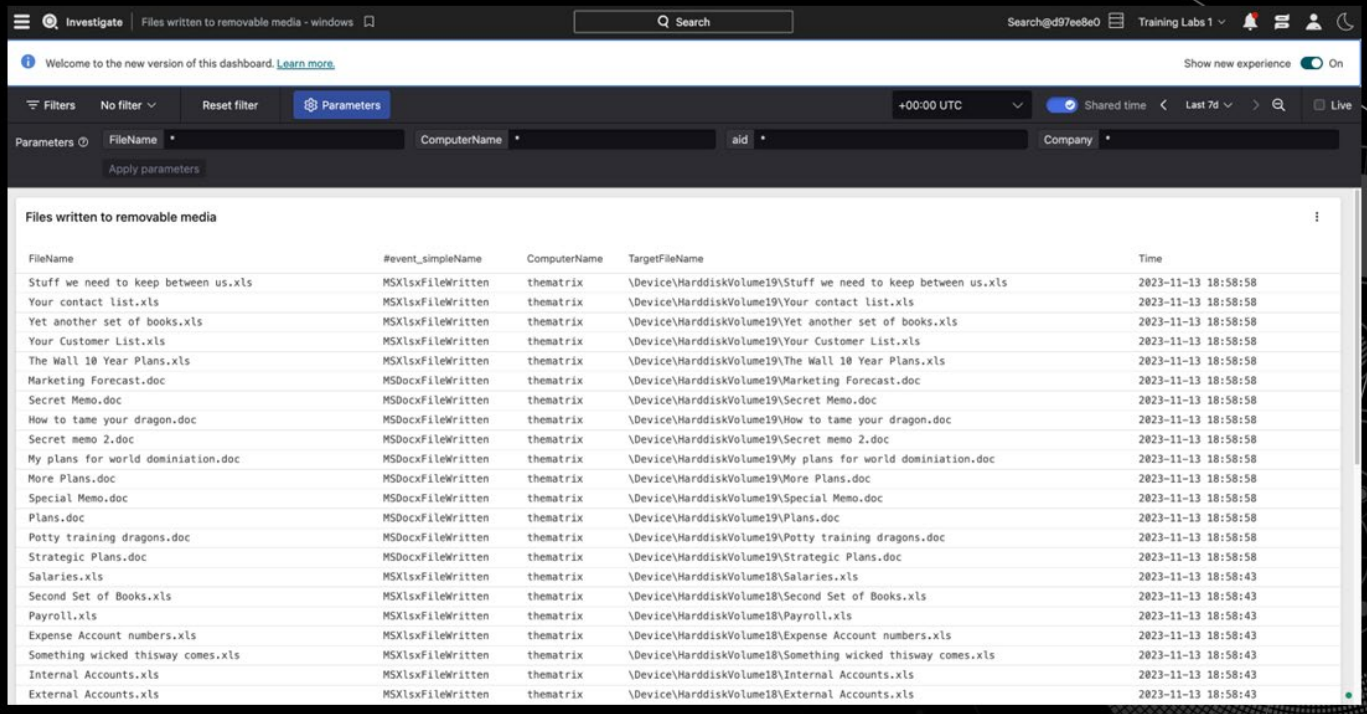

```
{
  "CommandLine":"C:\\temp\\c.exe",
  "ComputerName":"[redacted]",
  "ConfigBuild":"1007.3.0017506.1",
  "ConfigStateHash":"263646383",
  "ContextProcessId":"9233720866",
  "EffectiveTransmissionClass":"2",
  "Entitlements":"15",
  "EventOrigin":"1",
  "GrandparentCommandLine":"C:\\Windows\\system32\\svchost.exe -k DcomLaunch -p",
  "GrandparentImageFileName":"\\Device\\HarddiskVolume1\\Windows\\System32\\svchost.exe",
  "GrandparentProcessId":"14074983",
  "GrandparentProcessPatternIdList":"7140,7150,7410,7411,7412,7426",
  "ImageFileName":"\\Device\\HarddiskVolume1\\Temp\\c.exe",
  "LocalAddressIP4":"10.1.1.66",
  "ParentCommandLine":"C:\\Windows\\system32\\wbem\\wmiprvse.exe -secured -Embedding",
  "ParentImageFileName":"\\Device\\HarddiskVolume1\\Windows\\System32\\wbem\\WmiPrvSE.exe",
  "ParentProcessId":"9231672724",
  "ParentProcessPatternIdList":"218,7119,7141,7200,7201,7391,7402,7410,7411,7412,7647,7652,7654,7655,7675,7683",
  "PatternId":"10126",
  "PatternIdList":"171,218,3450,5765,7079,7093,7142,7143,7149,7200,7205,7214,7217,7223,7224,7225,7249,7252,7254,7256,7357,7398,7410,7411,7412,7428,7429,7430,7475,7566,7607,7646,7661,7675,7792,7900,7904,7912,10199,10251,10378,51324,51325",
  "Tags":"41, 53, 184, 197, 812, 843, 862, 874, 1218, 1225, 1226, 180388736803, 180388736922, 180388737277, 180388737404, 180388737948, 180388738074, 10995116277909, 10995116277927, 10995116277930, 10995116278019, 10995116278036, 10995116278186",
  "TemplateInstanceId":"15726",
  "TemplateInstanceIdList":"2932,3429,7355,7411,15308",
  "aid":"62d90c0e240a42a7ad0391cb8f4e6691",
  "aip":"100.26.62.1",
  "cid":"3a84673e94cc4070b8bdcb48468b3f64",
  "event_platform":"Win",
  "event_simpleName":"TemplateDetectAnalysis",
  "id":"4d86e3f2-00f3-4338-b592-9cc0f50b3894",
  "name":"TemplateDetectAnalysisV11",
  "timestamp":"1697231862934"
}
```

FALCON TRIGGERS

FALCON TRIGGERS - EXPOSURE MANAGEMENT

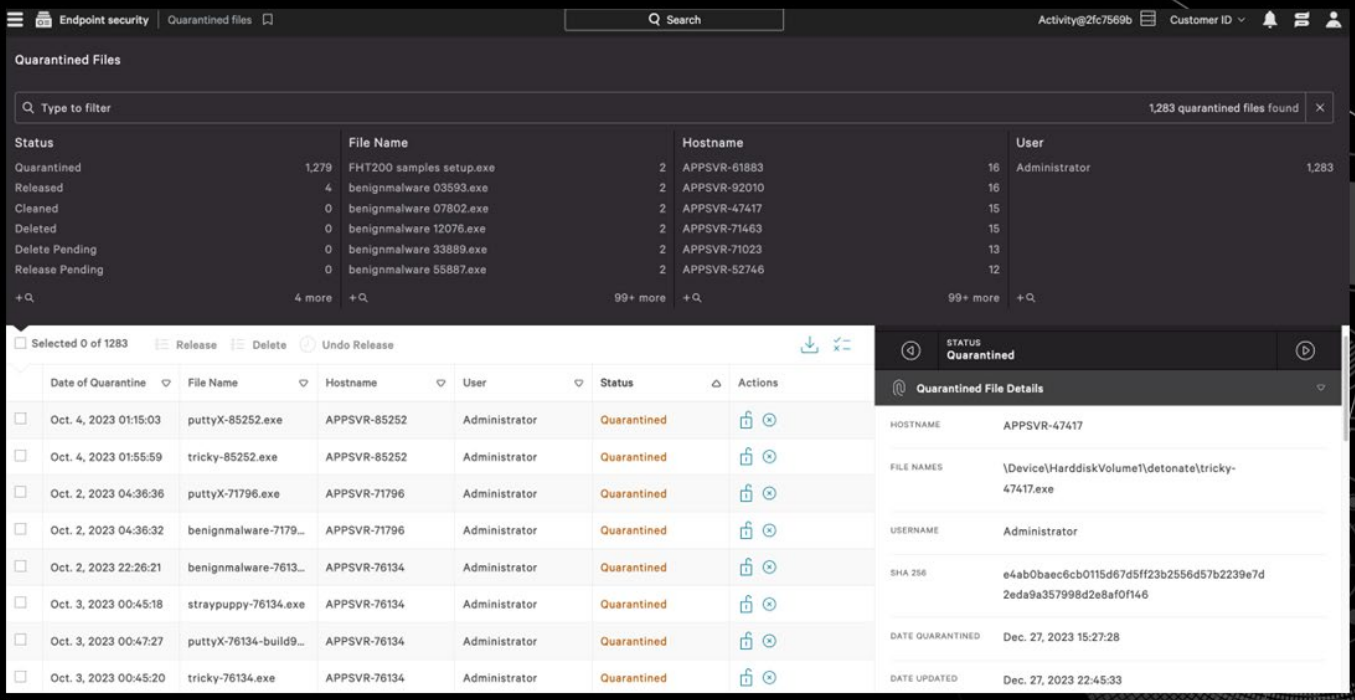


FALCON TRIGGERS - REMOVABLE MEDIA



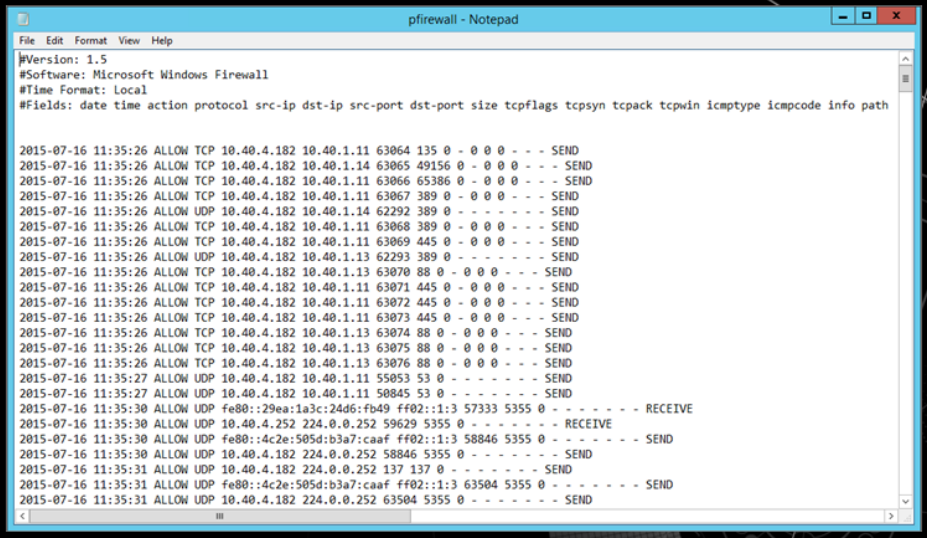
FALCON TRIGGERS

FALCON TRIGGERS - QUARANTINED FILES



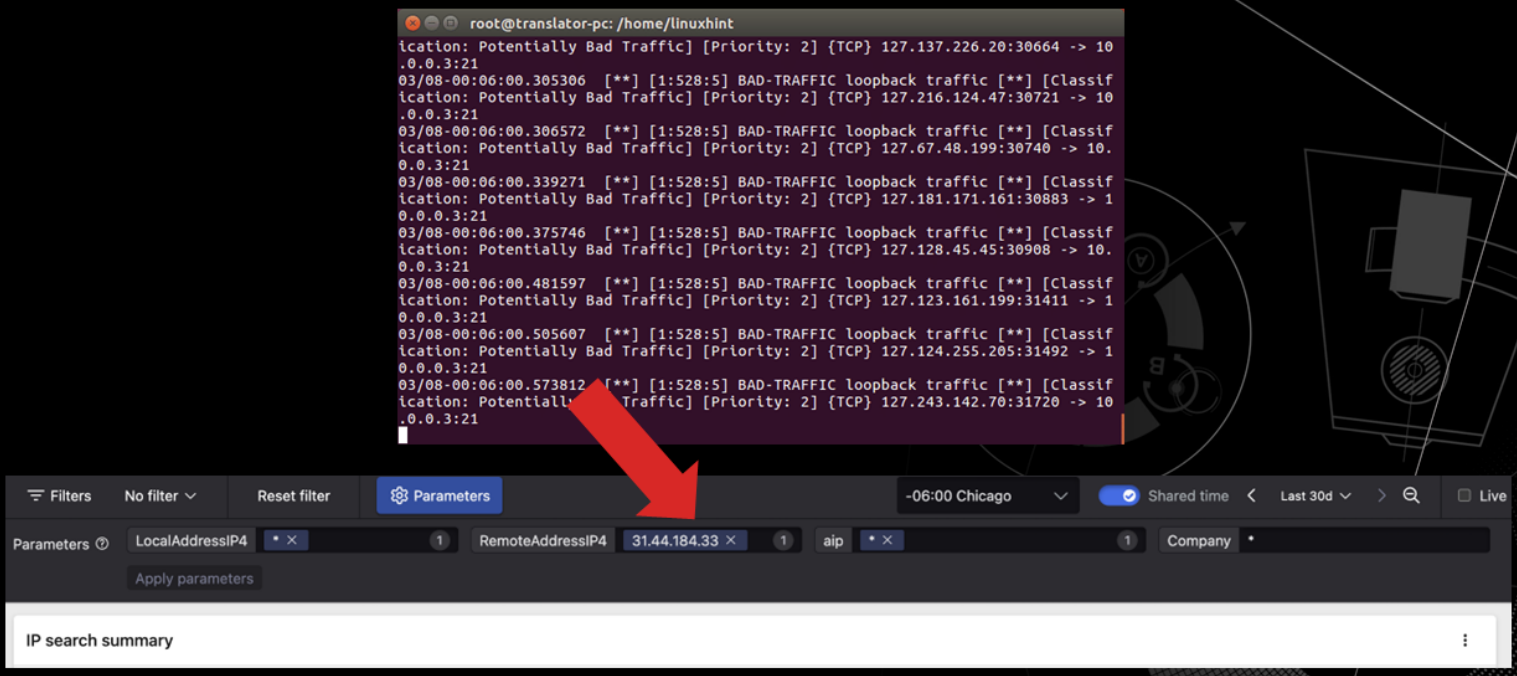
ENTERPRISE TRIGGERS

- Every enterprise is unique – threat hunters must know their enterprise in detail
- Leads can be found in dozens (or even hundreds) of locations in a typical enterprise
- Security appliances are often the best starting points
- Dead-box forensics
- Help Desk tickets

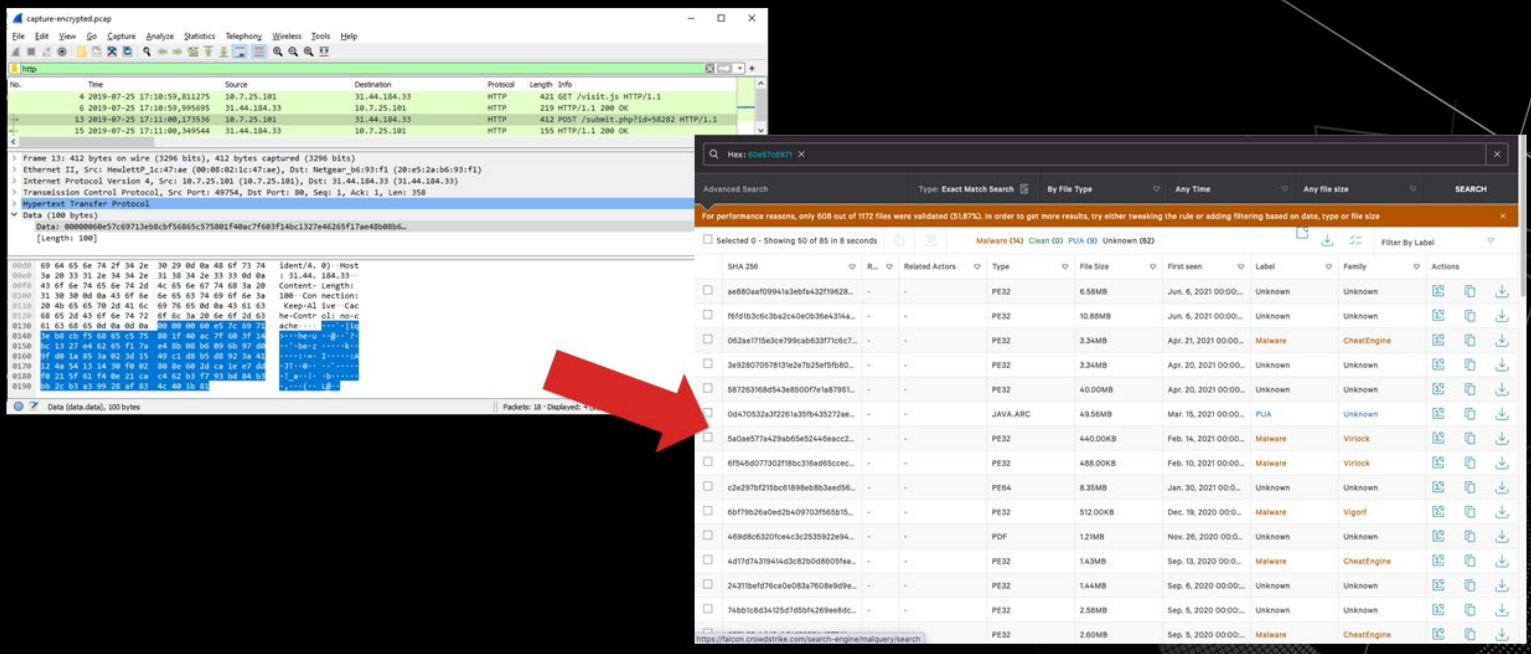


ENTERPRISE TRIGGERS

ENTERPRISE TRIGGERS - SECURITY APPLIANCE LOGS



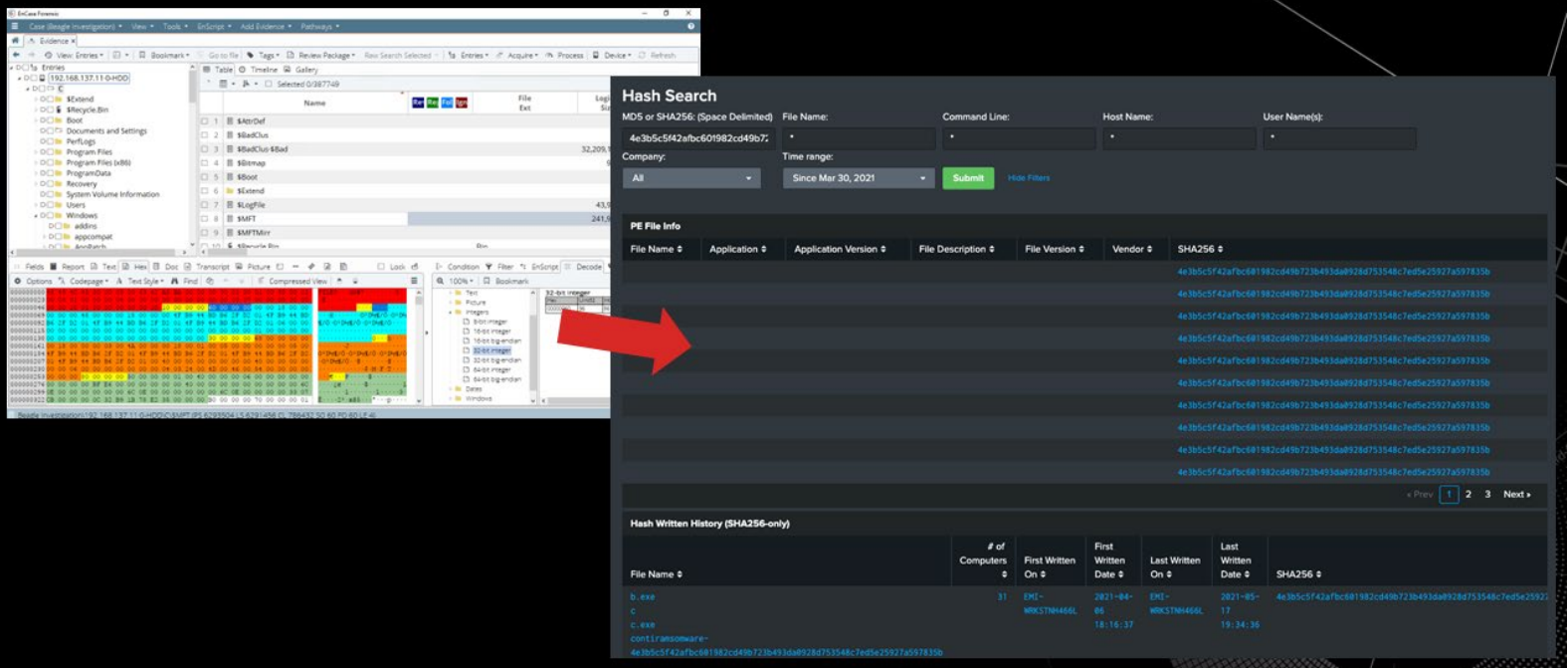
ENTERPRISE TRIGGERS - PACKET CAPTURE



Packet capture of Cobalt Strike callback to the C2

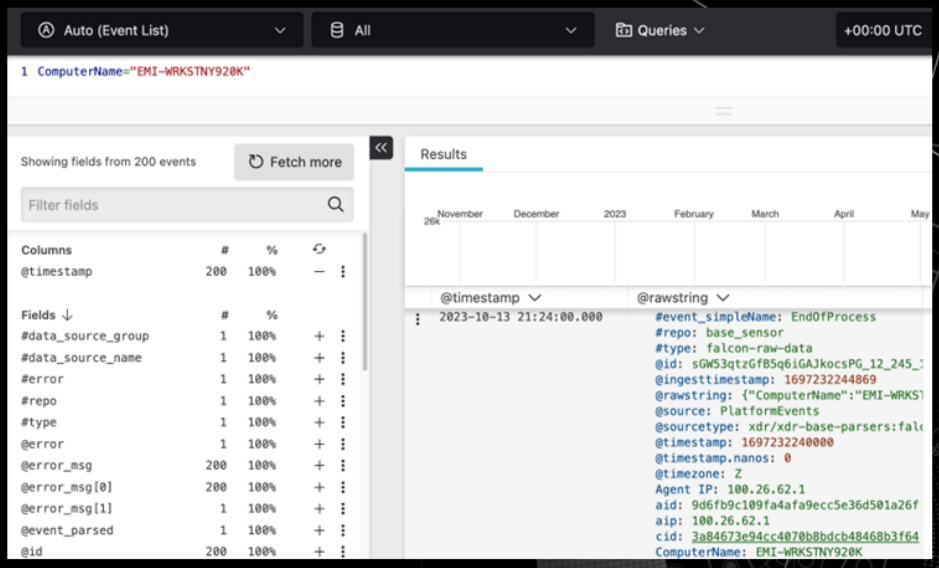
ENTERPRISE TRIGGERS

ENTERPRISE TRIGGERS - ENDPOINT FORENSICS



ENTERPRISE TRIGGERS - HELP DESK TICKETS

HELP DESK TICKET	
Name:	Jeanne Ferrer
Workstation:	EMI-WRKSTNY920K
Time/Date:	534pm – 13 Oct 2024
Issue:	
User clicked on a link in an email without thinking about it and now system is unresponsive and fan is loud.	
Actions:	
Referred to IR/TH team.	



NEWS TRIGGERS

News articles on cybersecurity issues, CVE announcements, and cyber threat intelligence reports are often the starting point for specific hunts.

CROWDSTRIKE

NEWS ARTICLE EXAMPLE

Russian Hackers Are Trying to Brute-Force Hundreds of Networks

While SolarWinds rightly drew attention earlier this year, Moscow's Fancy Bear group has been on a password-guessing spree this whole time.

THE DISCOVERY OF Russia's devastating SolarWinds spy campaign put the spotlight on the sophisticated supply chain hijacking techniques of Moscow's foreign intelligence hackers. But it's now apparent that, throughout that SolarWinds spying and its fallout, another group of Kremlin hackers has kept up up their usual daily grind, using basic but often effective techniques to pry open practically any vulnerable network they could find across the US and the global internet.

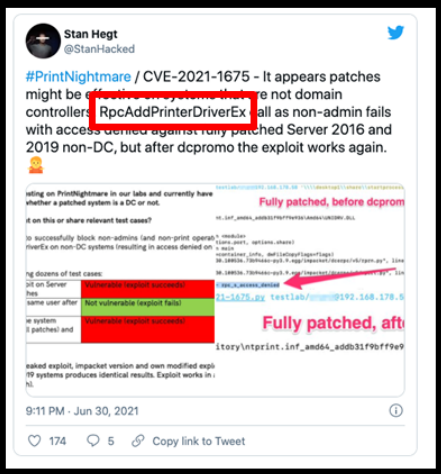
On Thursday the NSA, the FBI, the DHS's Cybersecurity and Infrastructure Security Agency, and the UK's National Cybersecurity Centre issued a joint advisory warning of hundreds of attempted brute-force hacker intrusions around the world, all carried out by Unit 26165 of Russia's GRU military intelligence agency, also widely known as Fancy Bear or APT28. The hacking campaign has targeted a broad swath of organizations, including government and military agencies, defense contractors, political parties and consultancies, logistics companies, energy firms, universities, law firms, and media companies. In other words, practically every sector of interest on the internet.

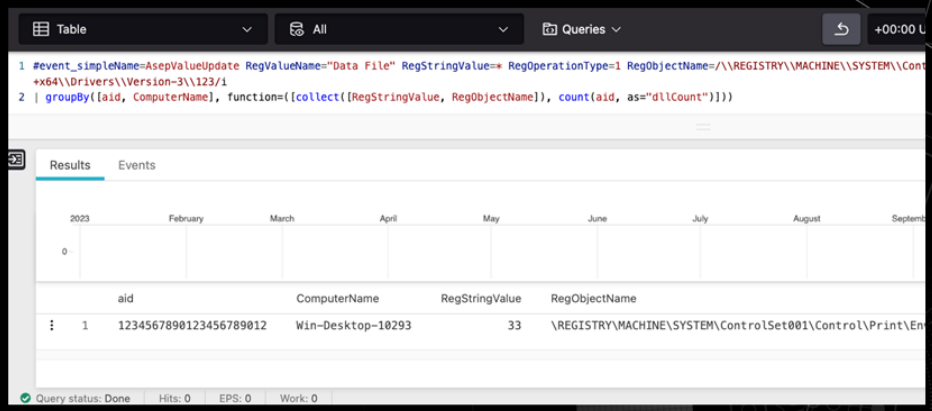
The hacking campaign has used relatively basic techniques against those targets, guessing usernames and passwords en masse to gain initial access. But cybersecurity agencies warn that the Fancy Bear campaign has nonetheless successfully breached multiple entities and exfiltrated emails from them—and that it's not over. "This lengthy brute force campaign to collect and exfiltrate data, access credentials and more, is likely ongoing, on a global scale," the NSA's director of cybersecurity Rob Joyce wrote in a statement accompanying the advisory.

How can we find this using Falcon?

CROWDSTRIKE

SOCIAL MEDIA EXAMPLE





NEWS TRIGGERS

CROWDSTRIKE

CVE EXAMPLE

Printer-Friendly View

CVE-ID

CVE-2021-3613 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

OpenVPN Connect 3.2.0 through 3.3.0 allows local users to load arbitrary dynamic loadable libraries via an OpenSSL configuration file if present, which allows the user to run arbitrary code with the same privilege level as the main OpenVPN process (OpenVPNConnect.exe).

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://openvpn.net/vpn-server-resources/openvpn-connect-for-windows-change-log/
- URL:https://openvpn.net/vpn-server-resources/openvpn-connect-for-windows-change-log/

Assigning CNA

OpenVPN Inc.

Date Record Created

20210622 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20210622)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is a record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: Submit
You can also search by reference using the CVE Reference Maps.

For More Information: CVE Request Web Form (select "Other" from dropdown)

How can we find this using Falcon?

CROWDSTRIKE UNIVERSITY

CROWDSTRIKE

CYBER INTELLIGENCE EXAMPLE

Alert

WIZARD SPIDER Adds SMB Port Scanning in New Version of Conti Ransomware

CSA-201317 October 13, 2020 14:10:41

CrowdStrike Intelligence has identified notable changes in the latest variants of WIZARD SPIDER's *Conti* ransomware. WIZARD SPIDER's development and deployment of Conti is still ongoing, even with the recent return of *Ryuk* ransomware (CSA-201205). The simultaneous operation of both ransomware families in BGH campaigns suggests WIZARD SPIDER may have multiple sub-groups within their organization, each responsible for the development and deployment of their ransomware.

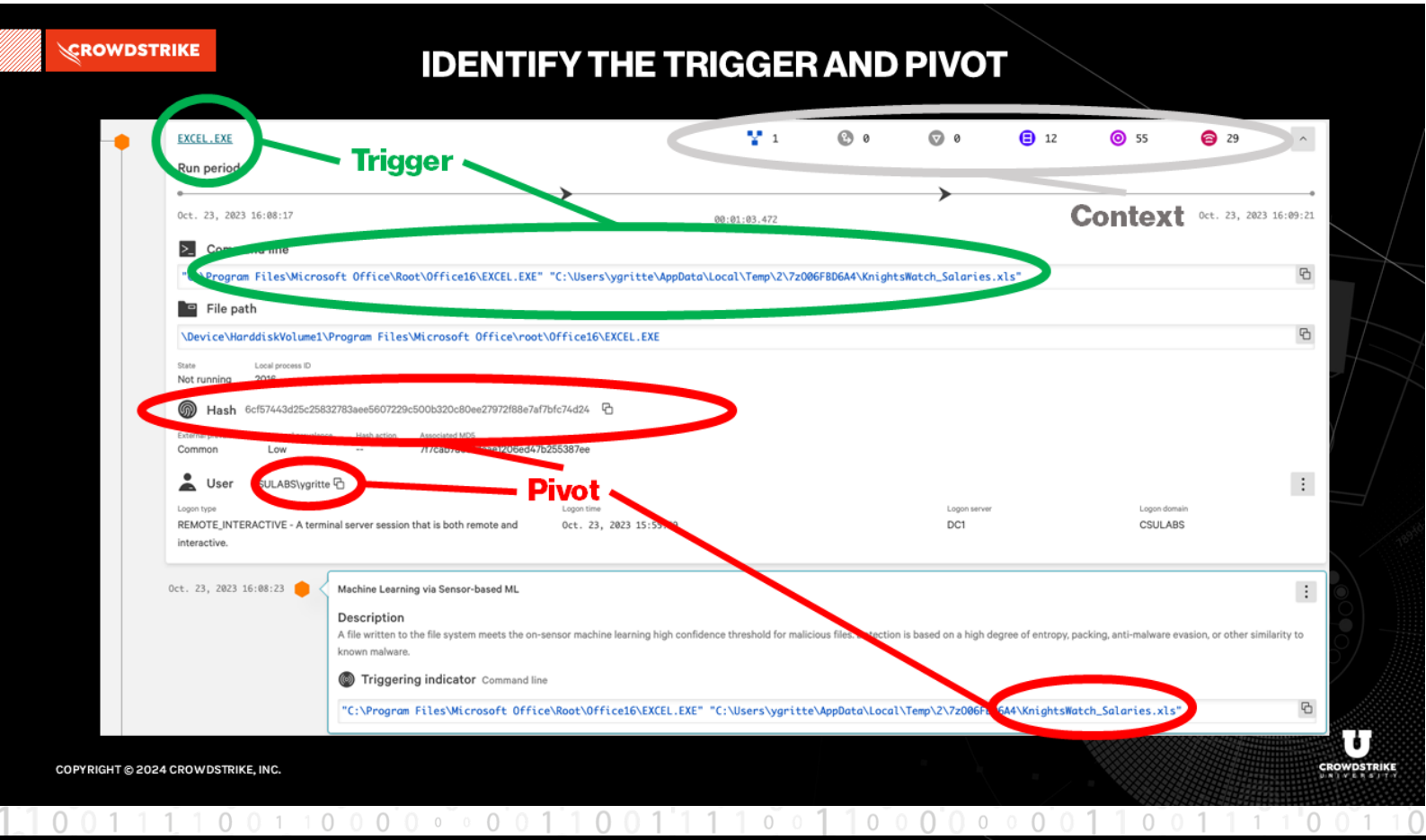
The following modifications to Conti have been observed since the publication of CSIT-20129 and CSA-201103:

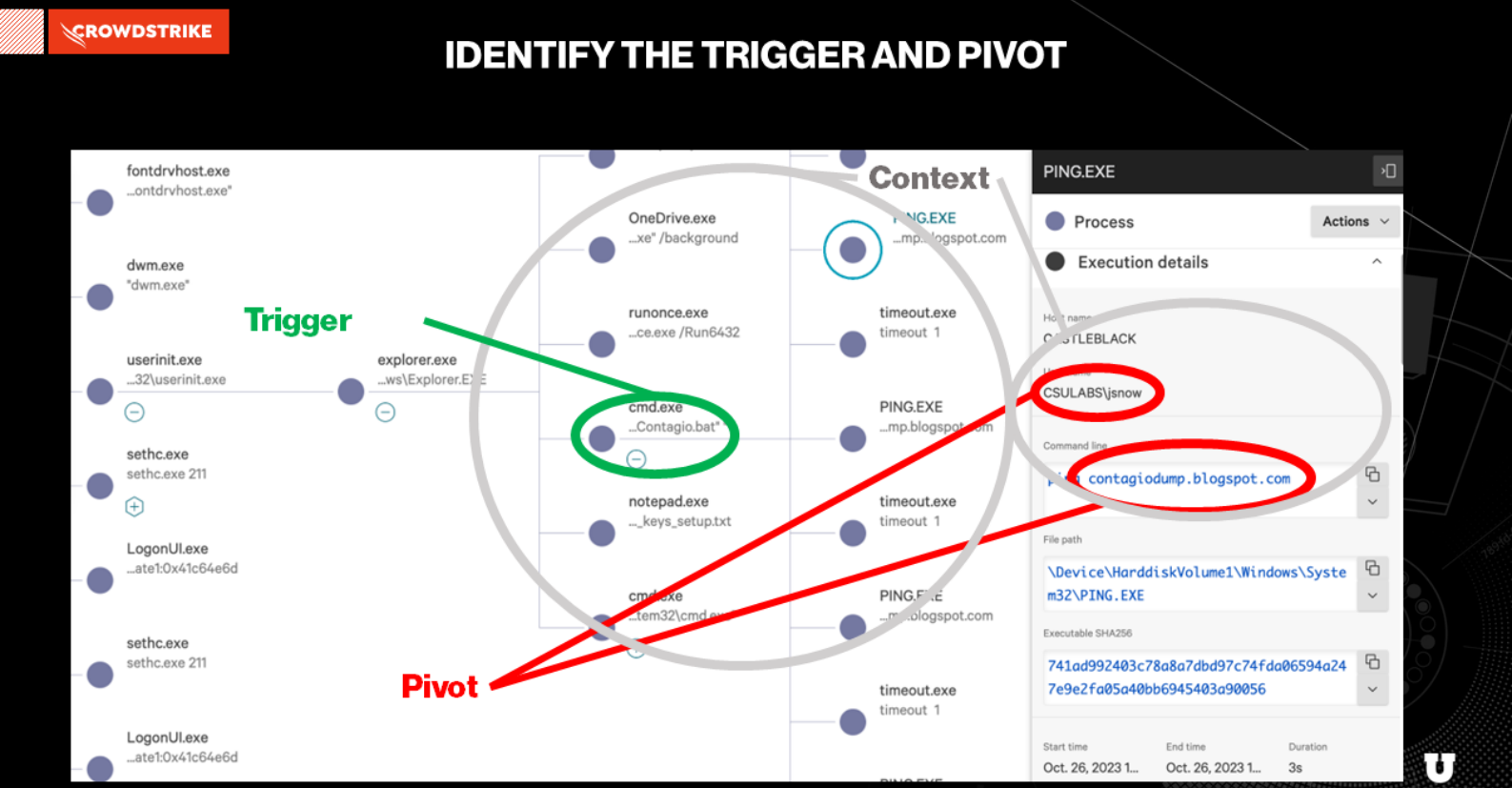
- The encrypted file extension is unique for each victim and is typically five seemingly random characters, such as `.DKVJI`, `.ILMWL`, or `.TUWUQ`.
- Ransom note file names are changed regularly and no longer identify the ransomware by name; e.g., `README.txt` or `R3ADM3.txt`.
- Scanning the local network to identify hosts with the TCP port 445 (SMB) open.
- The command-line arguments used to deploy the ransomware were changed to support additional functionality.
- Process termination functionality was reintroduced.
- Additional obfuscation of Windows API calls by resolving imported function addresses from precomputed MurMurHash2[1] hash values during execution.
- Removal of the PE resource section; all configuration values are now stored within the executable's `.data` section.

How can we find this using Falcon?

CROWDSTRIKE UNIVERSITY

PIVOTS


CROWDSTRIKE
IDENTIFY THE TRIGGER AND PIVOT
EXCEL.EXE
Trigger
Context
Pivot
File path
Hash
User
Machine Learning via Sensor-based ML
Description
Triggering indicator
Command line
COPYRIGHT © 2024 CROWDSTRIKE, INC.


CROWDSTRIKE
IDENTIFY THE TRIGGER AND PIVOT
Trigger
Context
Pivot
PING.EXE
Process
Actions
Execution details
CSULABS\jsnow
contagiodump.blogspot.com
\Device\HarddiskVolume1\Windows\System32\PING.EXE
741ad992403c78a8a7dbd97c74fda06594a247e9e2fa05a40bb6945403a90056
COPYRIGHT © 2024 CROWDSTRIKE, INC.

THREAT SOURCES

Threat Sources	Description
External Actors	Ping sweeps RDP password guessing
Insider Threats	File share access attempts Unauthorized use of removeable media Clicking of links in emails Download attachments from emails
Supply Chain	Lateral movement originating from inside Privilege escalation Malware deployment from inside Command and control from specified device Odd/new outbound IP connections after an update

INTEL 101

INTEL 101

Intel resource in Falcon	Description
Counter Adversary Operations > Intelligence Reports & Feeds	• Periodic reports on adversary activities, as well as frequently updated feeds of CEF, NetWitness, Snort/Suricata, and YARA rules
Actors	• Go to Threat intelligence > Research > Actors to find actor profiles and the intelligence CrowdStrike has gathered for each of them
Counter Adversary Operations > Indicators	• The Indicators page enables you to query the database of CrowdStrike Intelligence indicators of compromise (IOCs)
Falcon Sandbox	• Simplifies analysis of files and URLs that are suspicious or malicious into one automated workflow • Rapid access to associated indicators of compromise (file hashes, domains, and IP addresses) that you can use to fine tune your organization's security infrastructure • Provides report analyzing suspicious and malicious files and URLs to help validate whether a file is dangerous
Falcon Malquery	• Falcon MalQuery also provides rich context describing malware • This includes IOCs, such as hashes, a verdict whether the file is malware, the malware family, and if CrowdStrike has attributed the threat to an actor, links to the actor profile
Falcon Intelligence Recon	• Counter Adversary Operations > External monitoring > Recon • Falcon Intelligence Recon uncovers if adversaries are targeting your organization and whether any of your data is being mentioned, sold, or impersonated on the dark web, social media, forums, and other services
Global Search	• The global search is available in every page of the Falcon platform

3RD PARTY INTEL

Intelligence Reach

- **Your intelligence team isn't the only part of the company collecting intelligence.**
- **Critical to compare methods, timing, sources, and information.**
- **Intel Reach is the best way to VALIDATE intelligence your team has collected.**

CROWDSTRIKE

COLLABORATION EXAMPLES

InfraGard – FBI partnership with private sector; enacted to share information; 4/5 Fortune 500 companies have a rep

NCFTA – Pittsburgh-based non-profit for "identifying, mitigating, and neutralizing cyber crime threats globally."

Interpol – 192-member police organization; IGCI (Singapore) research & development between LE and private sector

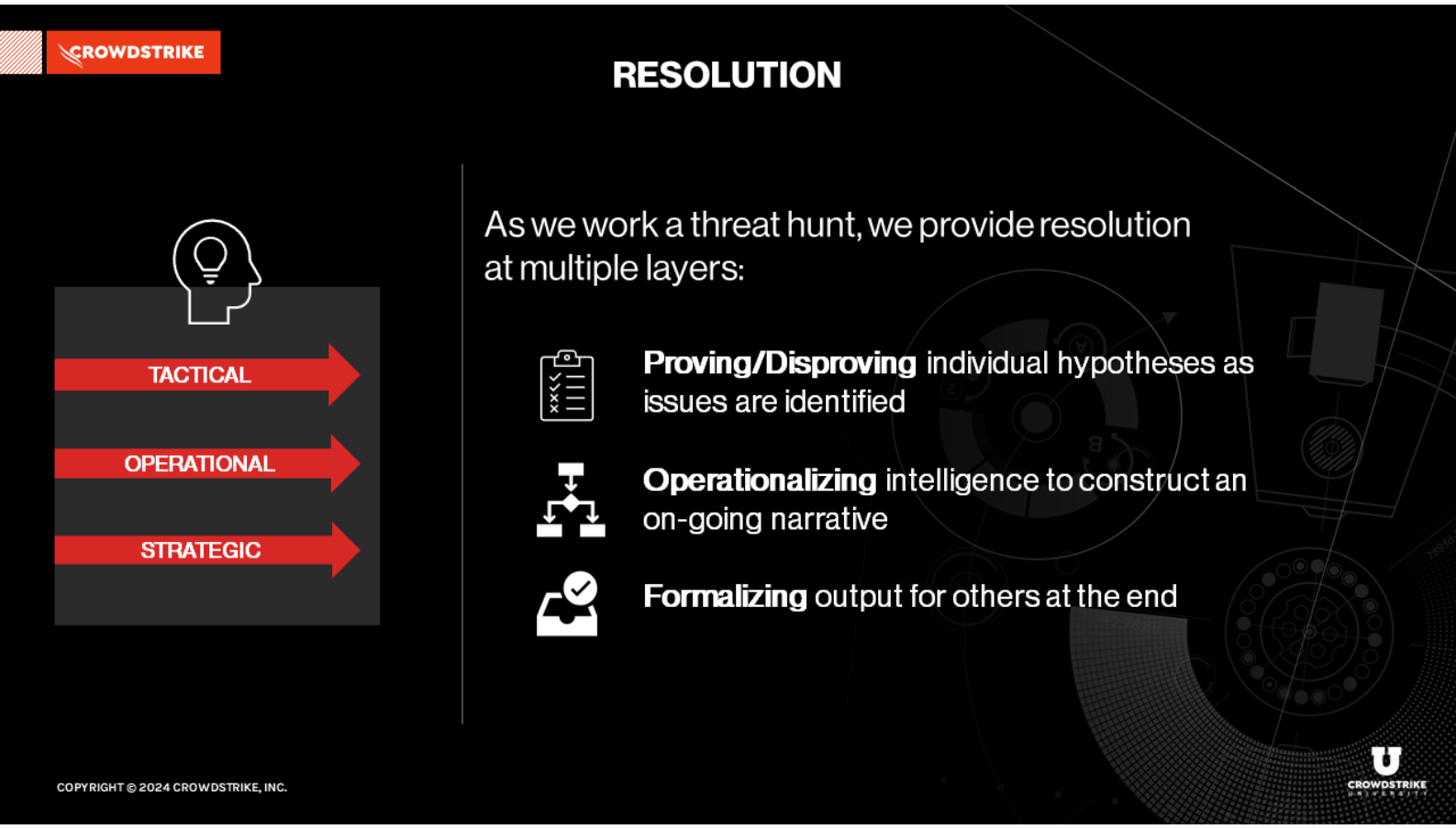
NCIJTF (CyWatch) – 20+ LE/ID/DoD members; coordinates, integrates, and shares information to support cyber crime investigations

Cyber Threat Alliance – members submit data, scored and totaled to keep in good standing; can extract other user's data; uses STIX

CISA– Cybersecurity & Infrastructure Security Agency has the Cyber Information Sharing and Collaboration Platform (CISCP); unclassified information exchange through trusted public-private partnerships

CROWDSTRIKE UNIVERSITY

RESOLUTION



RESOLUTION PRO TIP

TIPS

- Standardize note taking and documentation
- Notes may need to be shared internally, with LE, with lawyers, with insurance, etc

Threat Hunting Notes

Name	Ryan F
Date	2020-05-01
Hunting Topic / Objective	Threat hunt based on MITRE ATT&CK's APT31 evaluation
Timeframe	Last 7 days
Toolsets Used	CrowdStrike Falcon and SIEM PaloAlto logs

1. Search of Falcon Events for rundll32 utilization with Temp file paths.
    a. Query: event_simpleName=ProcessRollup2 FileName=rundll32.exe "Temp"
    b. Added filter NOT "ccm"
2. Further investigated the following data:
    a. Systemname = ABC123 CommandLine=rundll32.exe C:\Windows\Temp\xi32.dll,start

THREAT HUNT MATURITY ASSESSMENT

5
- ❑ Some threat hunting automation
- ❑Cyber Threat Intelligence is used to scope threat hunting

4
- ❑ Scheduled threat hunting is routinely conducted
- ❑ Cyber Threat Intelligence is used for operationalization
- ❑ APT metrics are tracked

3
- ❑Threat hunt hypotheses are informed by threat intelligence
- ❑Clearly defined transition from threat hunting to incident handling

2
- ❑Threat hunting is performed ad hoc during an incident
- ❑ IOC understanding derived from ad hoc OSINT collection

1
- ❑ Organization has minimal understanding or use of threat hunting

CROWDSTRIKE S.E.A.R.C.H.

CROWDSTRIKE

S.E.A.R.C.H.

- CrowdStrike Falcon OverWatch team's proven hunt methodology
- Precise balance of people, processes, and technology
- The OverWatch team performs at a world-class level because of this framework
- We can't completely rebuild S.E.A.R.C.H. for our own use – but we can take away some key ideas, tools, and processes

CROWDSTRIKE

OVERWATCH SEARCH THREAT HUNTING METHODOLOGY

S → E → A → R → C → H

SENSE ENRICH ANALYZE RECONSTRUCT COMMUNICATE HONE

COLLECT → REFINE → ANALYZE → PRODUCE → DISSEMINATE → FEEDBACK

S.E.A.R.C.H. TIPS

CROWDSTRIKE

TIPS

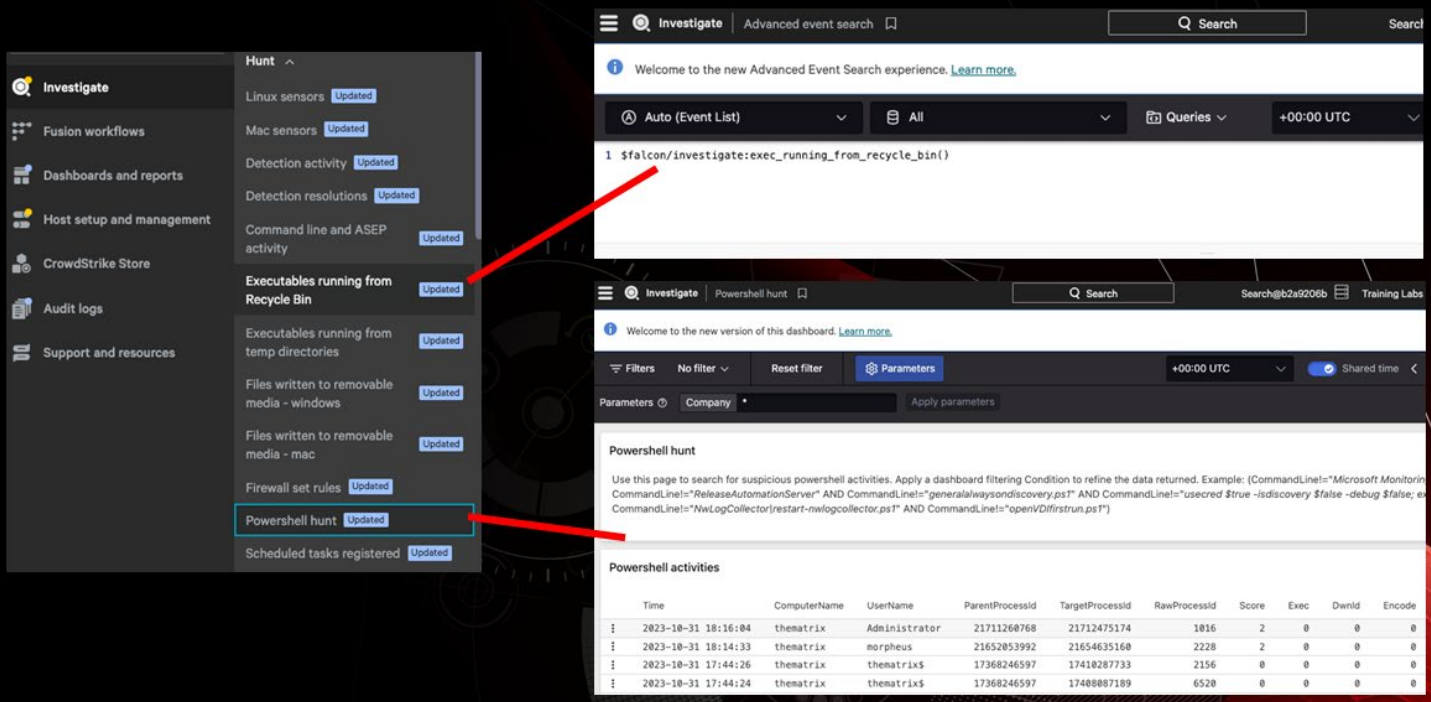
HOW TO COLLECT (SENSE) BETTER

- Ensure all endpoints have a Falcon agent installed
- Endpoints should be named smartly – be able to find an endpoint quickly
- Place endpoints in appropriate groups
- Create appropriate policies for the groups
- Create exclusions to reduce false positives
- Ensure sensor update policies are set correctly

CROWDSTRIKE UNIVERSITY

CROWDSTRIKE

STARTING POINTS



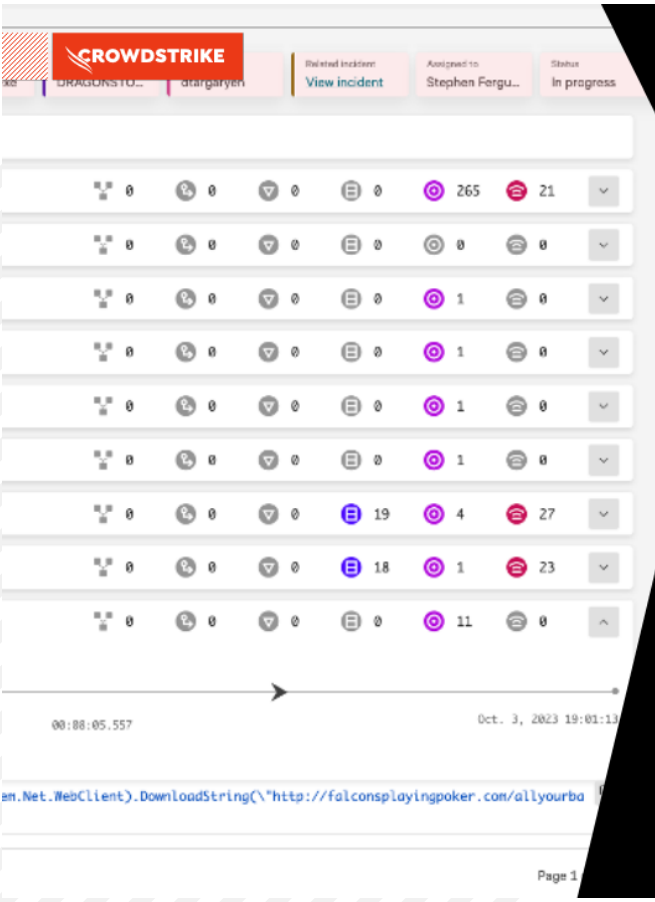
CROWDSTRIKE UNIVERSITY

S.E.A.R.C.H. TIPS

TIPS

HOW TO REFINE (ENRICH) BETTER

- Most of the enrichment is already done for you by the ThreatGraph
- Pay attention to newly released threat intelligence reporting
- Use the Actor Intelligence and Indicators portals to the greatest extent possible
- Learn to use ALL of the Investigate pages
- Practice your OSINT skills – use Falcon OSINT when you can
- Build your Event Search query skills, Learn YARA, understand Sandbox reports – use Falcon proficiently



ENRICH

- OverWatch identifies over 23 million hunting leads per day
- CONTEXT is EVERYTHING – must prioritize!
- ThreatGraph provides context to the events, building visualization between data points
- Hunting relies as much on threat intelligence as it does the raw data
- This is the biggest, most important part of the entire process!

S.E.A.R.C.H. TIPS

TIPS

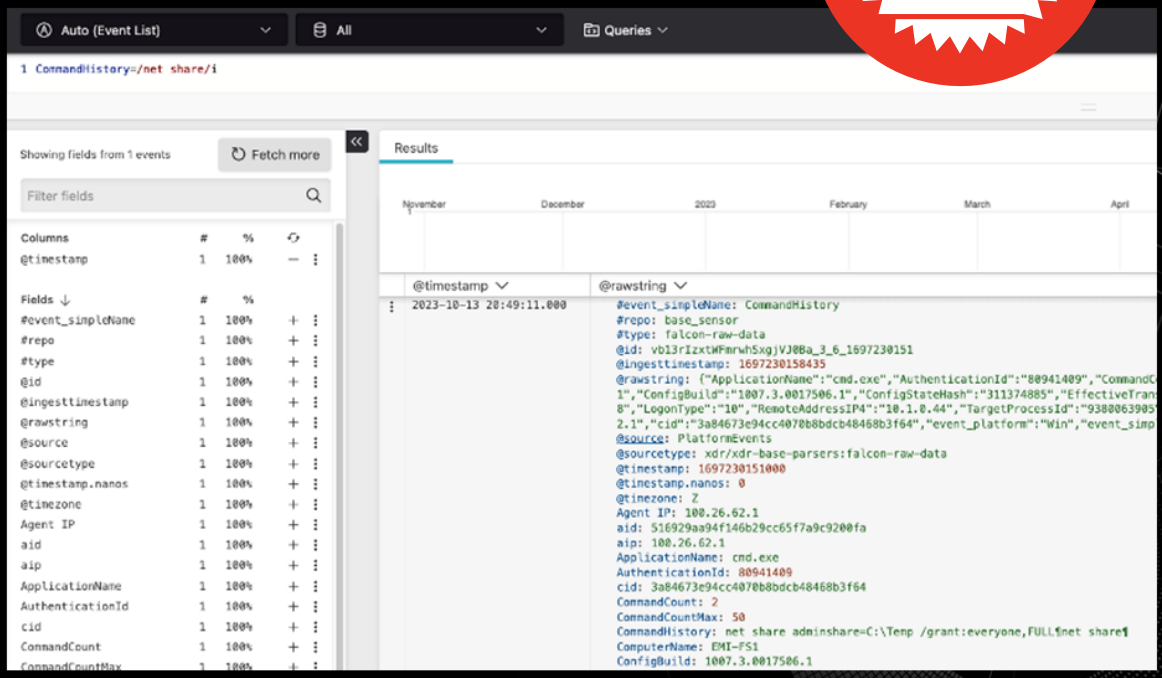
CROWDSTRIKE

ENRICHMENT

Now what?

- Username?
- Automated or hands-on? Parent process?
- Other endpoints with C:/Temp?
- Timeline this machine?

...so many ways to pivot!

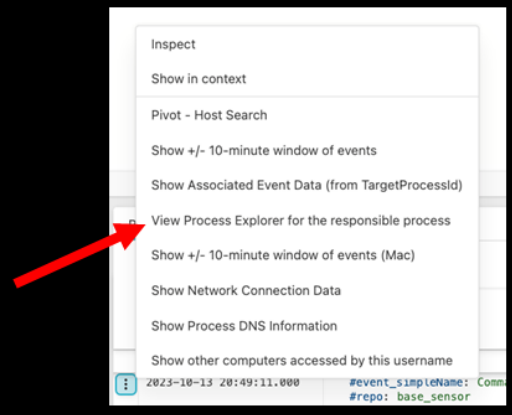


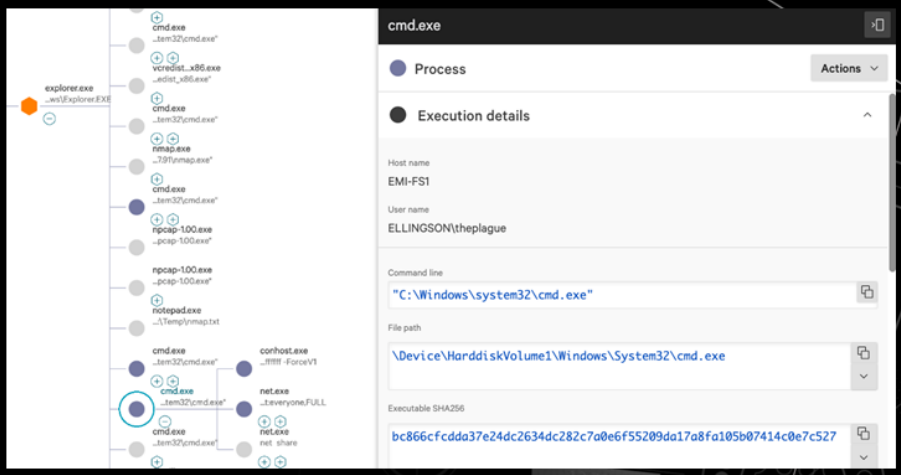
CROWDSTRIKE UNIVERSITY

CROWDSTRIKE

PIVOTING

- No ONE right way to pivot
- Experience and intuition
- Remember your threat hunt goals
  - Find impacted hosts
  - Actor attribution





CROWDSTRIKE UNIVERSITY

S.E.A.R.C.H. TIPS

CROWDSTRIKE

HOW TO ANALYZE BETTER

TIPS

- Learn structured analytics (attend CST 346)
- As a solo analyst – develop your own methodologies and stick to them
- As a team – learn each other's methodologies and use them to refine your own
- Study the particulars of various tactics and techniques – MITRE ATT&CK is perfectly setup for this
- Develop capabilities to merge automated analysis with human-derived analysis
- Review findings a month/year later – what did you get right and what did you get wrong?

CROWDSTRIKE UNIVERSITY

ANALYZE

- Statistical models are great, but human analysis is required too
- Blending advanced machine learning with human intuition provides the best analysis
- Use of structured analytics greatly assists deep understanding

CROWDSTRIKE UNIVERSITY

S.E.A.R.C.H. TIPS

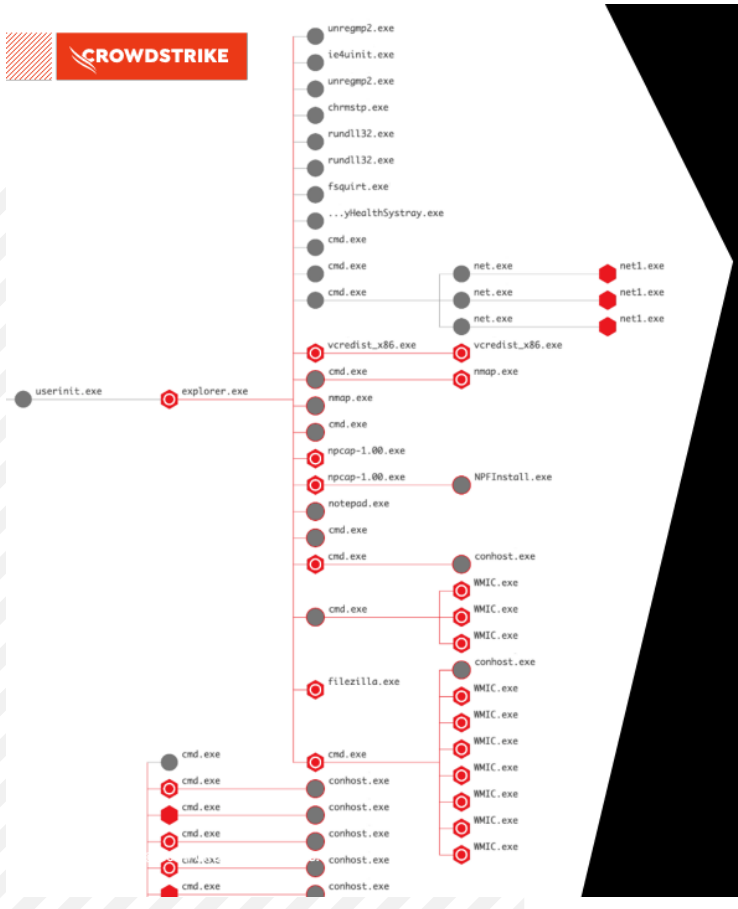
CROWDSTRIKE

TIPS

HOW TO PRODUCE (RECONSTRUCT) BETTER

- Have company-approved report formats and stick to them
- Practice writing technical reports – develop your ability to tell a story concisely
- Understand how to take screen shots from Falcon – it has already created the visuals for you
- Include temporal analysis as often as possible
- Peer review EVERYTHING!
- Appoint someone to be the last "eyes" on the report – consumers shouldn't be surprised by changes in language and format

CROWDSTRIKE UNIVERSITY



RECONSTRUCT

- Tying data together is critical to understanding the threat
- Automated ThreatGraph querying provides useful visualization of events
- Cloud performance built to withstand multiple simultaneous, sophisticated queries
- Temporal analytic views inherent in many Insight and Investigate pages

CROWDSTRIKE UNIVERSITY

S.E.A.R.C.H. TIPS

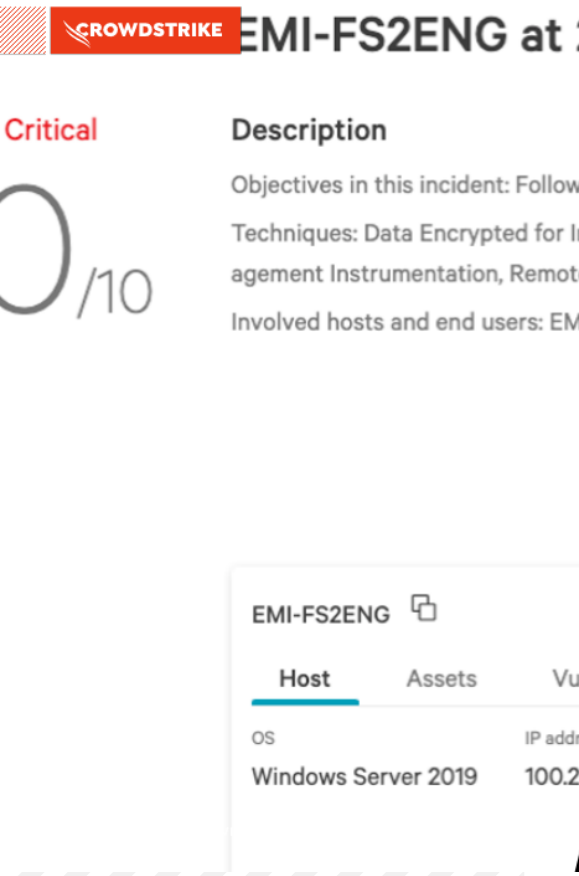
CROWDSTRIKE

TIPS

HOW TO PRODUCE (COMMUNICATE) BETTER

- Know your consumers – who are they and what information do they NEED?
- Understand the level of detail each of your customers need
- Develop hand-off procedures within the team for large/important hunts and incidents
- Keep metrics – they tell a story that managers understand
- Have reporting timing policies – at what point do you inform IR? Inform legal? Report to execs?
- Decide what stays internal and what should be shared with the community

CROWDSTRIKE



COMMUNICATE

- OverWatch analysis is incorporated into many parts of Falcon
- We won't fully benefit from all of OverWatch's insight without an OverWatch subscription
- But, Falcon includes other ways that our team members can share and communicte in the portal

S.E.A.R.C.H. TIPS

CROWDSTRIKE

TIPS

HOW TO THREAT HUNT BETTER

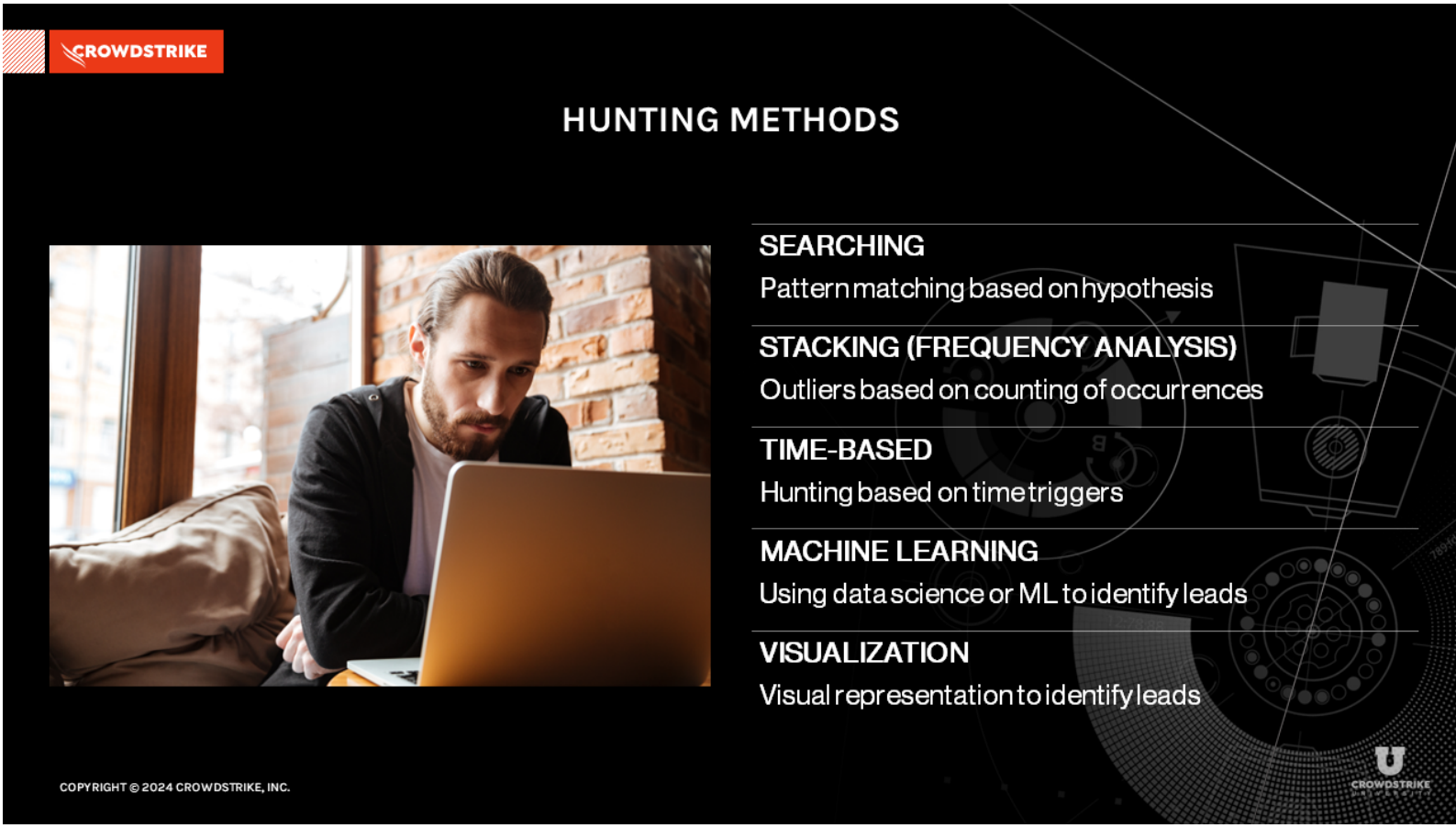
- Study your own team's reporting – actually use your lessons learned
- Study open source reporting – use others' lessons learned
- Include up-to-date threat intelligence – this is a moving target
- Continually refine your processes – WRITE IT. DOWN.
- Consider outside consulting to evaluate your team
- If you manage – get your team to cons and training

CROWDSTRIKE

HONE

- Continuous improvement of tools and processes
- Threat intelligence must be:
  - Up-to-date
  - Deeply analytic
  - Contextual
  - Accessible
- Training is key:
  - Table-top exercises
  - CTF events
  - Emerging forensic techniques

HUNTING METHODS



THREAT HUNTING METHODOLOGIES TIPS

TIPS

There are many types of hunting – automated hunts often involve machine learning; manual hunts usually start with a hypothesis and use searches of data stores.

Good utilization of the hypotheses cycle is critical; pattern-matching and stacking queries are essential for proving/disproving the hypotheses.

Organizations with a mature hunting capability use routine procedures before, during, and after the hunt; have an SOP for your hunts.

Problem statements are opportunities for hypotheses development; we create concise problem statements to frame the issue for better understanding.

HUNTING METHODS
Hypotheses Generation

CROWDSTRIKE

HYPOTHESES
"MAKING AN EDUCATED GUESS"

- Must be TESTABLE
  - To be testable, must include at least one variable
  - Hunters must know where the data is and have the ability to access it
- Must clearly state an end result or product that is reachable
- Often starts with the identification of a problem
  - Creation of a PROBLEM STATEMENT helps us narrow down the exact answer we need

HUNTING METHODS
Frequency Analysis

CROWDSTRIKE

FREQUENCY ANALYSIS - CQL EXAMPLE

```
#event_simpleName=ProcessRollup2
| groupBy(CommandLine)
```

CommandLine	_count ↑
C:\Windows\system32\DllHost.exe /Processid:{F9717507-6651-4EDB-BFF7-AE615179BCCF}	44
taskhostw.exe	43
"C:\Windows\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca	41
/0000000c	40
C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}	34
"C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /ua /installsource scheduler	29
C:\Windows\system32\svchost.exe -k netsvcs -p -s wuauserv	25
C:\Windows\system32\TSTheme.exe -Embedding	25
C:\Windows\system32\svchost.exe -k wsappx -p -s AppXSvc	17
C:\Windows\servicing\TrustedInstaller.exe	16
C:\Windows\System32\svchost.exe -k netsvcs -p -s NetSetupSvc	16
"C:\Windows\system32\SearchFilterHost.exe" 0 680 684 692 8192 688	16
taskhostw.exe KEYROAMING	15
C:\Windows\system32\compattelrunner.exe -m:aeinv.dll -f:UpdateSoftwareInventoryW	15
C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s WinHttpAutoProxySvc	12

1 2 3 4 5 6 7 ... 18

HUNTING METHODS
Frequency Analysis

CROWDSTRIKE

FREQUENCY ANALYSIS - CQL EXAMPLE

```
groupBy([ComputerName, FileName], function=collect([DomainName, MD5HashData, SHA256HashData], limit=100))
```

ComputerName	FileName	DomainName	MD5HashData	SHA256HashData
SE-SWH-RDP	taskhostw.exe	settings-win.data.microsoft.com	8bd7b08da6bca54df9b595e4d9281beb	de85f29a8bc7219f10a4ac88654c3901abc329d7505
FC-JBE-RDP	svchost.exe	download.windowsupdate.com geo.prod.do.dsp.mp.microsoft.com login.live.com cp601.prod.do.dsp.mp.microsoft.com fe2.update.microsoft.com fe3.delivery.mp.microsoft.com kv601.prod.do.dsp.mp.microsoft.com	4dd18f001ac31d5f48f50f99e4aa1761	2b105fb153b1bcd619b95028612b3a93c60b953eef6
SE-TMA-RDP	GoogleUpdate.exe	edgedl.me.gvt1.com update.googleapis.com clients2.google.com	94c4c8130e96785dd19b70a0fc1088f6	41793f27b823dbc1593df93b3181d0ae08cbbfe16ea
SE-SLT-RDP	taskhostw.exe	settings-win.data.microsoft.com	8bd7b08da6bca54df9b595e4d9281beb	de85f29a8bc7219f10a4ac88654c3901abc329d7505
SE-JBE-WIN10-CO	svchost.exe	settings-win.data.microsoft.com slscr.update.microsoft.com time.windows.com login.live.com tsfe.trafficshaping.dsp.mp.microsoft.com fs.microsoft.com	9520a99e77d6196d0d09833146424113	dd191a5b23df92e12a8852291f9fb5ed594b76a28a5

CROWDSTRIKE

FREQUENCY ANALYSIS - CQL EXAMPLE

Example Search

```
#event_simpleName=NetworkConnectIP4 RemoteAddressIP4!=10.1.0.0/8
RemoteAddressIP4!=127.0.0.1
| join({#event_simpleName=ProcessRollup2}, field=[ContextProcessId],
key=TargetProcessId, include=[CommandLine] , mode=left)
| groupBy([ComputerName, RemoteIP, RPort, CommandLine])
| sort(_count, order=asc, limit=20000)
```

HUNTING METHODS
Temporal Analysis

CROWDSTRIKE

TEMPORAL ANALYSIS

- Examination of events in a chronological order
- Modeling of a variable's behavior in a data set over time
- Statistical analysis differentiation over time intervals

Process executions 601 items

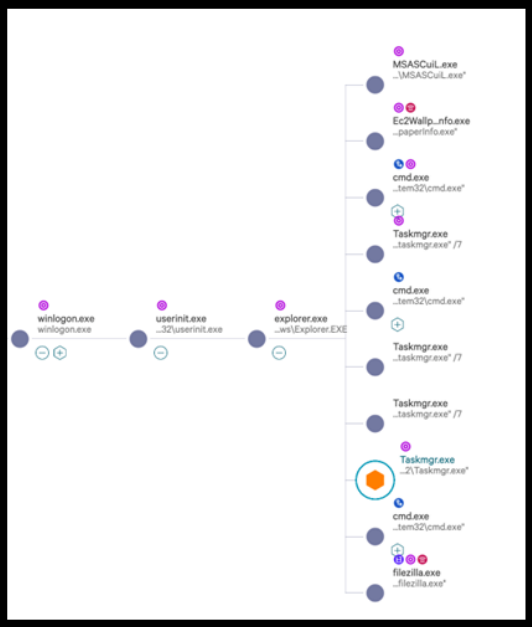
Filename | Command line | Excluded filename(s) | Excluded command line(s) | Exclude common processes | Apply

View in Advanced event search | Export

Time (UTC)	Computer...	Username	Filename	PID	Process ID	Command...	MD5	Parent file...	Pare...	Parent pr...	Parent co...
2024-01-04T19:58:48Z	EMI-WRKSTN...	EMI-WRKSTN...	SearchProtocolHos...	5264	4626275776	"C:\Windows\...	ae2b338f1629...	SearchIndexe...	4348	20651518	C:\Windows\s...
2024-01-04T19:58:48Z	EMI-WRKSTN...	EMI-WRKSTN...	SearchFilterHost.exe	928	4627266771	"C:\Windows\...	4281c1c543de...	SearchIndexe...	4348	20651518	C:\Windows\s...
2024-01-04T19:50:49Z	EMI-WRKSTN...	EMI-WRKSTN...	CSFalconService.exe	7028	4624597880	"C:\Program F...	0a19e2bbffa8...	CSFalconServ...	8468	4297332924	"C:\Program F...
2024-01-04T19:47:43Z	EMI-WRKSTN...	michael.rivas	dllhost.exe	4028	4623582852	C:\Windows\s...	2d29c0afcc8...	svchost.exe	940	12002012	C:\Windows\s...
2024-01-04T19:47:38Z	EMI-WRKSTN...	michael.rivas	backgroundTaskH...	7252	4622507671	"C:\Windows\...	00bdeae44f0...	svchost.exe	940	12002012	C:\Windows\s...
2024-01-04T19:47:13Z	EMI-WRKSTN...	michael.rivas	dllhost.exe	10552	4621513393	C:\Windows\s...	2d29c0afcc8...	svchost.exe	940	12002012	C:\Windows\s...

CROWDSTRIKE

TEMPORAL ANALYSIS - TIME CHART



	Event t...	Proces...	Command line	Status	Duration
Jan. 4, 2024 13:57:45	Proces...	... gr.exe	...:\Windows\System32\Taskmgr.exe"	Not ru...	1m 14s

	Event t...	Image file name	Target file name	SHA256
Jan. 4, 2024 13:57:56	DLL / ...	... e2\Windows\System32\version.dll	--	--
Jan. 4, 2024 13:57:56	DLL / ...	... e2\Windows\System32\dbgcore.dll	--	--
Jan. 4, 2024 13:57:56	DLL / ...	... e2\Windows\System32\dbghelp.dll	--	--
Jan. 4, 2024 13:57:56	DLL / ...	...me2\Windows\System32\verifier.dll	--	--
Jan. 4, 2024 13:57:56	DLL / ...	...lume2\Windows\System32\psapi.dll	--	--

HUNTING METHODS
Temporal Analysis

CROWDSTRIKE

TEMPORAL ANALYSIS - TIME CHART

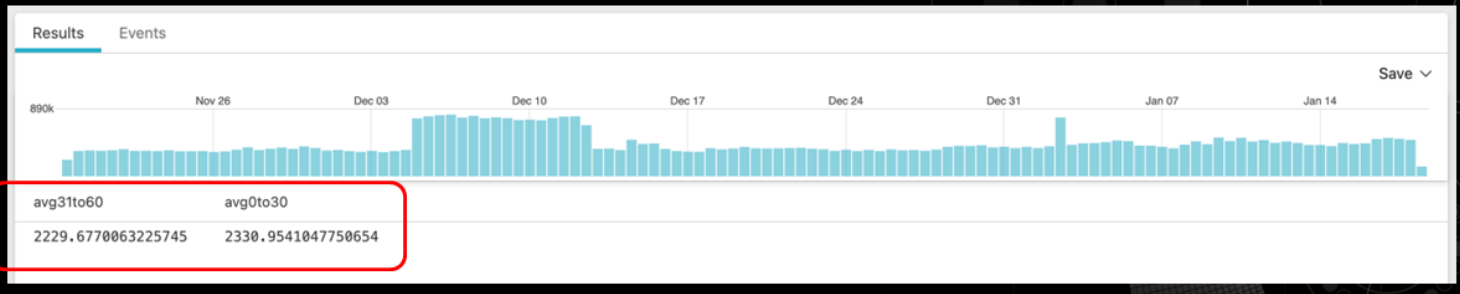
```
timechart(function=[avg ConfigStateHash, as=avgConfigStateHash), avg ConnectTime, as=avgConnectTime)]
```

CROWDSTRIKE UNIVERSITY

CROWDSTRIKE

TEMPORAL ANALYSIS - INTERVALS

```
// Run this query over the last 60 days.
#event_simpleName = ProcessRollup2
| case {
   test(@timestamp < (start()+(30*24*60*60*1000))) | eventSize(as=eventSize31to60);
   * | eventSize(as=eventSize0to30);
}
| stats([avg(as=avg31to60, field=eventSize31to60), avg(as=avg0to30, field=eventSize0to30)])
```



CROWDSTRIKE UNIVERSITY

HUNTING METHODS
Machine Learning

CROWDSTRIKE

UNDERSTANDING THE THREAT GRAPH

		Actual Values	
		Positive	**Negative**
Predicted Values	**Positive**	True Positive (TP)	False Positive (FP)
	Negative	False Negative (FN)	True Negative (TN)

- **True Positive:** *The model correctly predicted a file was malicious*
- **True Negative:** *The model correctly predicted that a file was not malicious*
- **False Positive:** *The model incorrectly predicted that a file was malicious (and it wasn't)*
- **False Negative:** *The model incorrectly predicted that a file wasn't malicious (and it was)*

CROWDSTRIKE UNIVERSITY

CROWDSTRIKE

MACHINE LEARNING IN FALCON

```
#repo: detections
#type: falcon-raw-data
@id: ikILlPL2zEx5DPxRcMIC0fRT_26_64_1704403577
```

```
PatternDispositionValue: 33024
PatternId: 10378
ProcessEndTime: 0
ProcessId: 4493377033
ProcessStartTime: 1704403540
SensorId: 0e05b927e42346848b12caa677140742
Severity: 4
SeverityName: High
SHA1String: 0000000000000000000000000000000000000000
SHA256String: 4e3b5c5f42afbc601982cd49b723b493da0928d753548c7ed5e25927a597835b
Tactic: Defense Evasion
tactic: Defense Evasion
Technique: Disable or Modify Tools
technique: Disable or Modify Tools
timestamp: 2024-01-04T21:26:17Z
UserName: theplague
UTCTimestamp: 1704403577000
```

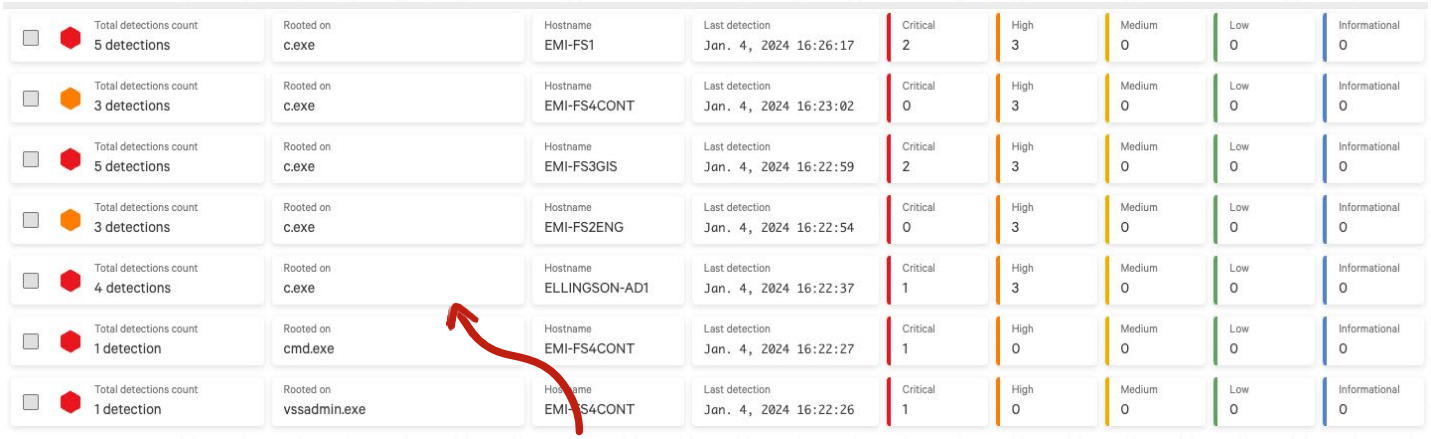

CROWDSTRIKE UNIVERSITY

VISUALIZATIONS

Falcon is mainly built on visualizations of ThreatGraph data

Visual aids in Falcon

Iconography – Use of Icons to highlight key items of the process node activity
Colorization – Different colors used for things such as detection criticality
Proximal context - showing the inter-relationships between the different nodes in the detection tree, such as Parent/Child and Sibling relationships
Aggregation - bringing it all together in a common viewpoint, i.e. the process Tree views



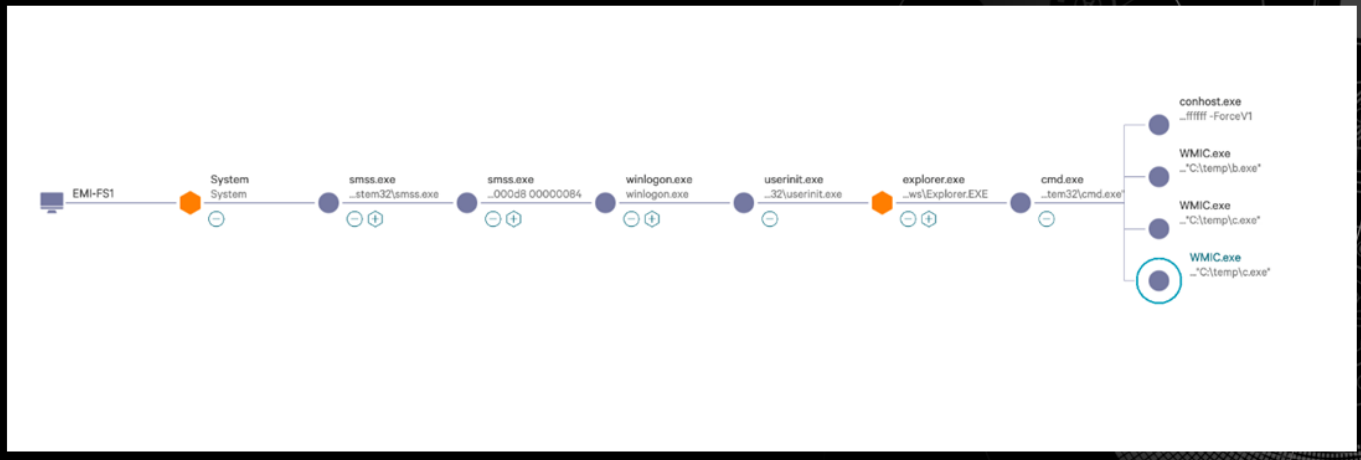
Falcon reports, dashboards, and other visualizations contain contextual pairings of charts, timelines, matrices, diagrams, lists, and more. This detection view is both a list and a timeline.

Advanced Hunting in EDR Data

CROWDSTRIKE

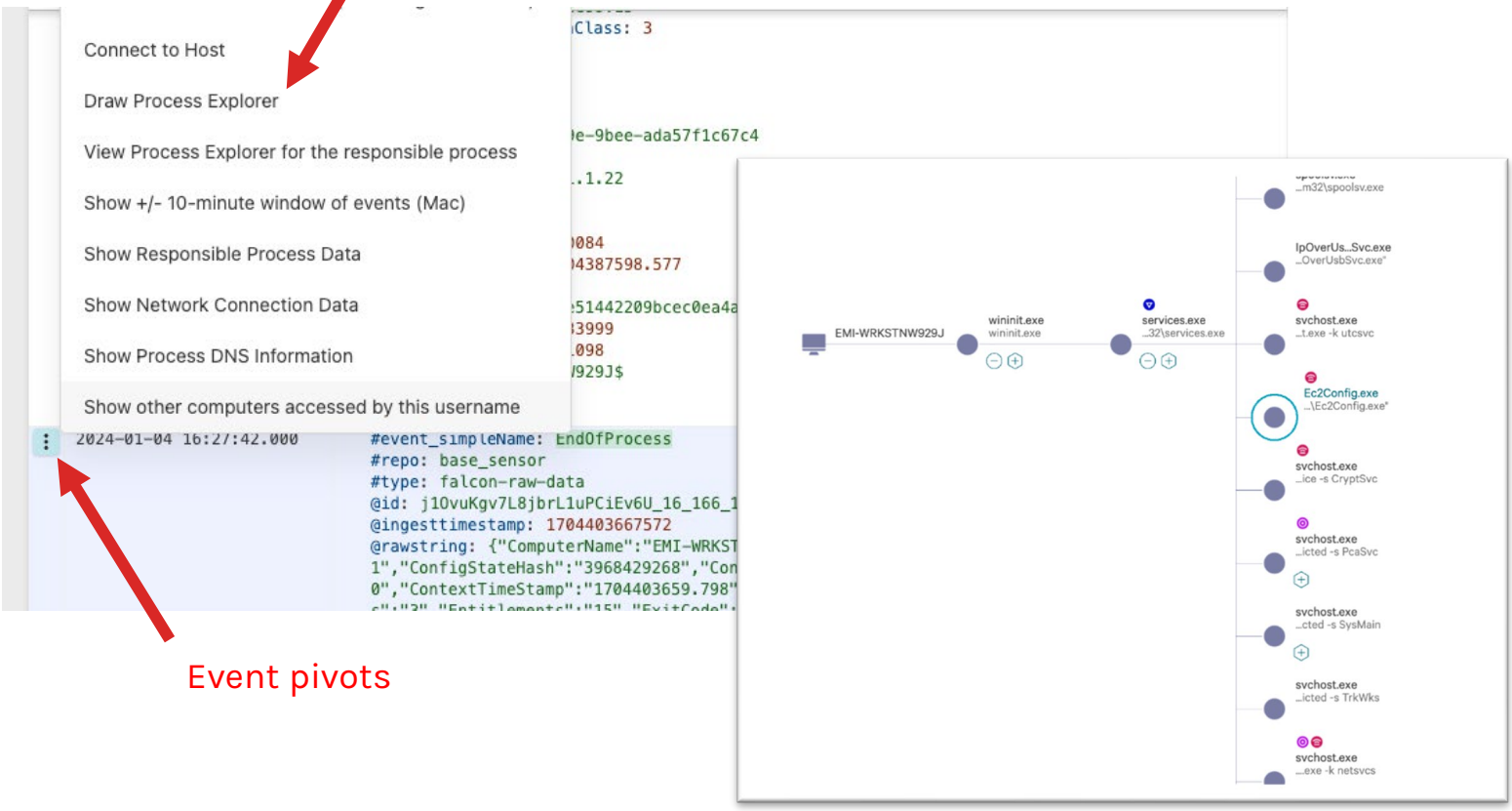
TRIAGE – THE IMPORTANCE OF PROCESS TREES

- Critical to understand the process tree:
  - Process relationships
  - Start times, stop times, and duration of processes
- Temporal analysis of process events (Timelining) around a given event



CROWDSTRIKE

Process trees with no detections



Event pivots

Advanced Hunting in EDR Data

Endpoint Detection & Response Data

Important data retention periods:

- Detections, Incidents, and other visual aids generally available for 90 days
- EDR data is available for your organization's retention agreement – generally 7 or 30 days
- End point/Falcon agent information is available for **45 days**
- Build advanced queries to find context
- For advanced threat hunting, it is often best to incrementally piece together your query

Example Search

```
aid=a4c18e8bf47a4003924cf55978533e72 #event_simpleName=NetworkConnectIP4
RemoteIP!=10.1.0.0/16 RemoteIP!=127.0.0.1
| join({#event_simpleName=ProcessRollup2}, field=[ContextProcessId],
key=TargetProcessId, include=[CommandLine] , mode=left)
| groupBy([ComputerName, RemoteIP, RPort, CommandLine])
```

EDR SEARCHES

Pivoting and Filtering

Example Search

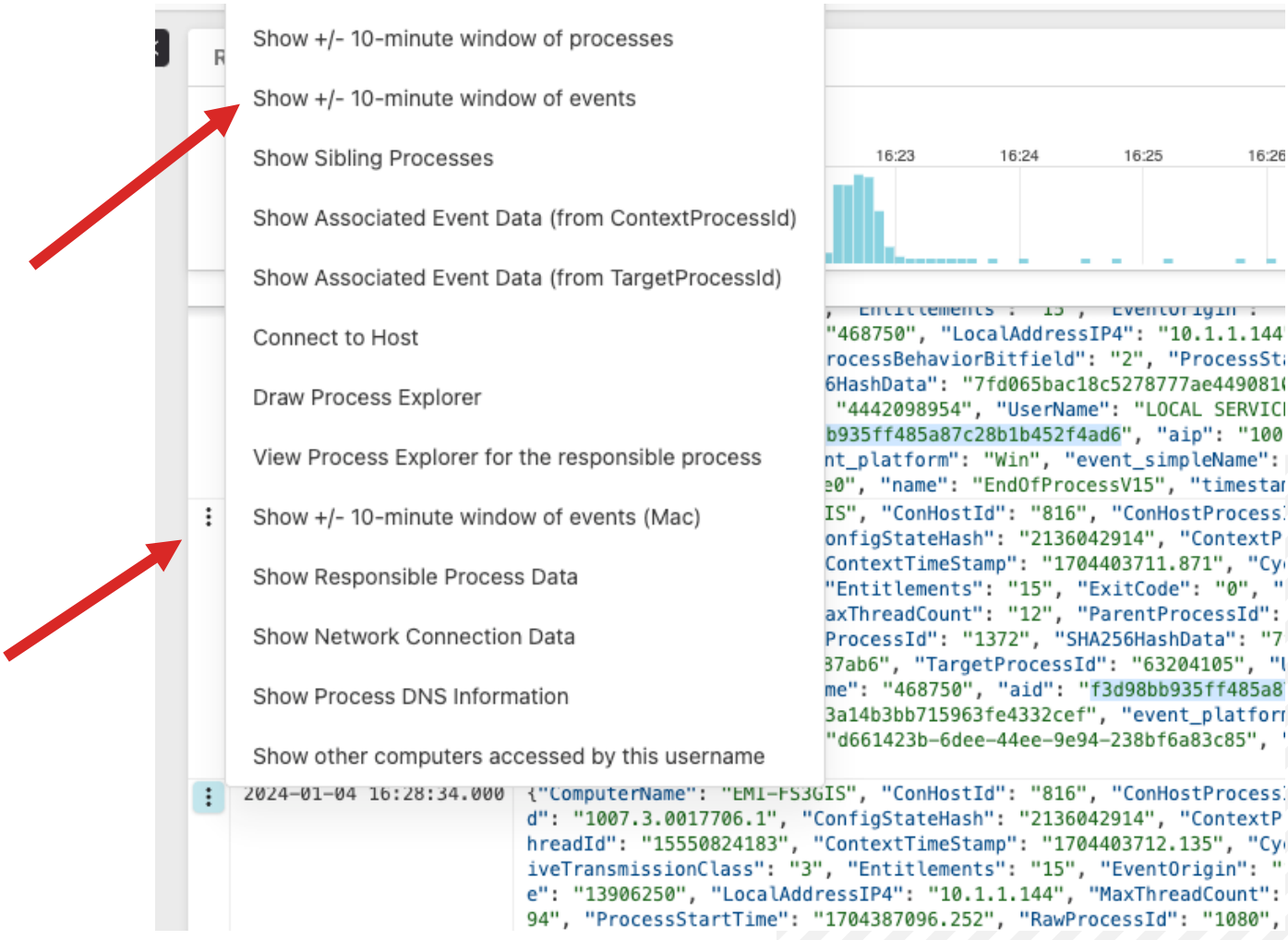
```
aid=a4c18e8bf47a4003924cf55978533e72
#event_simpleName=NetworkConnectIP4
RemoteIP!=10.1.0.0/16 RemoteIP!=127.0.0.1
| join({#event_simpleName=ProcessRollup2},
field=[ContextProcessId], key=TargetProcessId,
include=[CommandLine] , mode=left)
| groupBy([ComputerName, RemoteIP, RPort,
CommandLine])
```

Threat hunting is largely an exercise of anomaly detection and pivoting
We find something, we pivot our hunt to follow the leads

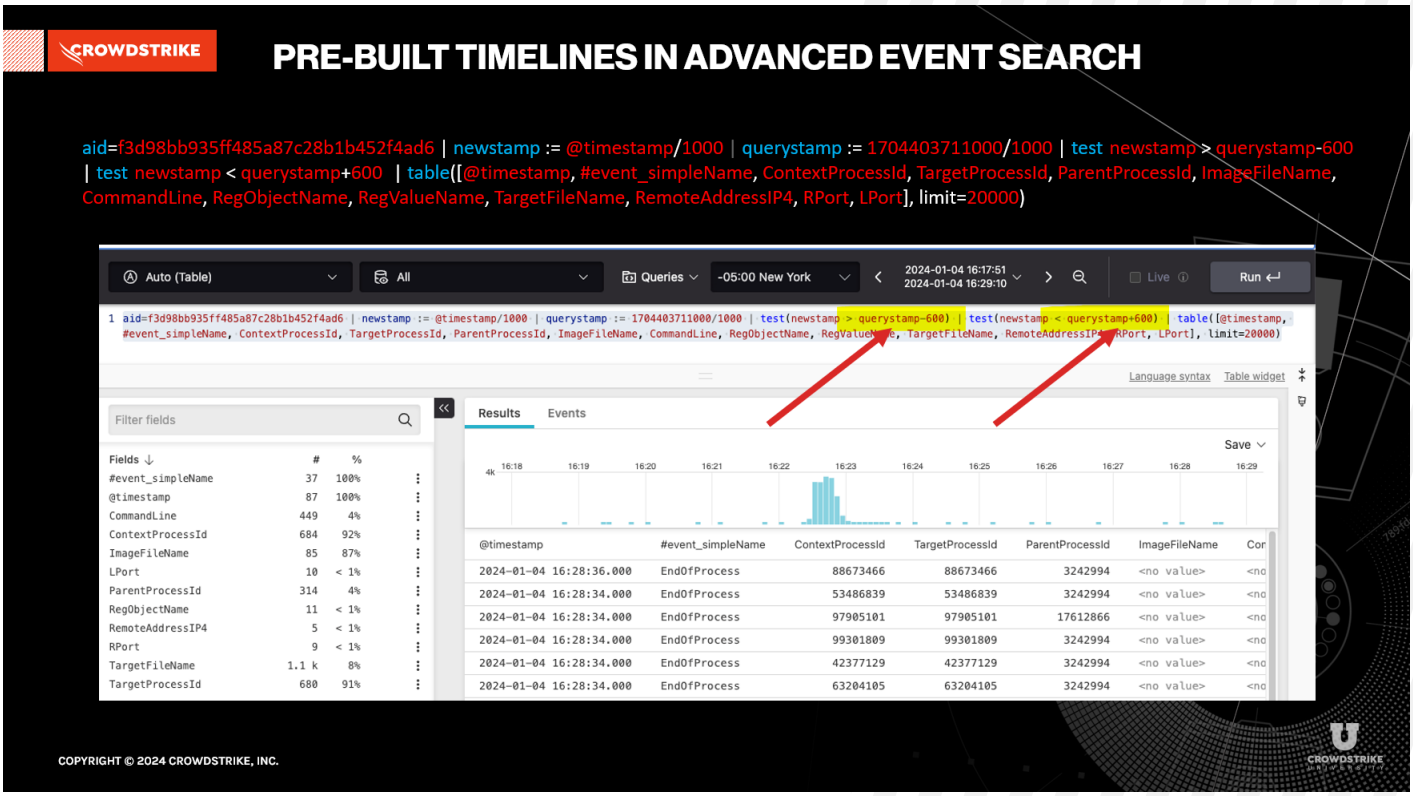
Reduction in noise or the amount of data to analyze is critical for efficiency

In CQL Event Search, it can come in several forms:
field!=value field!=value)
field!=[value, value, value, value]

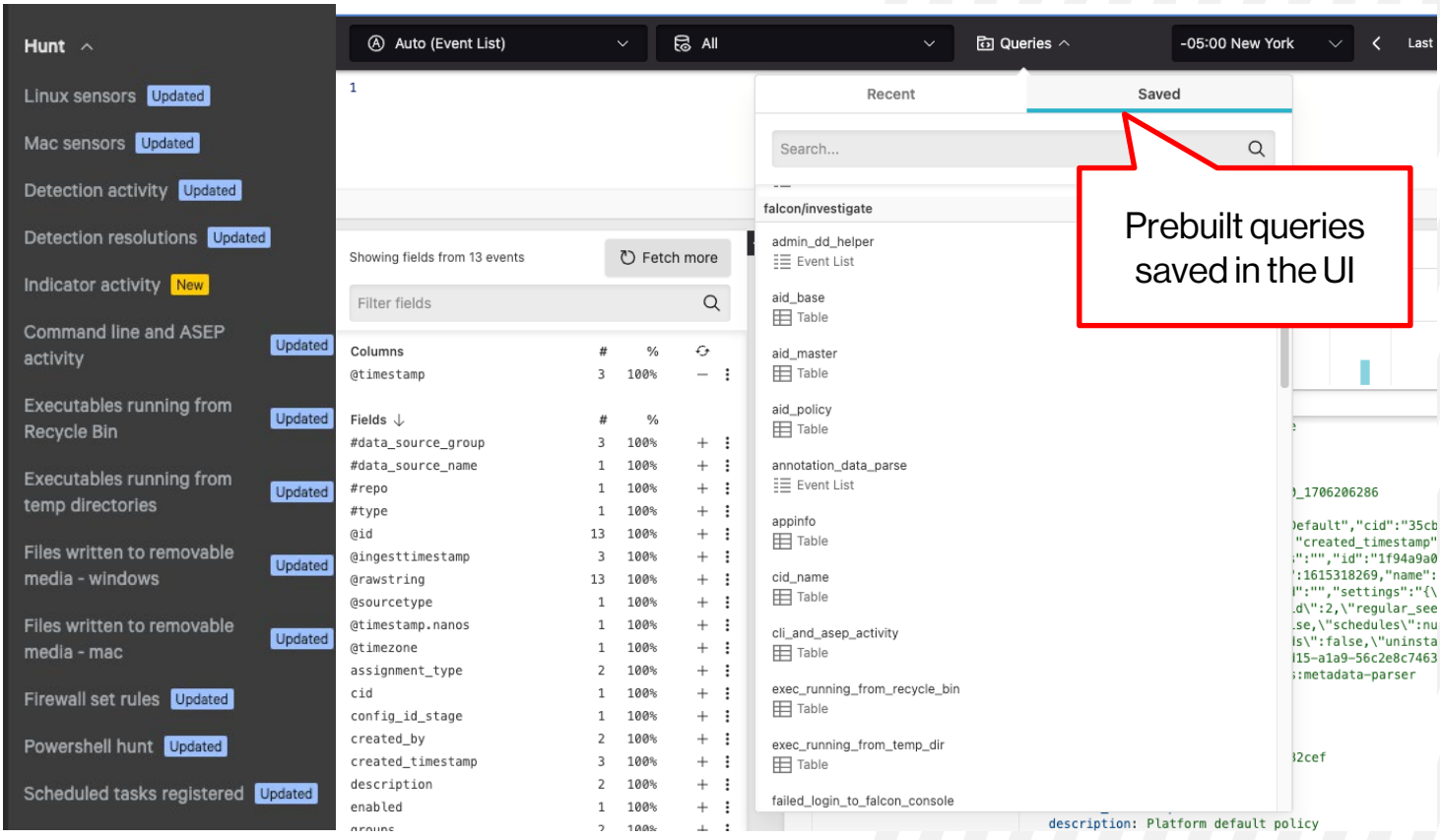
Prebuilt timelines in Advanced event search



EDR SEARCHES



HUNTING EDR FOR ENTERPRISE TRIGGERS



INTELLIGENCE MODELS

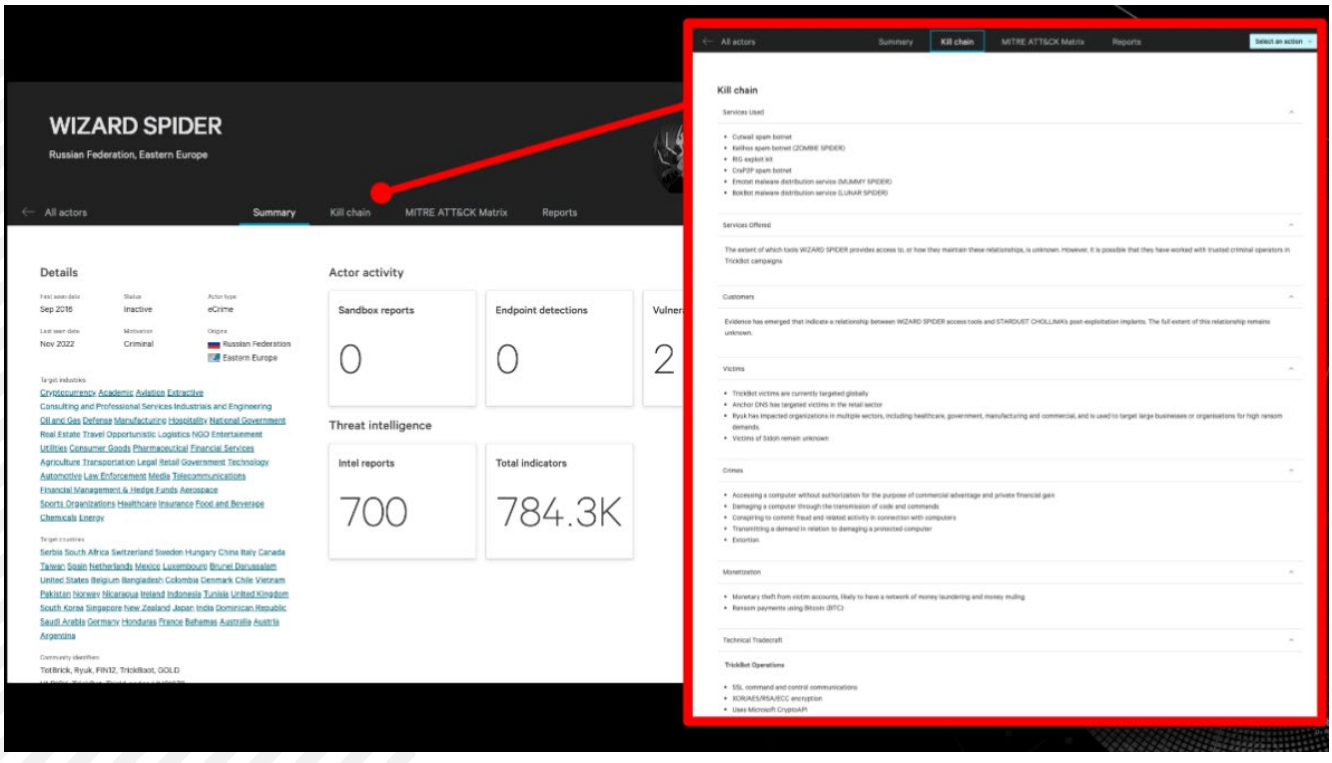
The Cyber Kill Chain model identifies what the adversaries must complete in order to achieve their objective.

CROWDSTRIKE

LOCKHEED'S SEVEN WAYS TO USE THE CYBER KILL CHAIN ®

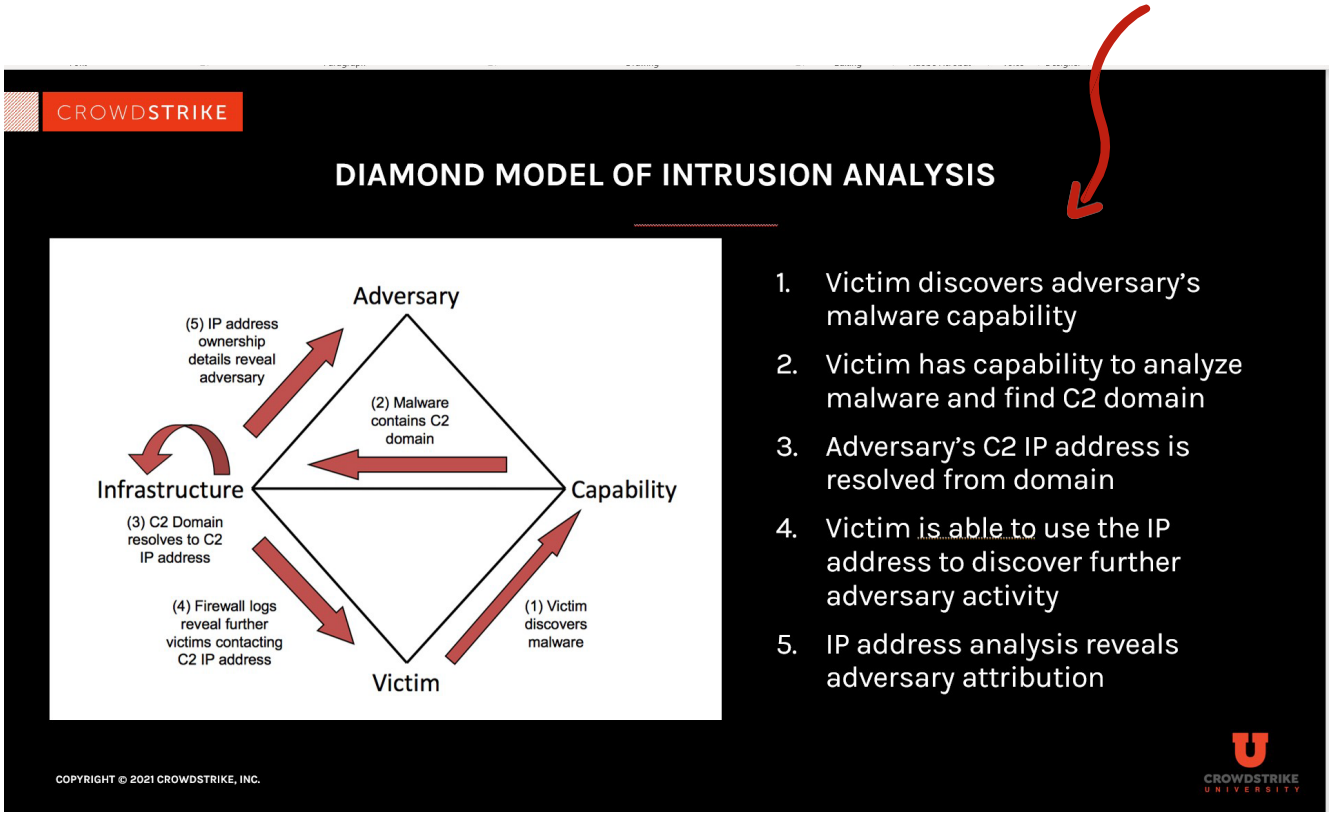
1. Prioritize Sensor Alerts
   - Detections mapped to latter stages of the kill chain should have higher priority
   - Should be automatically associated with other threat info in a threat platform
2. Prioritize Escalation
   - Detections of adversary activity that map to certain points in the kill chain should require escalated response – up to executive notification – this is a function of the SOP
3. Prioritize Investment
   - Create a two-dimensional graph outlining mitigation tools available to IR, mapped to each stage of the kill chain
4. Measure Effectiveness
   - Analysis of mitigated attacks should concentrate on the stage at which the attack was discovered and stopped, then build capability to stop earlier
5. Measure Resilience
   - Analyze mitigated attacks to assess if later stages would have caught it, if the stage at which it was actually stopped would have failed
6. Measure Analytic Completeness
   - Analyze the entire chain – even if the attack was stopped; understand what the actor would have done
7. Identify and Track Campaigns
   - Create a scorecard to provide insight into defensive effectiveness against an actor or across all actors

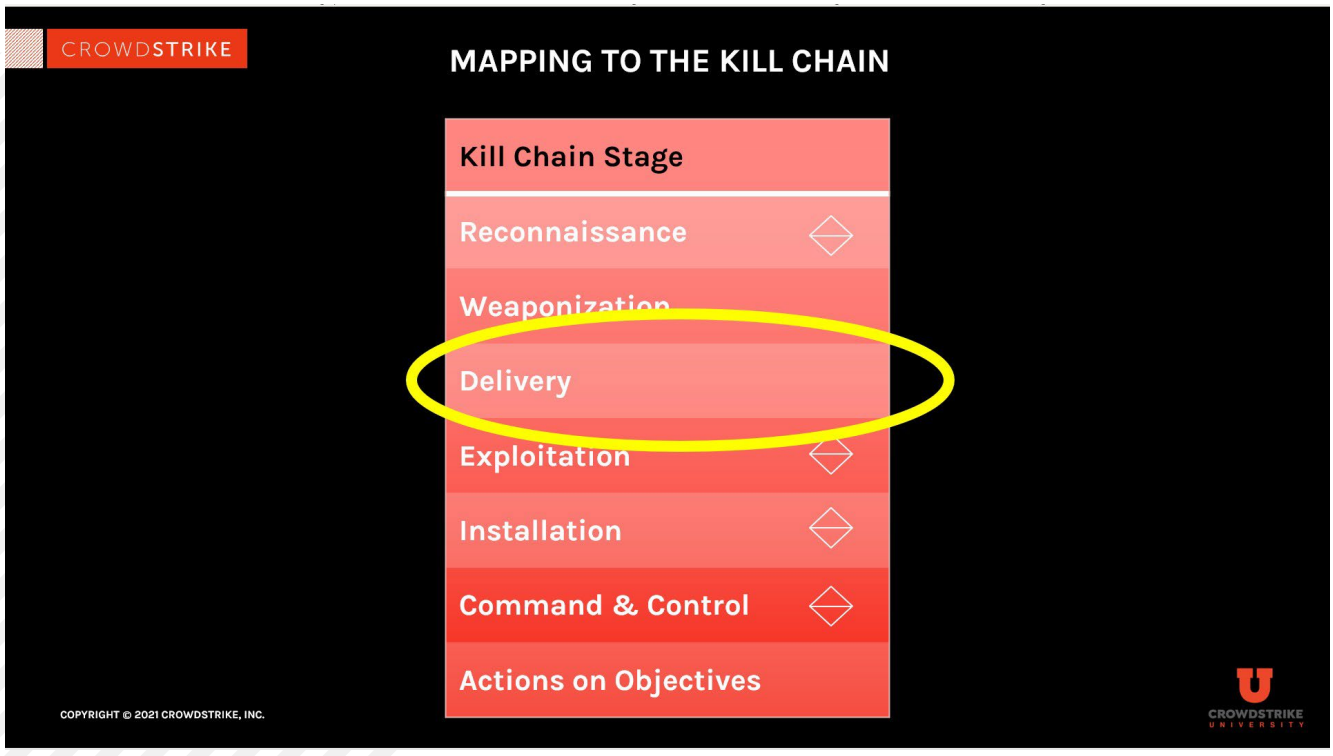
How Falcon applies the Cyber Kill Chain



INTELLIGENCE MODELS

The Diamond Model is "Used to describe an EVENT where an ADVERSARY takes a step towards an intended goal by using a CAPABILITY over INFRASTRUCTURE against a VICTIM producing a result."





MITRE ATT&CK

Organizations can use the ATT&CK Framework to measure their detection and response capabilities.

CROWDSTRIKE

FALCON AND THE MITRE ATT&CK FRAMEWORK

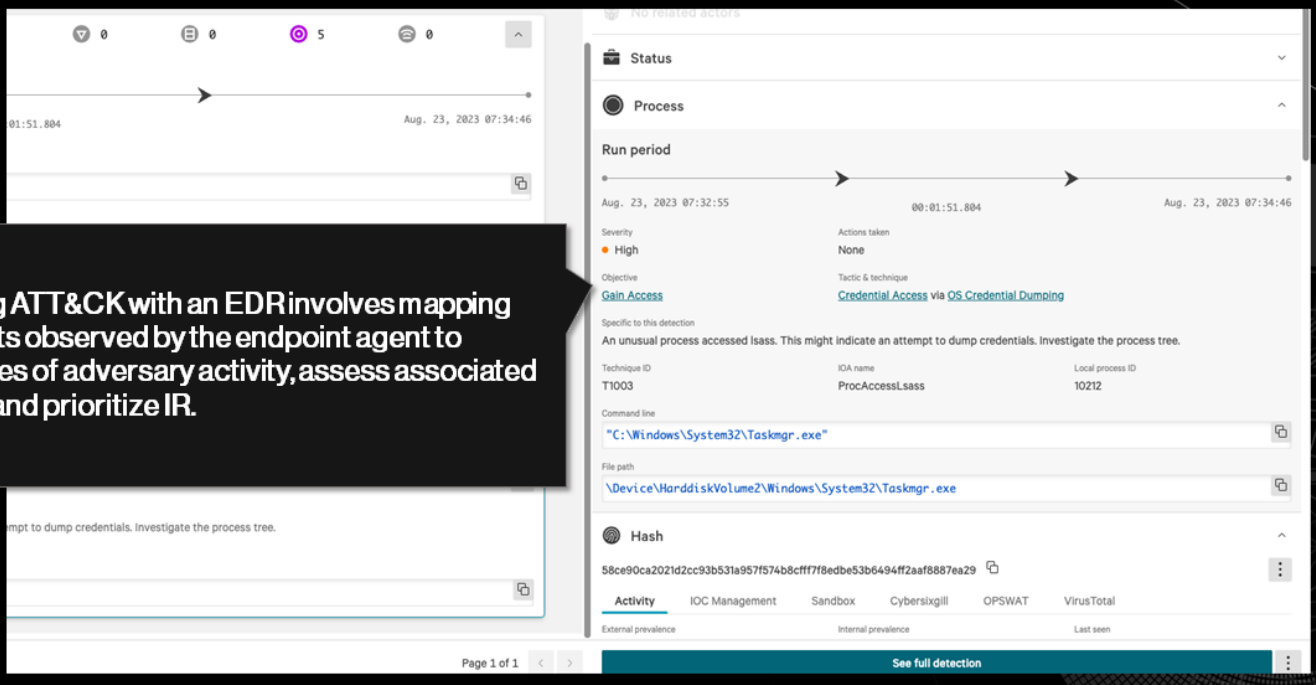
Detection event data is populated in the Falcon ThreatGraph immediately upon sensor identification of an IOA or Falcon Cloud identification of an IOC

Tactic and technique are included in the event data based on pre-mapped patterns

CrowdStrike's ThreatGraph is responsible for piecing together the elements for determinations and matching identified patterns to MITRE ATT&CK tactics and techniques.

CROWDSTRIKE

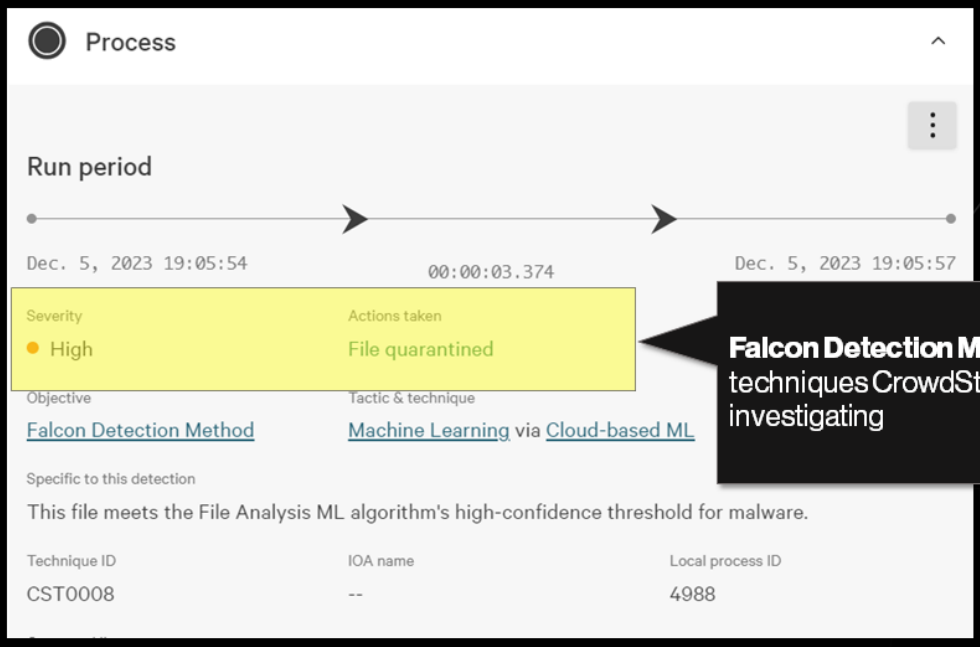
MITRE ATT&CK



Using ATT&CK with an EDR involves mapping events observed by the endpoint agent to phases of adversary activity, assess associated risk, and prioritize IR.

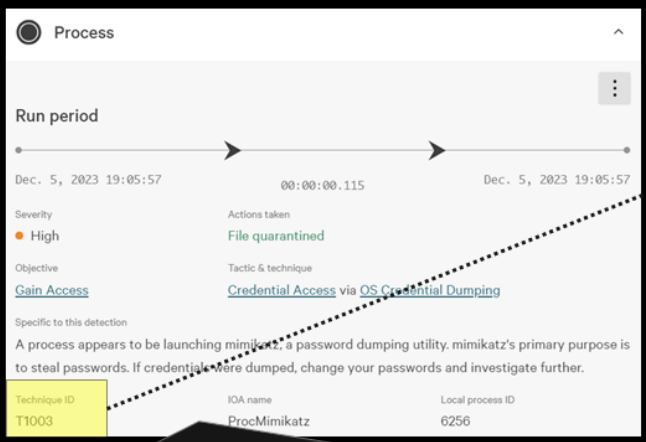
MITRE ATT&CK

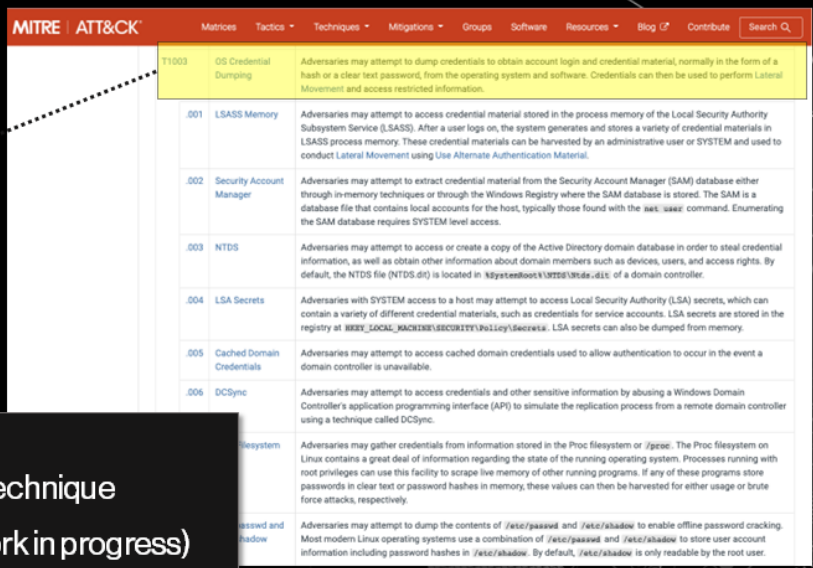
FALCON DETECTION METHOD



Falcon Detection Method (FDM) – a matrix for tactics and techniques CrowdStrike considers malicious and worth investigating

TECHNIQUE ID





Precisely identifies the MITRE ATT&CK Framework technique

Sub-techniques are not yet enumerated in Falcon (work in progress)

MITRE ATT&CK

USING ATT&CK INFO IN DETECTIONS

Assists understanding of what happened and what is next.

Run period

Dec. 5, 2023 19:05:57 — 00:00:00.115 — Dec. 5, 2023 19:05:57

Severity: High
Actions taken: File quarantined
Objective: Gain Access
Tactic & technique: Credential Access via OS Credential Dumping
Specific to this detection
A process appears to be launching mimikatz, a password dumping utility. mimikatz's primary purpose is to steal passwords. If credentials were dumped, change your passwords and investigate further.
Technique ID: T1003
IOA name: ProcMimikatz
Local process ID: 6256

T1003 — OS Credential Dumping
Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.

In this example, we would pivot to looking for **lateral movement.**

We can use the matrix to help build our hypotheses of which technique was most likely.

Credential Access (17 techniques)	Discovery (32 techniques)	Lateral Movement (9 techniques)
Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services
Brute Force (4)	Application Window Discovery	Internal Spearphishing
Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)
Forced Authentication	Cloud Service Dashboard	Remote Services (8)
Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media
Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools
	Container and Resource Discovery	

DETECTION LINKS TO DOCUMENTATION

Run period

Dec. 5, 2023 19:05:57 — 00:00:00.115 — Dec. 5, 2023 19:05:57

Severity: High
Actions taken: File quarantined
Gain Access
Credential Access via OS Credential Dumping
Specific to this detection
A process appears to be launching mimikatz, a password dumping utility. mimikatz's primary purpose is to steal passwords. If credentials were dumped, change your passwords and investigate further.
Technique ID: T1003
IOA name: ProcMimikatz
Local process ID: 6256

Gain Access

Objective Description

Gaining access to your endpoints is a key phase in an adversary's attack strategy. A common way to get in is access, an adversary works to gain more access by escalating privileges on compromised accounts.

Common Tactics – Enterprise

Credential Access

The adversary is trying to steal account names and passwords.
Credential Access consists of techniques for stealing credentials like account names and passwords. Techni legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the

Show Related Techniques

Initial Access

The adversary is trying to get into your network.
Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a netw exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for c limited-use due to changing passwords.

Show Related Techniques

Privilege Escalation

The adversary is trying to gain higher-level permissions.

MORPHOLOGICAL ANALYSIS

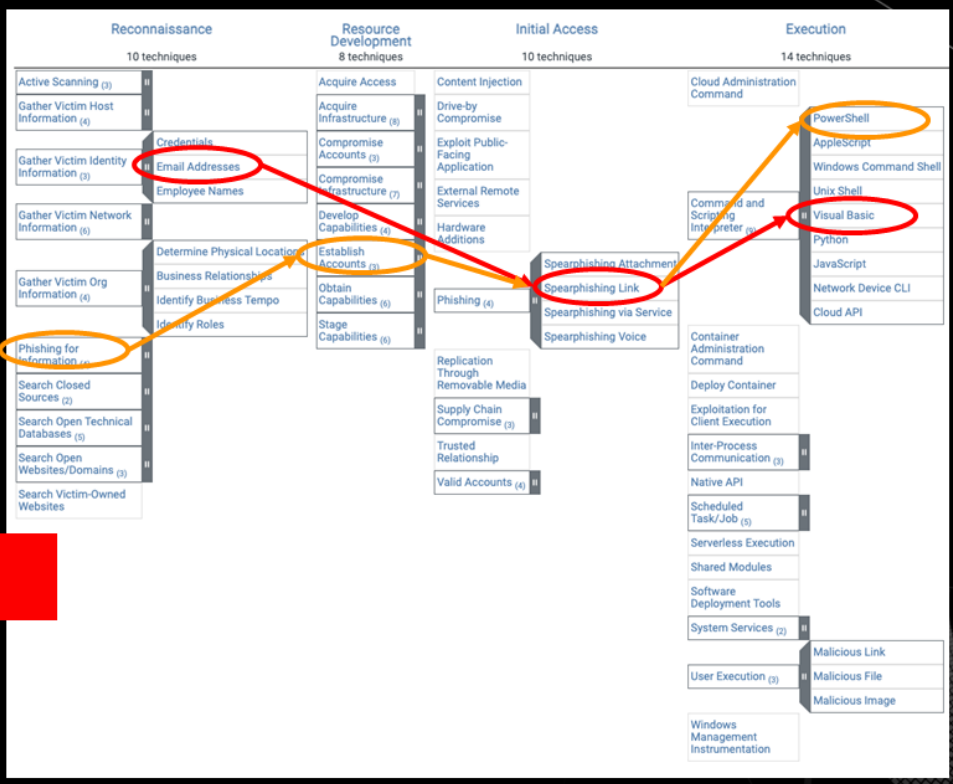
CROWDSTRIKE

POSSIBLE ATTACK PATHS

- While hunting, I found what appears to be a parent-child relationship indicative of a spearphishing attempt
- What do you think are the parent and child processes?
- Majority of analysts would likely say "Outlook to Chrome" - but why?
- You created a hypothesis based on past experience – and you used **morphological analysis** to do it!

CROWDSTRIKE

POSSIBLE ATTACK PATHS



This is just one hypothesis!

MORPHOLOGICAL ANALYSIS

MORPHOLOGICAL REASONING

Identifying a Complete Set of Relationships

Exploring all possible solutions and relationships to a complex, non-quantifiable issue; forces a new way of thinking.

Category:	Imaginative Thinking
Complexity:	Medium
Collaboration:	Individual or Group

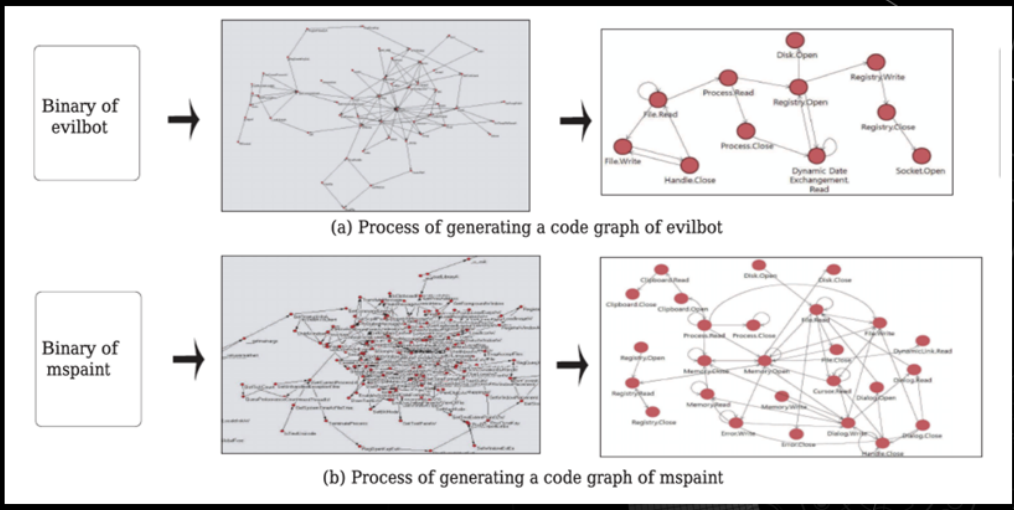
I = Initial energy form
T = Transmission form
S = Final Storage form

I	T	S
K (Kinetic)	K	K
E (Electrical)	E	E
C (Chemical)	C	C
T (Thermal)	T	T
N (Nuclear)	N	N

Figure 2: Energy Conversion Matrix (example)

"ZWICKY-STYLE" MORPHOLOGICAL REASONING

- Problem to be solved must be very concisely formulated
- All parameters that might be of importance must analyzed
- Morphological box or multi-dimensional matrix, which contains all of the potential solutions of the given problem, is constructed
- All solutions contained in the morphological box are evaluated
- Best solutions are selected and are practically applied



(a) Process of generating a code graph of evilbot

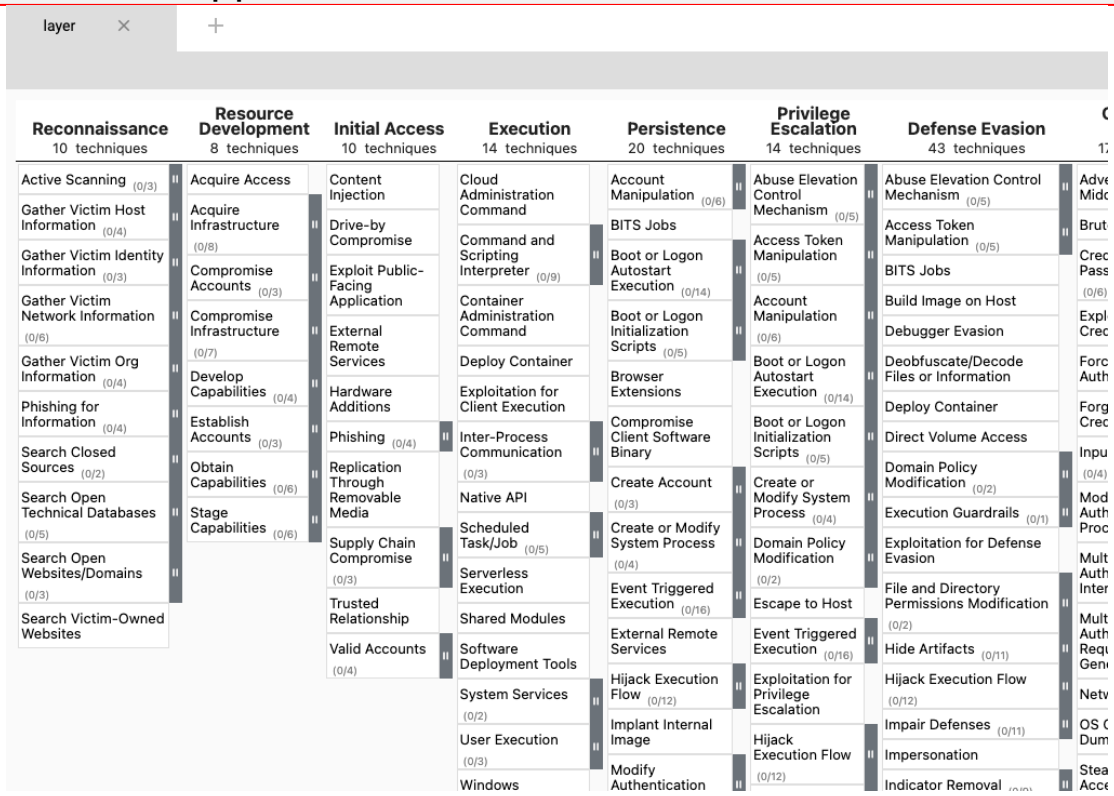
(b) Process of generating a code graph of mspaint

Detecting Metamorphic Malwares using Code Graphs (Jan 2010)
Jusuk Lee, Kyoochang Jeong, and Heejo Lee
Div. of Computer & Communication Engineering
Korea University

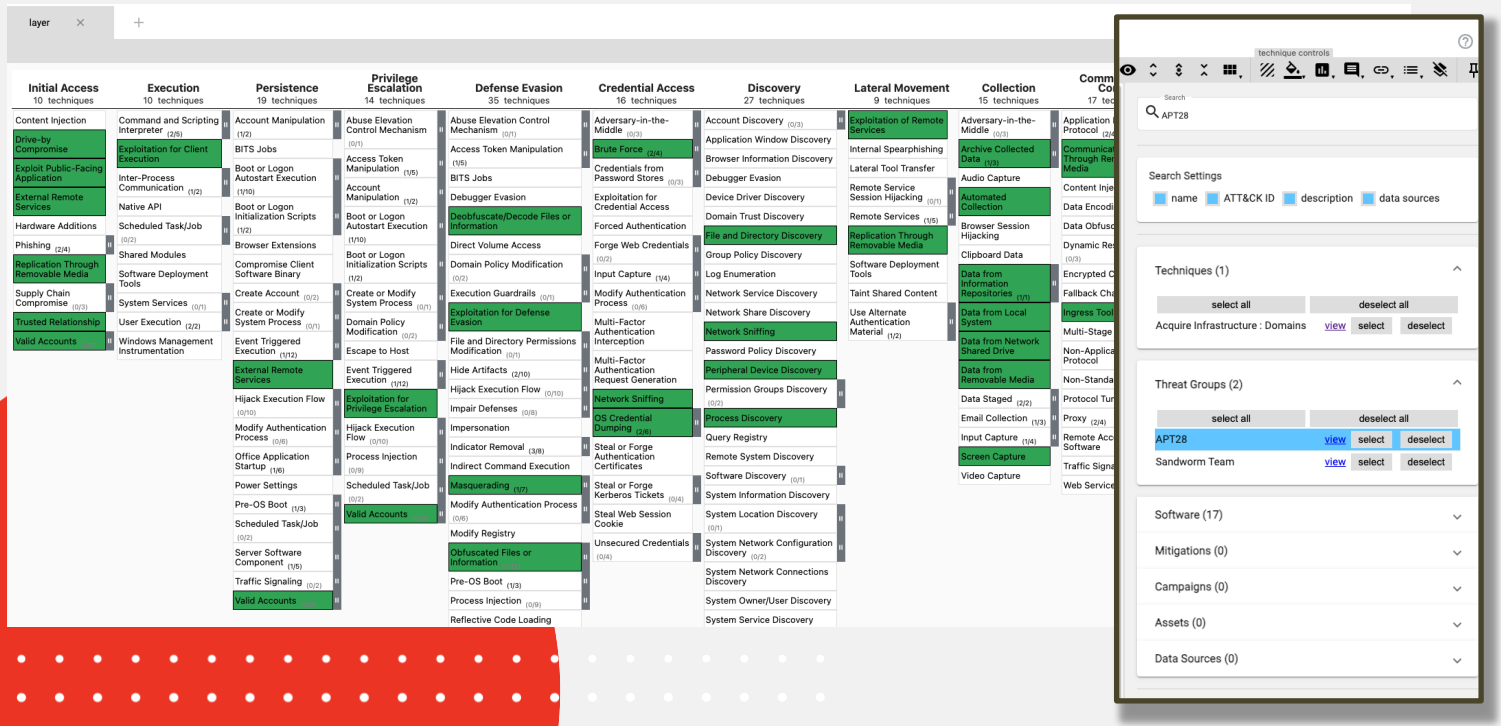
Concept Pioneered by Fritz Zwicky (1966)

ATT&CK NAVIGATOR

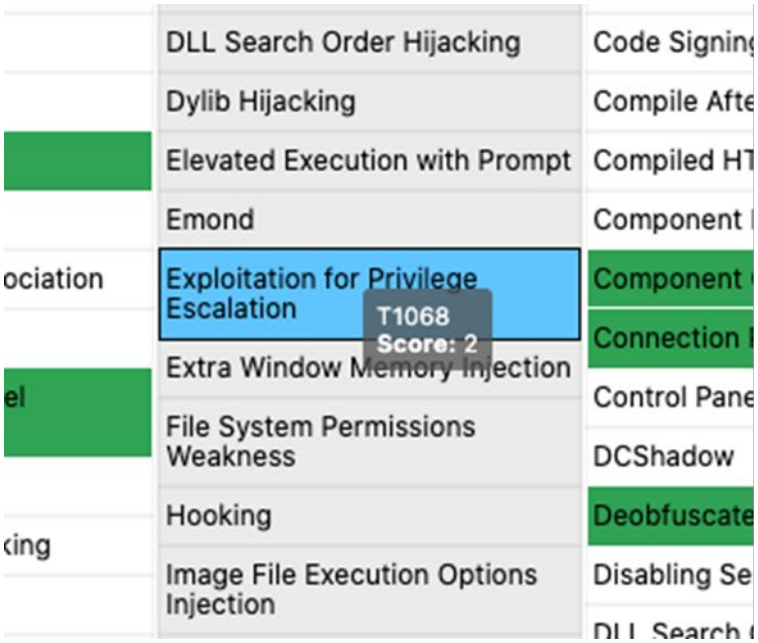
- Provides basic navigation and annotation on ATT&CK matrices
- Allows colorization, enumeration, comments, and the ability to define layers (custom views)
- Hosted webapp at GitHub, but also downloadable to run locally

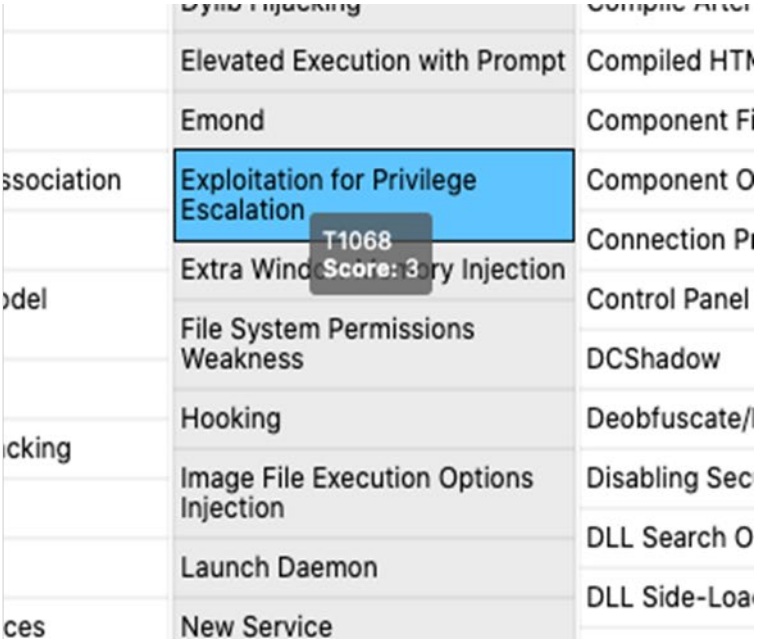


Known Adversary TTP SET



ATT&CK NAVIGATOR
Aggregate Scoring





The ATT&CK Navigator is a great tool to visualize adversary TTPs

ATT&CK NAVIGATOR
Aggregate Scoring

FANCY BEAR x (a) SKELETON SPIDER x (b) new tab x +

MITRE ATT&CK®

Create New Layer — Create a new empty layer

Open Existing Layer — Load a layer from your computer or a URL

Create Layer from other layers — Choose layers to inherit properties from

score expression: a+b — Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found here. Leave blank to initialize scores to 0.

coloring — Choose which layer to import manually assigned colors from. Leave blank to initialze with no colors.

comments — Choose which layer to import comments from. Leave blank to initialize with no comments.

states — Choose which layer to import enabled/disabled states from. Leave blank to initialize all to enabled.

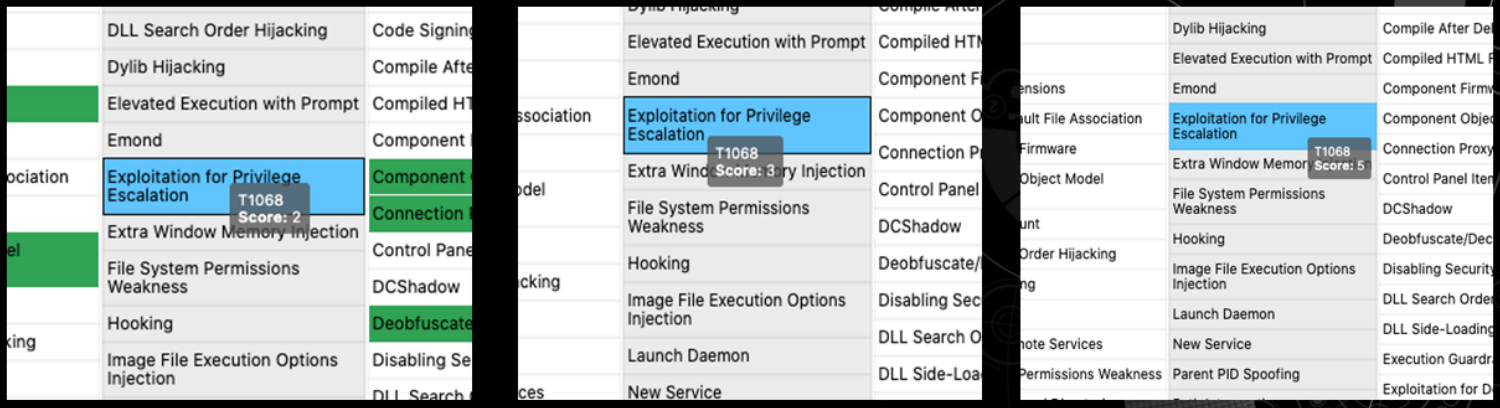
filters — Choose which layer to import filters - stages and platforms - from. Leave blank to initialize with no filters.

legend — Choose which layer to import the legend from. Leave blank to initialize with an empty legend.

Create

Create Customized Navigator — Create a hyperlink to a customized ATT&CK Navigator

A + B = NEW LAYER



THREAT HUNT AUTOMATION

THREAT HUNT AUTOMATION

Tools don't hunt – analysts do

- Tools are only as good as their developer and user
- Tools can only pivot in ways they are taught to pivot
- Tools can only use the context provided to them– they cannot inherently infer context on their own
- Even the best tools don't (yet) think like the human mind, we must supplement with human hunting

FALCON APIs

- Falcon has many APIs – but for this course we are concerned with Threat Graph APIs
- The official documentation has a wealth of information on how to set APIs up and utilize them
- All APIs are based on OAuth2

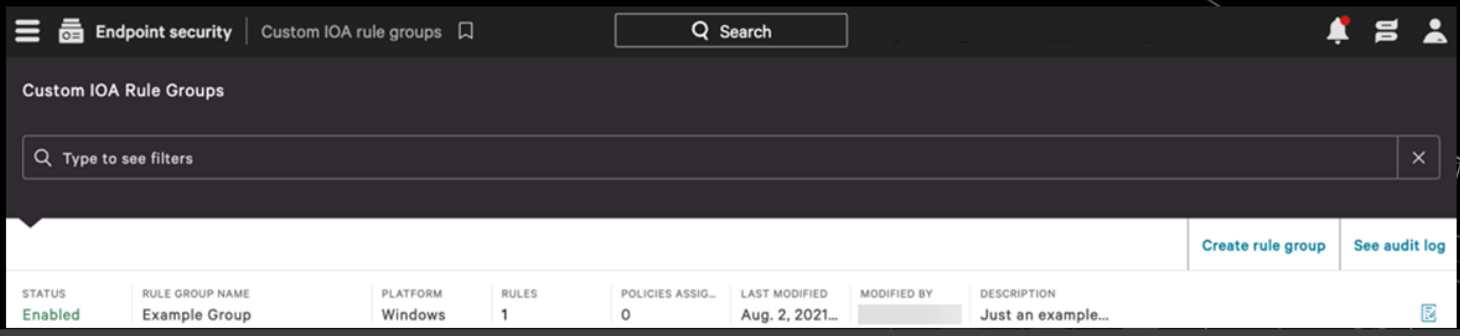
Endpoint Security APIs

Detection and Prevention Policy APIs	Incident, Detection, and Alert Monitoring APIs	Real Time Response APIs
Real Time Response Policy APIs	USB Device Control Policy APIs	Falcon Firewall Management APIs
Zero Trust Assessment APIs	Threat Graph API (key-based)	Windows On-Demand Scanning APIs

APIs can be used in scripting languages like Python or in programs like Postman
Requires support ticket to enable the APIs

THREAT HUNT AUTOMATION

CUSTOM IOAs



With **Falcon Insight:**

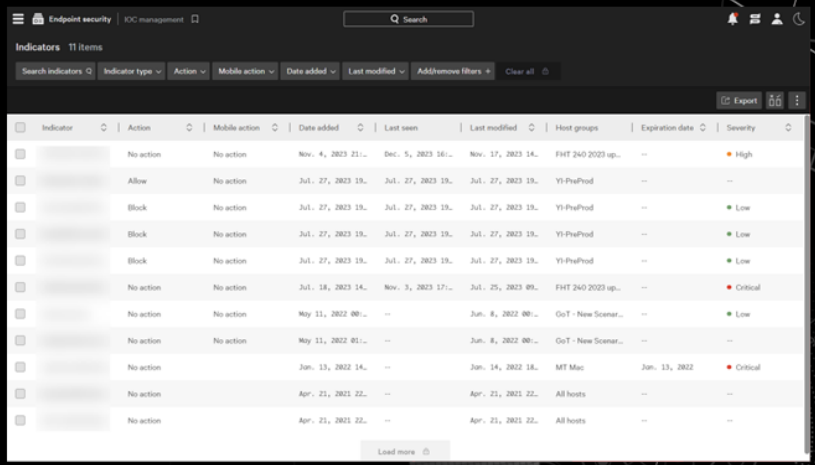
- **M**onitor for unique circumstances and environments

With **Falcon Prevent** customers can also:

- Block and kill processes
- Add (or exclude) specific process executions or events
- Create rules for events that are NOT malicious

CUSTOM IOCs

- Hashes, domains, and IP addresses
  - Limit of 90,000 hashes
- Can be applied to ALL HOSTS or selected GROUPS
- Set your own severity
- Create individually or upload csv or json file



THREAT HUNT AUTOMATION

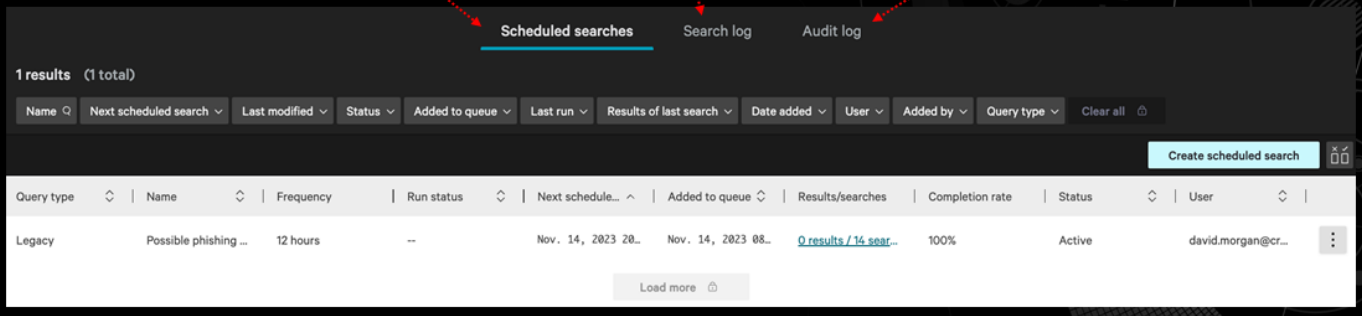
CROWDSTRIKE

SCHEDULED SEARCH TABS

View your scheduled searches

Log of all previous searches with number of hits

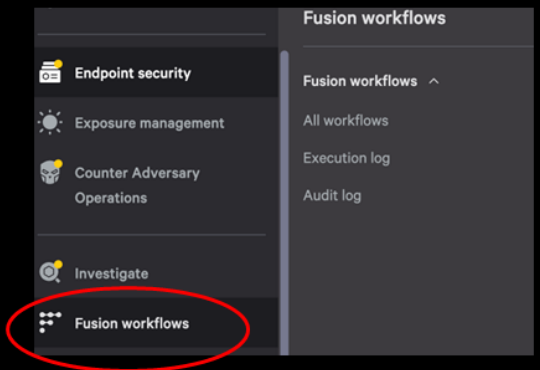
Audit trail – only accessible by admins



CROWDSTRIKE

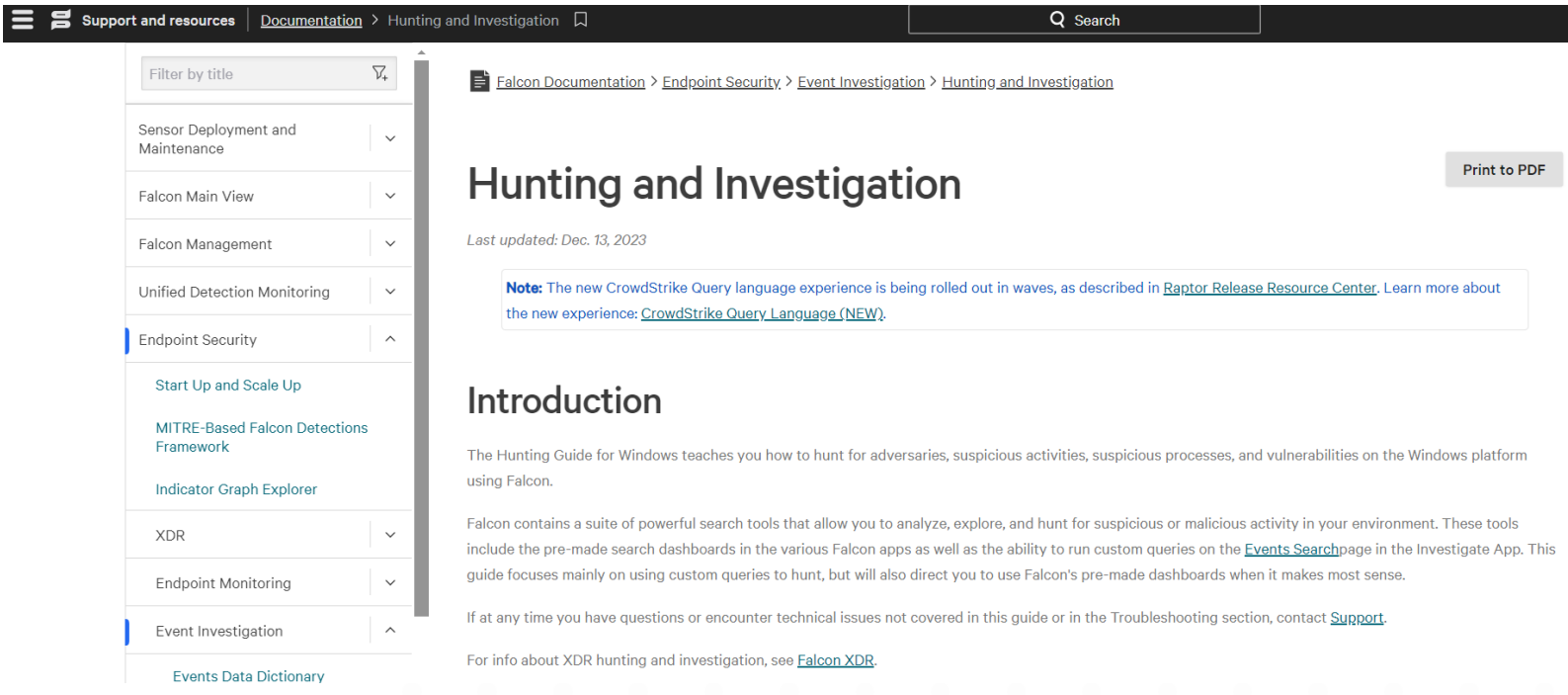
FALCON FUSION

- Granular definitions for automated actions for incidents, detections, etc
- Actions dependent on role-based access and subscriptions
- Some actions may require a connector form the Crowdstrike Store



HUNTING RESOURCES

The hunting guide offers best practices for introductory threat hunting in Falcon, hunting queries, and focuses on IOCs. It also includes various search pages in Investigate



RESOURCES

Access documentation in the Falcon platform by going to Support > Docs

CROWDSTRIKE UNIVERSITY