

Twitter: @aboutsecurity

Presentation based on SEC530: Defensible Security
Architecture and Engineering

SANS

Prioritizing your Threat Hunting & Blue Teaming Strategy with MITRE ATT&CK Analytics

© 2020 Ismael Valenzuela | All Rights Reserved

About Me

Ismael Valenzuela

- SEC530 Co-author
- 10 yrs teaching for SANS internationally DFIR, CyberDefense & BlueTeam curriculum
- GSE # 132, plus 11 other GIAC certifications
- Sr. Principal Engineer at McAfee
- +20 yrs ‘Defending All The Things!’
- **Twitter:** @aboutsecurity





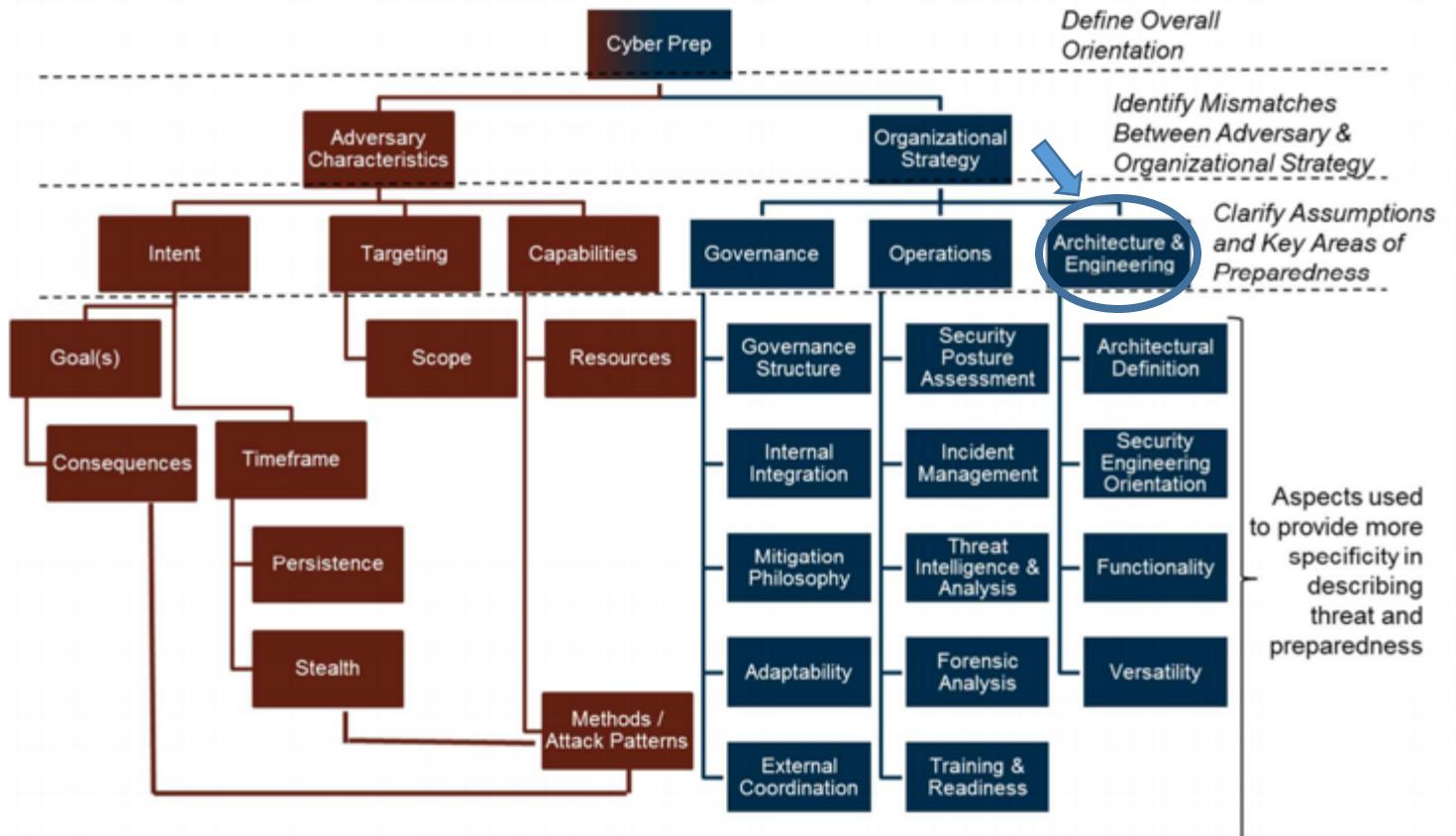
MITRE WHAT?

Think Red, Act Blue



Practical Threat Modeling: Purple Teaming

- We need to determine the characteristics of the adversaries which could be expected to target our systems so we can define and implement effective architectures and controls
- Purple teaming (**red** + **blue**) facilitate this by **working together** through simulation of specific threat scenarios



MITRE Cyber Prep 2.0, May 2017



Where do we start?

Use case: HACME CATS

Biz: Online retailer – Organic food for cats

Threat: FIN-Dogs (super-scary-APT)

Tools:

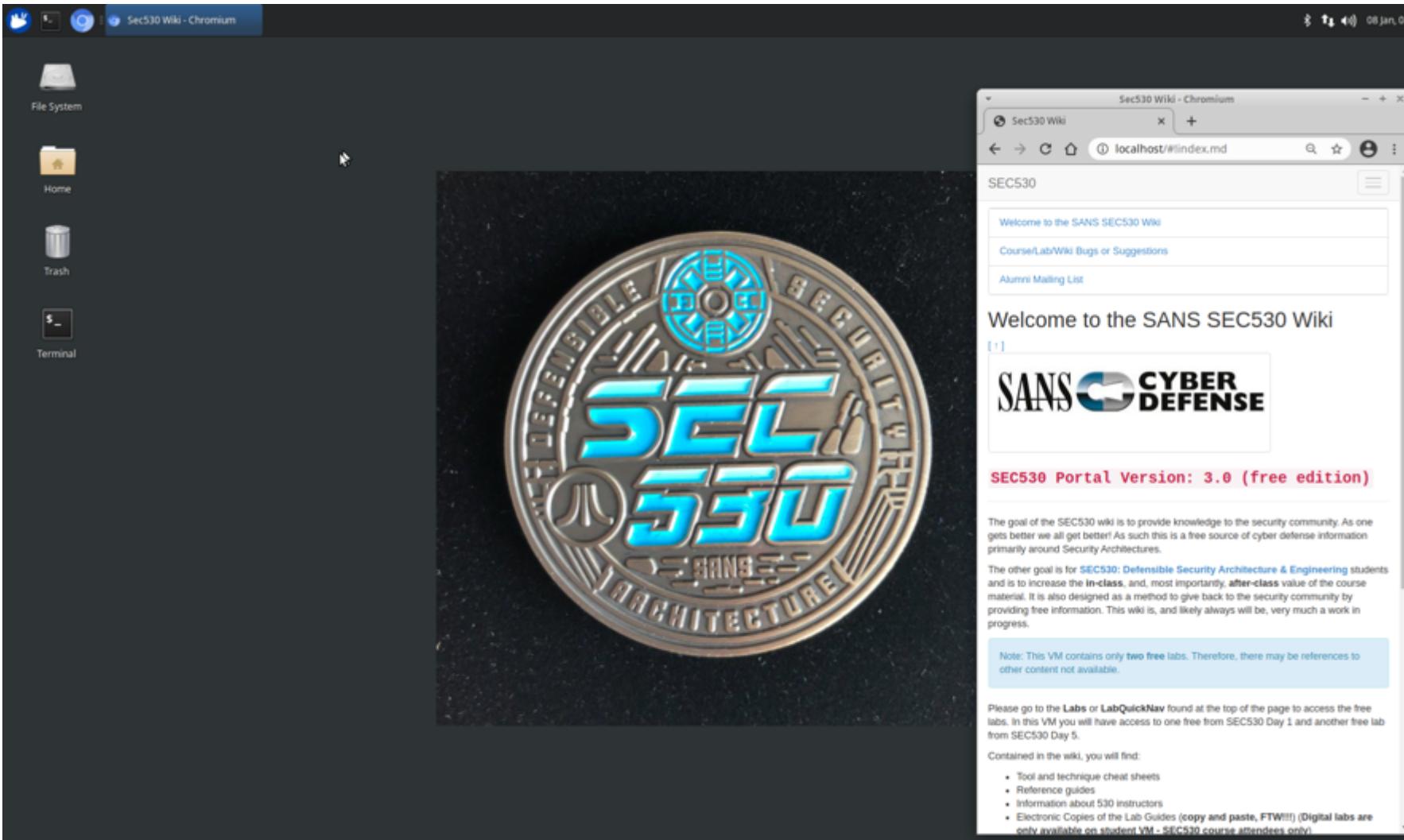
MITRE ATT&CK

- <https://attack.mitre.org/>

ATT&CK Navigator

- <https://mitre-attack.github.io/attack-navigator/>

Use the FREE Security 530 VM and included Wiki with sample Labs



ATT&CK

Matrices Tactics Techniques Mitigations Groups Software Resources Blog Contribute

retail

FIN6, ITG08, Group G0037
... as stolen payment card data and sold it for profit on underground marketplaces. This group has aggressively targeted and compromised point of sale (PoS) systems in the hospitality and retail sectors.^{[1][2]} ID: G0037 Associated Groups: ITG08 Contributors: Drew Church, Splunk Version: 2.0 Created: 31 May 2017 Last Modified: 15 October 2019 Associated Group Descriptions Name Descr...

FIN7, Group G0046
FIN7 FIN7 is a financially-motivated threat group that has primarily targeted the U.S. retail, restaurant, and hospitality sectors since mid-2015. They often use point-of-sale malware. A portion of FIN7 was run out of a front company called Combi Security. FIN7 is sometimes referred...

FIN8, Group G0061
FIN8 FIN8 is a financially motivated threat group known to launch tailored spearphishing campaigns targeting the retail, restaurant, and hospitality industries. [1] [2] ID: G0061 Version: 1.0 Created: 18 April 2018 Last Modified: 01 October 2019 Techniques Used Domain ID Name Use Enterprise T1059 Command-Lin...

Get Started » Contribute » Check out our Blog

Embed View on Twitter

<https://attack.mitre.org/>

FIN6 x FIN7 x FIN8 x layer by operation x +



Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Valid Accounts (0/4)	Command and Scripting Interpreter (4/8)	Valid Accounts (0/4)	Exploitation for Privilege Escalation	Obfuscated Files or Information (0/9)	Credentials from Password Stores (1/3)	Remote System Discovery	Exploitation of Remote Services	Archive Collected Data (2/3)	Ingress Tool Transfer	Automated Exfiltration (0/1)
Scanning IP Blocks	Botnet	Cloud Accounts	PowerShell	Cloud Accounts	Valid Accounts (0/4)	Binary Padding	Network Service Scanning	Internal Spearphishing	Archive via Custom Method	Non-Application Layer Protocol	Traffic Duplication	Data Transfer Size Lim
Vulnerability Scanning	DNS Server	Default Accounts	Windows Command Shell	Default Accounts	Compile After Delivery	Indicator Removal from Tools	Keychain	Account Discovery (1/4)	Lateral Tool Transfer	Non-Standard Port	Protocol Tunneling	Exfiltration Over Alternative Protoc
Gather Victim Host Information (0/4)	Domains	Domain Accounts	JavaScript/JScript	Domain Accounts	Software Packing	Steganography	Securityd Memory	Domain Account	Remote Service Session Hijacking (0/2)	Web Service (1/3)	Bidirectional Communication	Exfiltration Over Unencrypted/Obfu Non-C2 Protocol
Client Configurations	Server	Local Accounts	Visual Basic	Local Accounts	Access Token Manipulation (0/4)	Valid Accounts (0/4)	Brute Force (1/4)	Email Account	Automated Collection	Dead Drop Resolver	One-Way Communication	Exfiltration Over Asymmetric Encry Non-C2 Protocol
Firmware	Virtual Private Server	Drive-by Compromise	AppleScript	Account Manipulation (0/4)	Add Office 365 Global Administrator Role	Create Process with Token	Cloud Accounts	Local Account	RDP Hijacking	One-Way Communication	Application Layer Protocol (1/4)	Exfiltration Over C2 Channel
Hardware	Web Services	Exploit Public-Facing Application	Network Device CLI	Additional Cloud Credentials	Make and Impersonate Token	Default Accounts	Cloud Account	Application Window Discovery	SSH Hijacking	Confluence	DNS	Exfiltration Over O Network Medium
Software	Compromise Accounts (0/2)	Email Accounts	Python	Exchange Email Delegate Permissions	Domain Accounts	Domain Accounts	Cloud Infrastructure Discovery	Cloud Infrastructure Discovery	Remote Desktop Protocol	Sharepoint	File Transfer Protocols	Exfiltration Over Bluetooth
Gather Victim Identity Information (0/3)	External Remote Services	Social Media Accounts	Unix Shell	Parent PID Spoofing	Local Accounts	Local Accounts	Cloud Service Dashboard	Cloud Service Dashboard	SMB/Windows Admin Shares	Data from Local System	Clipboard Data	Exfiltration Over P Medium (0/1)
Credentials	Hardware Additions	Hardwre Additions	Windows Management Instrumentation	SID-History Injection	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Cloud Share Discovery	Cloud Share Discovery	Distributed Component Object Model	Screen Capture	Audio Capture	Exfiltration over U!
Email Addresses	Phishing (3/3)	Phishing Attachment	Exploitation for Client Execution	SSH Authorized Keys	Create Process with Token	Create Process with Token	Domain Trust Discovery	Domain Trust Discovery	SSH	Video Capture	Mail Protocols	Exfiltration Over W Service (0/2)
Employee Names	Compromise Infrastructure (0/6)	Botnet	Inter-Process Communication (1/2)	BITS Jobs	Abuse Elevation Control Mechanism (0/4)	Make and Impersonate Token	File and Directory Discovery	File and Directory Discovery	VNC	Clipboard Data	Web Protocols	Exfiltration to Clou Storage
Gather Victim Network Information (0/6)	DNS Server	Spearphishing Link	Dynamic Data Exchange	Component Object Model	Bypass User Account Control	Parent PID Spoofing	Network Share Discovery	Network Share Discovery	Data from Cloud Storage Object	Data from Configuration Repository (0/2)	Communication Through Removable Media	Exfiltration to Code Repository
DNS	Domains	Spearphishing via Service	BITS Jobs	Native API	Elevated Execution with Prompt	SID-History Injection	Network Sniffing	Network Sniffing	Windows Remote Management	Data from Configuration Repository (0/2)	Data Encoding (0/2)	Scheduled Transfer
Domain Properties	Server	Replication Through Removable Media	Component Object Model	Registry Run Keys / Startup Folder	Token Impersonation/Theft	Token Impersonation/Theft	>Password Policy Discovery	Peripheral Device Discovery	Replication Through Removable Media	Non-Standard Encoding	Standard Encoding	Transfer Data to Clou Account
IP Addresses	Virtual Private Server	Malware	Scheduled Task Job (1/6)	Authentication Package	Setuid and Setgid	Modify Registry	Credential API Hooking	Keylogging	Network Device Configuration Dump	SNMP (MIB Dump)	Data Obfuscation (0/3)	
Network Security Appliances	Web Services	Code Signing Certificates	Compromise Hardware Supply Chain	Kernel Modules and Extensions	Sudo and Sudo Caching	Abuse Elevation Control Mechanism (0/4)	GUI Input Capture	Web Portal Capture	Software Deployment Tools			
Network Topology	Develop Capabilities (1/4)	Malware	Supply Chain Compromise (0/3)	At (Linux)	Boot or Logon Autostart Execution (1/12)	Bypass User Account Control	Man-in-the-Middle (0/2)	Domain Groups	Cloud Groups	Taint Shared Content		
Network Trust Dependencies	Network Trust Dependencies	Code Signing Certificates	Compromise Software Dependencies and Frameworks	At (Windows)	LSASS Driver	Elevated Execution with Prompt	Cloud Groups	Cloud Groups	Data from Network Shared Permis			
Gather Victim Org Information (0/4)	Business Relationships	Digital Certificates	Cron	Plist Modification	Launchd	Registry Run Keys / Startup Folder	Man-in-the-Middle (0/2)	Domain Groups	Taint Shared Content			
Determine Physical Locations	Fault Tolerance	Endpoint Monitoring	Network Monitoring	Port Monitoring	Port Monitoring	Authorization	Cloud Groups	Cloud Groups	Data from Network Shared Permis			

<https://mitre-attack.github.io/attack-navigator/enterprise/#>

Let's play with some analytics

ATT&CK scripts:

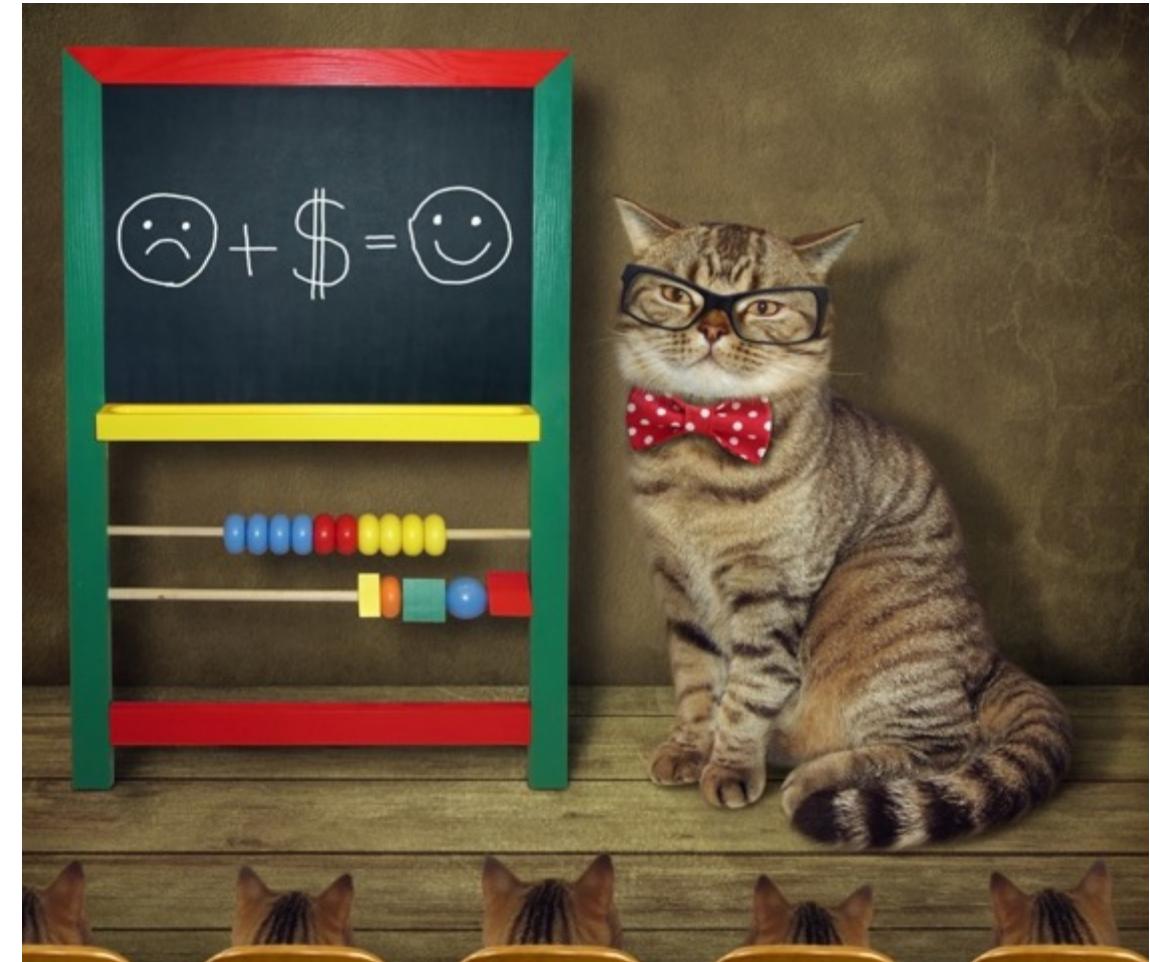
<https://github.com/mitre-attack/attack-scripts>

Jupyter notebook:

<https://mybinder.org/v2/gh/mitre-attack/attack-scripts/master>

ATT&CK Python client:

<https://github.com/hunters-forge/ATTACK-Python-Client>



Jupyter Notebooks - <https://mybinder.org/v2/gh/mitre-attack/attack-scripts/master>

Data Source Investigation

Let's use the [ATT&CK Python Client](#) to manually examine the techniques, list the data sources, and build a heatmap out of our selected sources.

If you're looking for less development or a more in-depth and finely-grained dive, check out:

- [DeTTACK](#)
- [AttackDatamap](#)

Consider: What have you used to track data sources? What has worked well, and what has not worked so well?

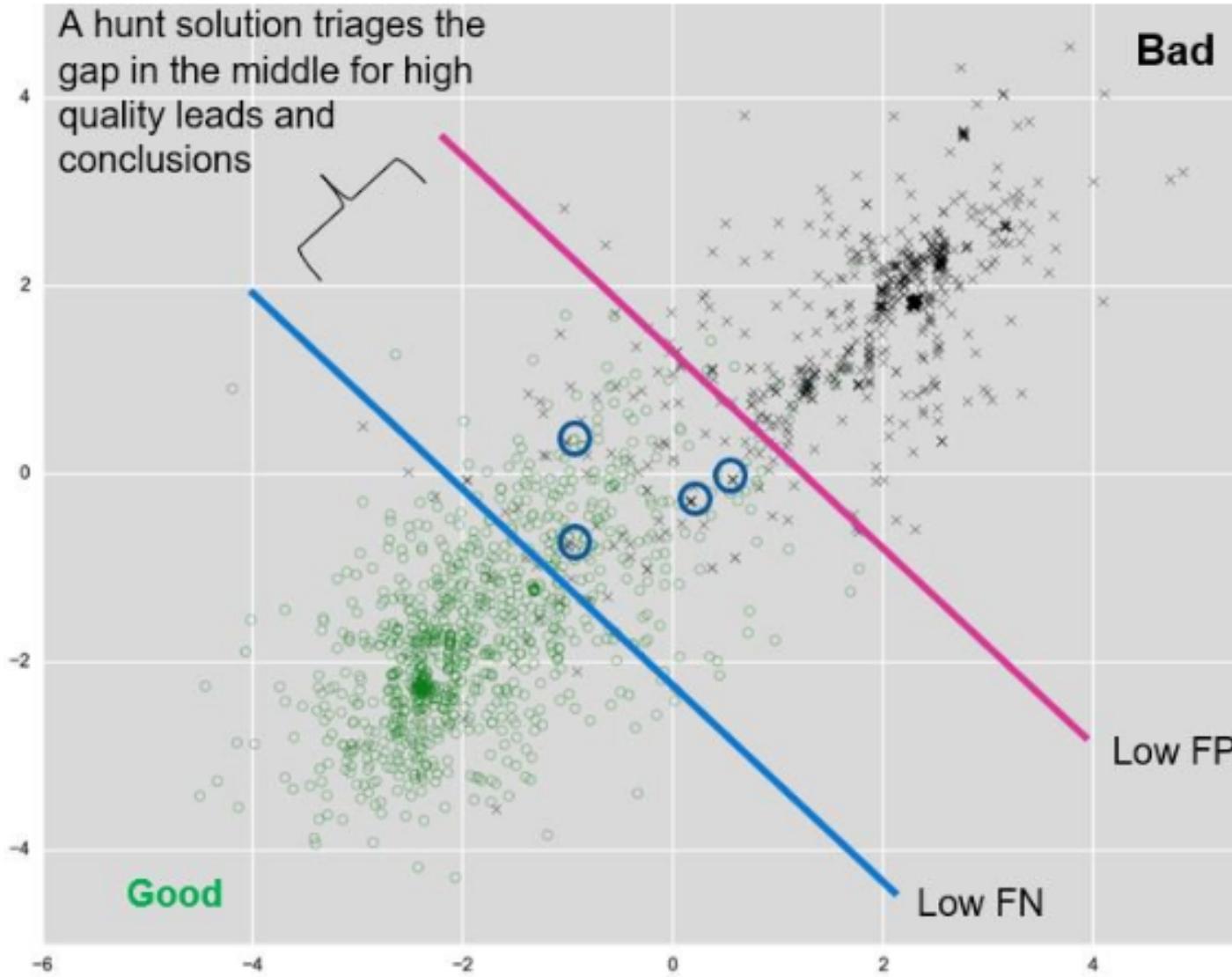
```
In [ ]: # Import the packages we'll need

# Some basic python and jupyter stuff
from collections import defaultdict
import json
from IPython.display import FileLink, FileLinks

# Visualization and data libraries
import altair as alt
import pandas as pd

# ATT&CK Python Client, by @HuntersForge (https://github.com/hunters-forge/ATTACK-Python-Client)
from attackcti import attack_client

# Because this is in Jupyter notebooks we need to enable that renderer for the altair charts to work
alt.renderers.enable('notebook')
```



Visibility vs Detection

Most products focused on detection are not good enough for hunting. Why? It's a matter of focus:

- Detection (and prevention)-- Few FPs
- Visibility and Hunting – Few FNs

<https://deltarisk.com/blog/why-most-real-time-defensive-solutions-are-poor-threat-hunting-solutions/>

Time Based Security: Protection only buys you “time”



If the attacker steals the safe and brings it home, he eventually wins. It's a matter of time.

$$P < D + R$$



Time-based Security



Schwartau, "If it takes longer to detect and to respond to an intrusion than the amount of protection time afforded by the security measures, that is if $P < D + R$, then effective security is impossible to achieve in this system."



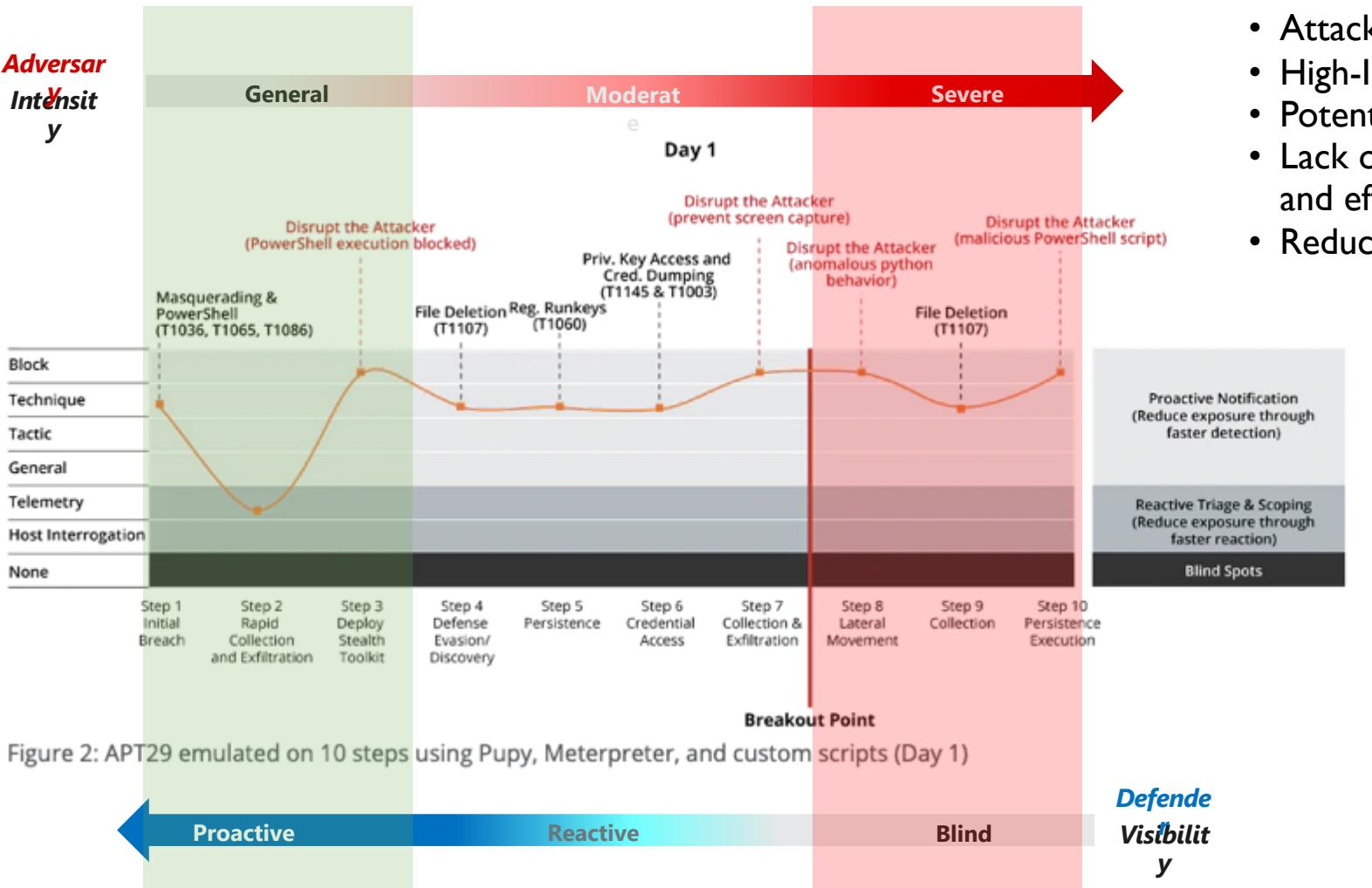
$$P > D + R$$



While prevention works, detecting and responding early help to mitigate impact.

It's All About Time: Racing With the Adversary

- Attacker is breaking through the front door
- Contained compromise
- Scoped, investigated, mitigated
- Cheap \$\$\$
- Effective security
- Reusable Intel



- Attacker left the building
- High-Impact Incident
- Potential Breach \$\$\$\$
- Lack of visibility, detection, and effective response
- Reduced value Intel

DeTT&CT

Framework to manage, assess
and compare the quality of:

- Data sources
- Visibility
- Detection
- Threat actors

<https://github.com/rabobank-cdc/DeTTECT>

Data Sources

<https://github.com/rabobank-cdc/DeTECT/wiki/Data-sources>

Almost 60 different sources mapped to different platforms

Home > Techniques > Enterprise > Standard Application Layer Protocol

Standard Application Layer Protocol

Adversaries may communicate using a common, standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic.

Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are RPC, SSH, or RDP.

<https://attack.mitre.org/techniques/T1071/>

ID: T1071

Tactic: Command And Control

Platform: Linux, macOS, Windows

Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Malware reverse engineering, Process monitoring

Requires Network: Yes

Version: 1.0





HOME

DATA SOURCES

TECHNIQUES

GROUPS

Data Sources

New file

Select YAML file

File details

Filename: data-sources-new.yaml
File type: data-source-administration
Version: 1.0
Name: example
Platform: all Windows Linux macOS AWS GCP Azure Azure AD Office 365 SaaS

Save YAML file

+ Add data source

filter

Name	Date	Products	
registered			
DNS records	2020-04-11	Zeek sensor, DNS Logs from Windows Server	
Netflow/Enclave netflow	2020-04-11	Zeek sensor	
Network intrusion detection system	2020-04-11	Zeek sensor	





DeTT&CT
Editor

HOME

DATA SOURCES

TECHNIQUES

GROUPS

Adjust visibility and detection

T1046	Network Service Scanning	
T1047	Windows Management Instrumentation	
T1048	Exfiltration Over Alternative Protocol	
T1065	Uncommonly Used Port	
T1071	Standard Application Layer Protocol	
T1076	Remote Desktop Protocol	
T1090	Connection Proxy	
T1094	Custom Command and Control Protocol	
T1095	Standard Non-Application Layer Protocol	
T1100	Web Shell	
T1102	Web Service	
	Multi-Stage Channels	
	Remote File Copy	
	LLMNR/NBT-NS Poisoning and Relay	
	Multi-hop Proxy	
T1189	Drive-by Compromise	
T1192	Spearphishing Link	
T1193	Spearphishing Attachment	
T1219	Remote Access Tools	
T1221	Template Injection	

Score date: 2020-04-12



Score logbook

Custom key value pairs

Add detection

Visibility

all

Visibility is applicable to

all

applicable to

Comment

...

Score date: 2020-04-10



Score logbook

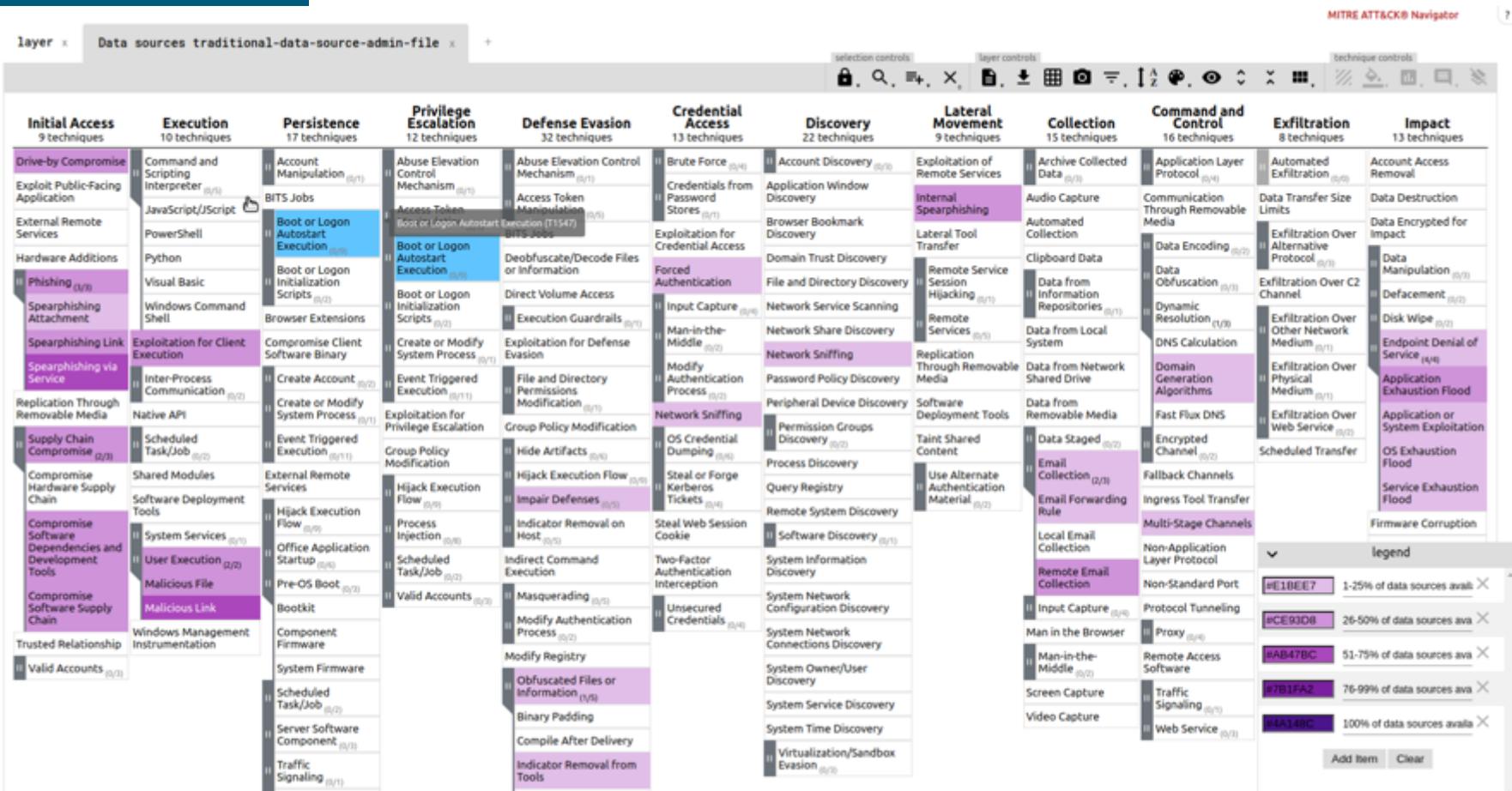
Custom key value pairs

Visibility

<https://github.com/rabobank-cdc/DeTTECT/wiki/Visibility-coverage>

Generates a JSON file with the coverage of visibility based on the techniques administration template: **python dettect.py v -ft sample-data/techniques-administration-endpoints.yaml -fd input/data-sources-sec530.yaml -l**

Legend indicates the type of visibility based on the input given

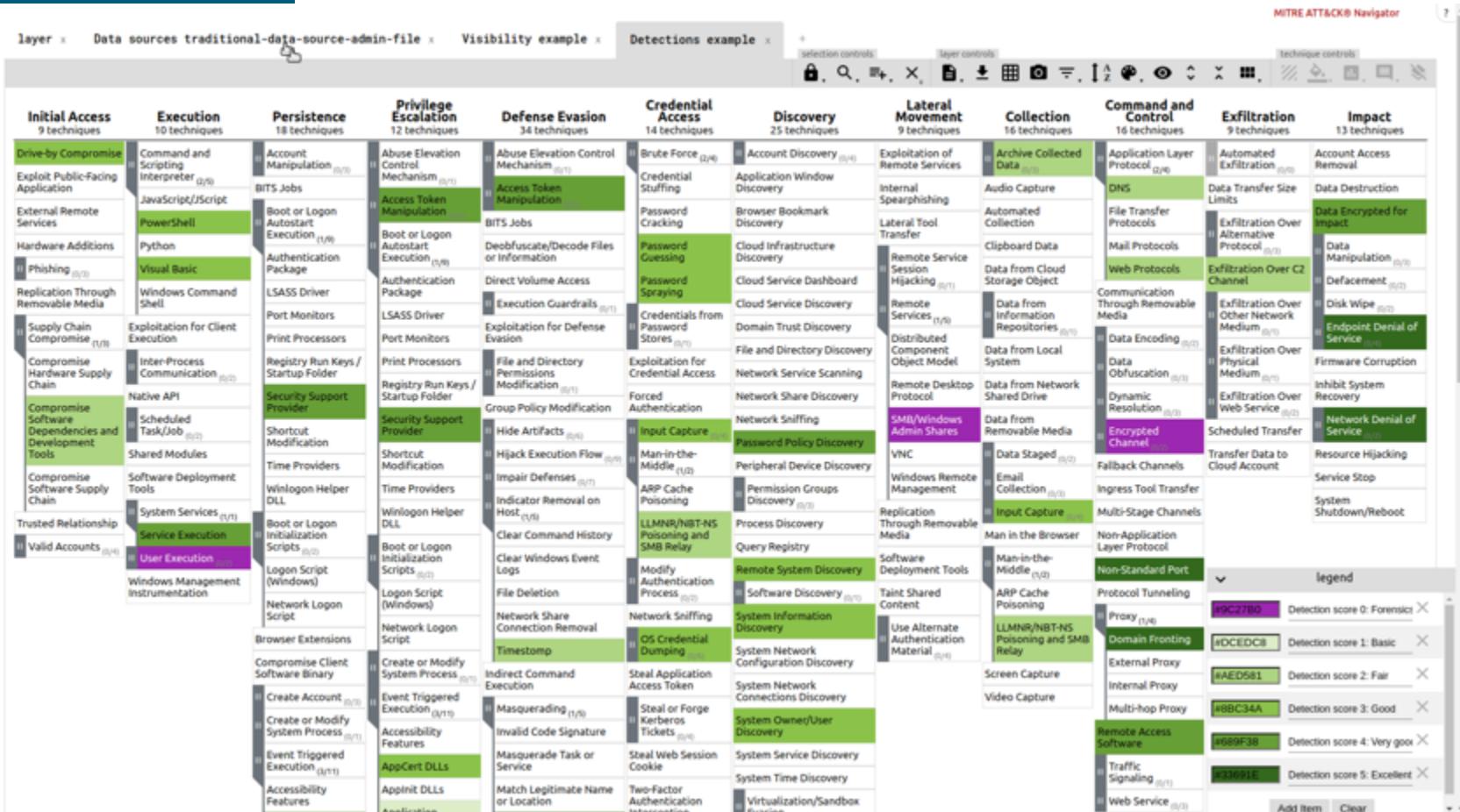


Detection

<https://github.com/rabobank-cdc/DeTECT/wiki/Detection-coverage>

Generates a JSON file with the coverage of detection based on the techniques administration template: : `python detect.py d -ft sample-data/techniques-administration-endpoints.yaml -l`

Legend indicates the quality of detection based on the input given

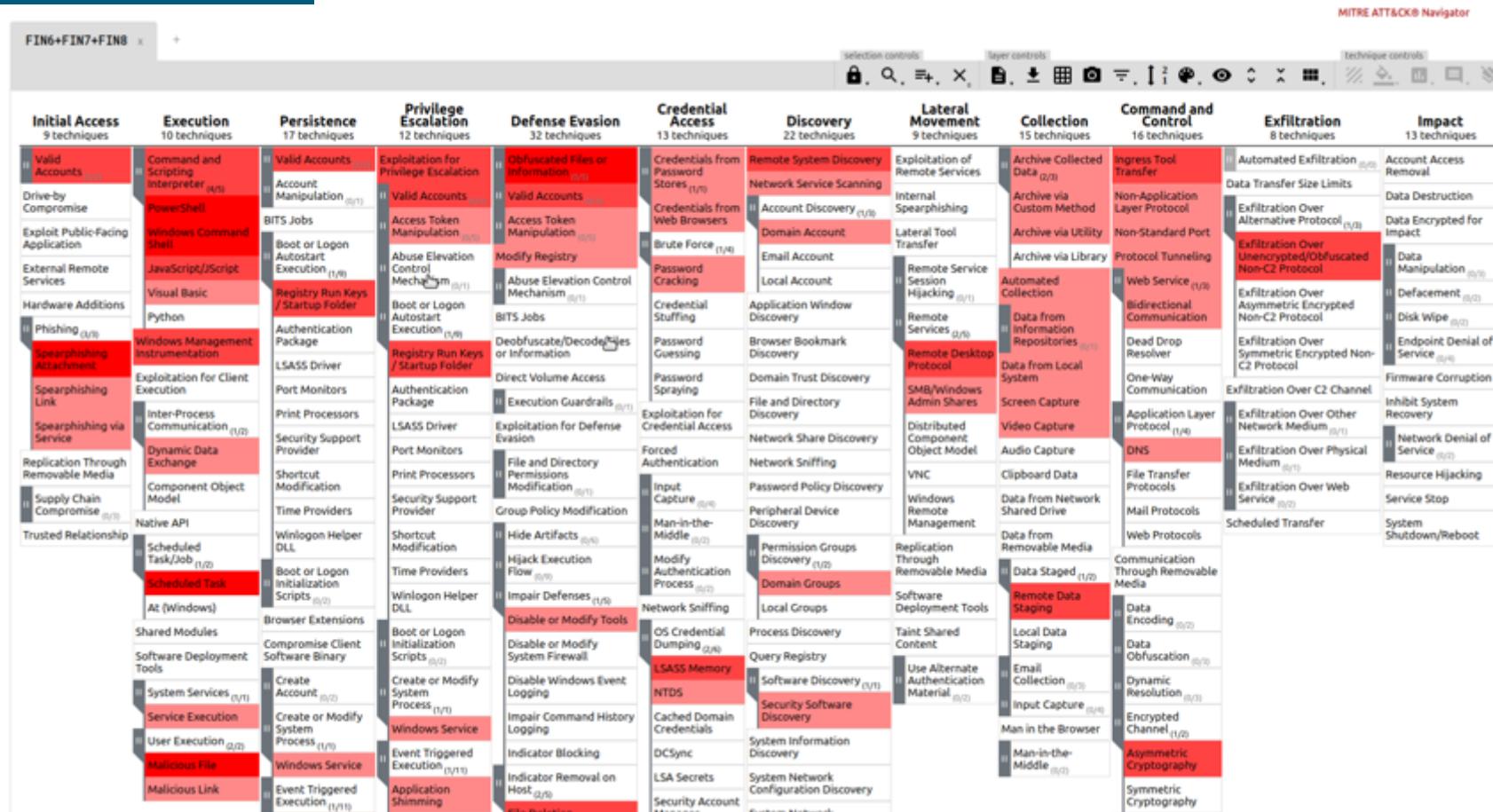


Threat Actors

<https://github.com/rabobank-cdc/DeTTECT/wiki/Threat-actor-group-mapping>

Generates a JSON file with a heatmap of the groups we're interested in (FIN6, FIN7, FIN8): **python dettect.py g -g 'fin7,fin8,fin6'**

Results are sorted by most common techniques (darker red)



The diagram illustrates a comprehensive threat landscape across several categories:

- Initial Access:** 9 techniques (Drive-by Compromise, Exploit Public-Facing Application, External Remote Services, Hardware Additions, Phishing (3/3), Spearphishing Attachment, Spearphishing Link, Spearphishing via Service, Replication Through Removable Media).
- Execution:** 10 techniques (Command and Scripting Interpreter (0/5), BITS Jobs, PowerShell, Python, Visual Basic, Windows Command Shell, Exploitation for Client Execution, Inter-Process Communication (0/2), Native API, Scheduled Task/Job (0/2)).
- Persistence:** 17 techniques (Account Manipulation (0/1), Abuse Elevation Control Mechanism (0/1), Access Token Manipulation (0/5), BITS Jobs, Boot or Logon Autostart Execution (0/9), Boot or Logon Initialization Scripts (0/2), Browser Extensions, Compromise Client Software Binary, Create or Modify System Process (0/1), Create Account (0/2), Create or Modify System Process (0/1), Event Triggered Execution (0/11), Exploitation for Privilege Escalation, Group Policy Modification, Hijack Execution Flow (0/9), External Remote Services, Office Application Startup (0/6), Process Injection (0/8), Scheduled Task/Job (0/2), Valid Accounts (0/3), User Execution (2/2), Malicious File, Malicious Link, Windows Management Instrumentation, Valid Accounts (0/3)).
- Privilege Escalation:** 12 techniques (Abuse Elevation Control Mechanism (0/1), Access Token Manipulation (0/5), BITS Jobs, Boot or Logon Autostart Execution (0/9), Boot or Logon Initialization Scripts (0/2), Deobfuscate/Decode Files or Information, Direct Volume Access, Exploitation for Defense Evasion, Exploitation for Privilege Escalation, Group Policy Modification, Hide Artifacts (0/6), Hijack Execution Flow (0/9), Impair Defenses (0/5), Indicator Removal on Host (0/5), Indirect Command Execution, Invalid Accounts (0/3), Masquerade (0/4), Modify Registry (0/4), Modify Resource (0/4), Obfuscate Information (1/5), Binary Padding, Compile After Delivery, Indicator Removal from Tools).
- Defense Evasion:** 32 techniques (Brute Force (0/4), Credentials from Password Stores (0/1), Exploitation for Credential Access, Forged Authentication, Input Capture (0/4), Man-in-the-Middle (0/2), Modify Authentication Process (0/2), Network Sniffing, OS Credential Dumping (0/6), Steal or Forge Kerberos Tickets (0/4), Two-Factor Authentication, System Information Discovery, Virtualization/Sandbox Evasion (0/3)).
- Credential Access:** 13 techniques (Account Discovery (0/3), Application Window Discovery, Browser Bookmark Discovery, Domain Trust Discovery, File and Directory Discovery, Network Service Scanning, Network Share Discovery, Network Sniffing, Password Policy Discovery, Peripheral Device Discovery, Permission Groups Discovery (0/2), Process Discovery, Query Registry, Remote System Discovery, Software Discovery).
- Discovery:** 22 techniques (FIN5, FIN6, FIN7, FIN8, Frankenstein, 3PARA RAT, 4H RAT, ABK, adbupd, ADVSTORESHELL, Account Use Policies, Active Directory Configuration, Antivirus/Antimalware, Application Developer Guidance, Application Isolation and Sandboxing, Collection, Non-Standard Port, Protocol Tunneling, Proxy, Remote Access Software, Screen Capture, Traffic Signaling (0/1), Web Service (0/3)).
- Threat Groups:** FIN5, FIN6, FIN7, FIN8, Frankenstein, 3PARA RAT, 4H RAT, ABK, adbupd, ADVSTORESHELL, Account Use Policies, Active Directory Configuration, Antivirus/Antimalware, Application Developer Guidance, Application Isolation and Sandboxing, Collection, Non-Standard Port, Protocol Tunneling, Proxy, Remote Access Software, Screen Capture, Traffic Signaling (0/1), Web Service (0/3).
- Command and Control:** 16 techniques (Application Layer Protocol, Communication through Removable Media, Data Encoding (0/2), Dynamic Resolution (1/3), Job Obfuscation (0/3), Job Generation Algorithms, Last Flux DNS, Encrypted Channel (0/2), Back Channels, Process Tool Transfer, Multi-Stage Channels, Application Layer Protocol, Remote Email Collection, Input Capture (0/4), Man in the Browser, Man-in-the-Middle (0/2), Screen Capture, Traffic Signaling (0/1), Web Service (0/3)).
- Exfiltration:** 8 techniques (Automated Exfiltration (0/0), Data Transfer Size Limits, Data Encrypted for Impact, Data Manipulation (0/3), Defacement (0/2), Disk Wipe (0/2), Endpoint Denial of Service (4/4), Application Exhaustion Flood, Scheduled Transfer).
- Impact:** 13 techniques (Account Access Removal, Data Destruction, Data Encrypted for Impact, Data Manipulation (0/3), Defacement (0/2), Disk Wipe (0/2), Endpoint Denial of Service (4/4), Application Exhaustion Flood, OS Exhaustion Flood, Service Exhaustion Flood, Firmware Corruption).

A central callout box highlights "Gap Analysis (Purple Teaming)".

Additional Resources

Thinking Red, Acting Blue -

<https://www.sans.org/webcasts/defensible-security-architecture-engineering-2-thinking-red-acting-blue-mindset-actions-109710>

The Githubification of InfoSec by John Lambert

- <https://medium.com/@johnlatwc/the-githubification-of-infosec-afbdbfaad1d1>

DETT&CT - <https://github.com/rabobank-cdc/DeTTECT>

MITRE's Red Teaming dataset -

<https://github.com/mitre/brawl-public-game-001>

Playbook for this talk (step by step commands):
<https://github.com/aboutsecurity/Talks-and-Presentations/blob/master/coron4con.md>

MITRE Assistant by dfirence (Carlos Diaz)

<https://github.com/dfirence/mitre-assistant>

Prioritizing your Threat Hunting & Blue Teaming strategy with
MITRE ATT&CK analytics

Tools

- MITRE ATT&CK Navigator <https://mitre-attack.github.io/attack-navigator/enterprise/#>
- MITRE Jupyter Notebook <https://mybinder.org/v2/gh/mitre-attack/attack-scripts/master>
- DeTTECT <https://github.com/rabobank-cdc/DeTTECT/>

Installing DeTT&CT:

Download the docker image:

```
docker pull rabobankcdc/detect:latest
```

Start DeTT&CT:

Linux & MacOS:

```
docker run -p 8080:8080 -v $(pwd)/output:/opt/DeTTECT/output -v $(pwd)/input:/opt/DeTTECT/input --name detect
```

Windows (cmd.exe):

```
docker run -p 8080:8080 -v %cd%/output:/opt/DeTTECT/output -v %cd%/input:/opt/DeTTECT/input --name detect -it
```

PowerShell:

```
docker run -p 8080:8080 -v ${PWD}/output:/opt/DeTTECT/output -v ${PWD}/input:/opt/DeTTECT/input --name detect
```

Purple Teaming & SOC Engineering

*<https://medium.com/anton-on-security/can-we-have-detection-as-code-96f869cfdc79>

*Anton Chuvakin on Detection Engineering (Set 2020)**

- *100% Detection content versioning*
- *Proper “QA” for detection content*
- *Content (code) reuse and modularity of detection content*
- *Metrics and improvement are also key*
- *Full CI/CD pipeline for detections to continuously build, refine, deploy and run detection logic*



<https://www.youtube.com/watch?v=H3bsV0lGZfg>

Cross-org Training, Purple Teaming & Risk Mitigation

- SOC rotations
- Customer calls
- SANS courses
- Research
- Defend The Flag!



Presentation based on SEC530: Defensible Security Architecture and Engineering

Thank you!! Follow @SecurityMapper & @aboutsecurity for updates and new webinars!

The screenshot shows a blog post on the SANS website. The header includes the SANS logo and navigation links for Find Training, Online Training, In-Person Training, Programs, and Resources. The breadcrumb navigation shows Home > Blog > Becoming an All-Around Defender: Building an Enterprise-Grade Home Lab. The author is Michelle Petersen. The main title is "Becoming an All-Around Defender: Building an Enterprise-Grade Home Lab". A subtitle below it says "Emphasis on "building" – not "deploying."". The date is May 19, 2020.

The graphic has a dark blue background with concentric circular patterns. The text "All-Around Defenders: New Year, New Start" is displayed in large white font, followed by "A Community Gathering" in a smaller white font. Below this, the date "Jan 8, 2021 | 10:00 AM – 3:00 PM (EST)" and the location "via Zoom" are shown. To the right is the SANS Blue Team Ops logo, which features a shield icon and the text "SANS BLUE TEAM OPS".



References

<https://www.sans.org/course/defensible-security-architecture-and-engineering>

