

SANS

# Managing & Showing Value during Red Team Engagements & Purple Team Exercises

## T1033 - System Owner/User Discovery – Jorge Orchilles

- Chief Technology Officer - SCYTHE
- C2 Matrix Co-Creator
- Certified SANS Instructor: SEC560, SEC504
- Author SEC564: Red Team Exercises and Adversary Emulation
- 10 years @ Citi leading offensive security team
- CVSSv3.1 Working Group Voting Member
- GFMA: Threat-Led Pen Test Framework
- ISSA Fellow; NSI Technologist Fellow



## T1033 - System Owner/User Discovery – Phil Wainwright

- Director at Security Risk Advisors, focus on technical testing and software delivery
- InfoSec consultant for 15 years, promoted to “cyber” in recent years
- Background in pen testing, appsec/product security, network & cloud security
- More recent focus in purple teaming & adversary emulation past ~7 years
- Manages team working on the VECTR platform
- Black Hat Arsenal 2019 & FS-ISAC speaker



# Red Team Exercises and Adversary Emulation

- Learn the skills needed to perform safe, professional Red Team Exercises and Adversary Emulations
- Introduce and follow repeatable frameworks and methodologies
- Tips and tricks to save time, enhance quality, and avoid risk
- Perform hands-on exercises to reinforce the topics, in a class-long, intelligence led, Adversary Emulation Red Team Exercise

## Agenda

- Definitions – because we said Red Team and must debate
- Framework and Methodology
- Cyber Threat Intelligence
- Planning an Adversary Emulation
- Emulating an Adversary
- Exercise Closure – Showing Value with VECTR
- ~70% Live Demos
  - And screenshots for those that only read slides
  - Yeah, we know who you are

## Red Team

- **Definition:** Red Team performs Tactics, Techniques, and Procedures (TTPs) to test people, processes, and technology in a target environment.

*“The practice of looking at a problem or situation from the perspective of an adversary” – Red Team Journal 1997*

- **Goal:** Make Blue Team better. Train and measure blue teams' detection and response policies, procedures, and technologies are effective.
- **Effort:** Manual; lots of tools (see C2 Matrix)
- **Frequency:** Intelligence-led (new exploit, tool, or TTP)
- **Customer:** Blue Teams

## Blue Team

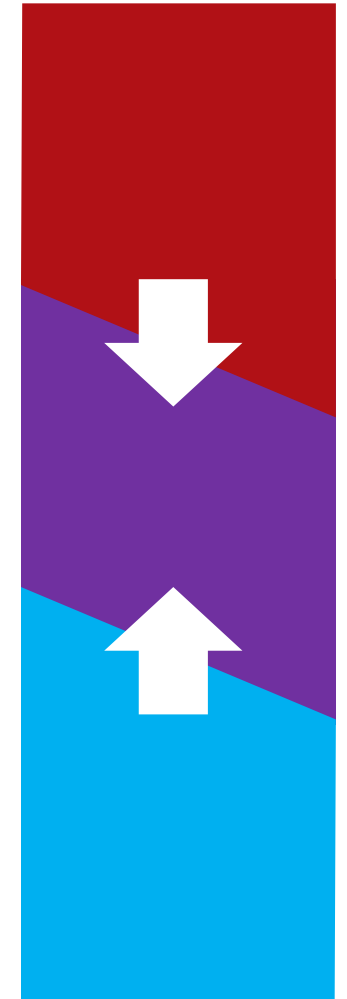
- **Definition:** the defenders in an organization entrusted with identifying and remediating attacks. Generally associated with Security Operations Center or Managed Security Service Provider (MSSP), Hunt Team, Incident Response, and Digital Forensics. Really, it is everyone's responsibility!
- **Goal:** identify, report the attack, contain, and eradicate attacks
- **Effort:** Automated and Manual. People are the best defenders
- **Frequency:** Every Day 24/7
- **Customer:** entire organization

## Adversary Emulation

- **Definition:** A type of Red Team exercise where the Red Team emulates how an adversary operates, following the same tactics, techniques, and procedures (TTPs), with a specific objective like those of realistic threats or adversaries.
- **Goal:** Emulate an end-to-end attack against a target organization. Obtain a holistic view of the organization's preparedness for a real, sophisticated attack.
- **Effort:** Manual; more setup than a limited scope Penetration Test
- **Frequency:** Twice a year or yearly
- **Customer:** Entire organization

## Purple Team

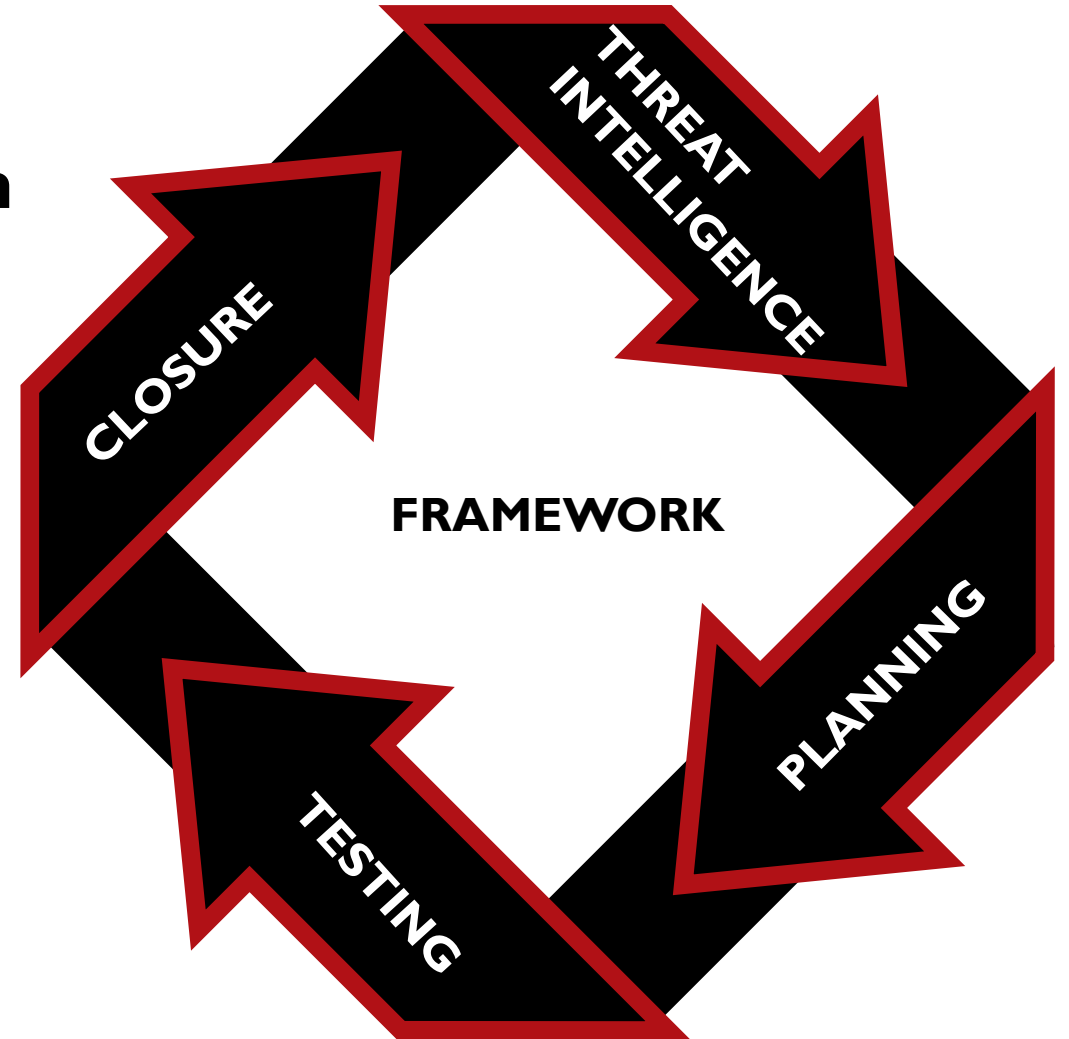
- **Definition:** A function, or virtual team, where red and blue work together to improve the overall security of the organization. Red Team does not focus on stealth as they normally would.
- **Goal:** Red Team emulates adversary TTPs while blue teams watch and improve detection and response policies, procedures, and technologies in real time.
- **Effort:** Manual
- **Frequency:** Intelligence-led (new exploit, tool, or TTP)
- **Customer:** Red Team & Blue Team



## Framework for SEC564

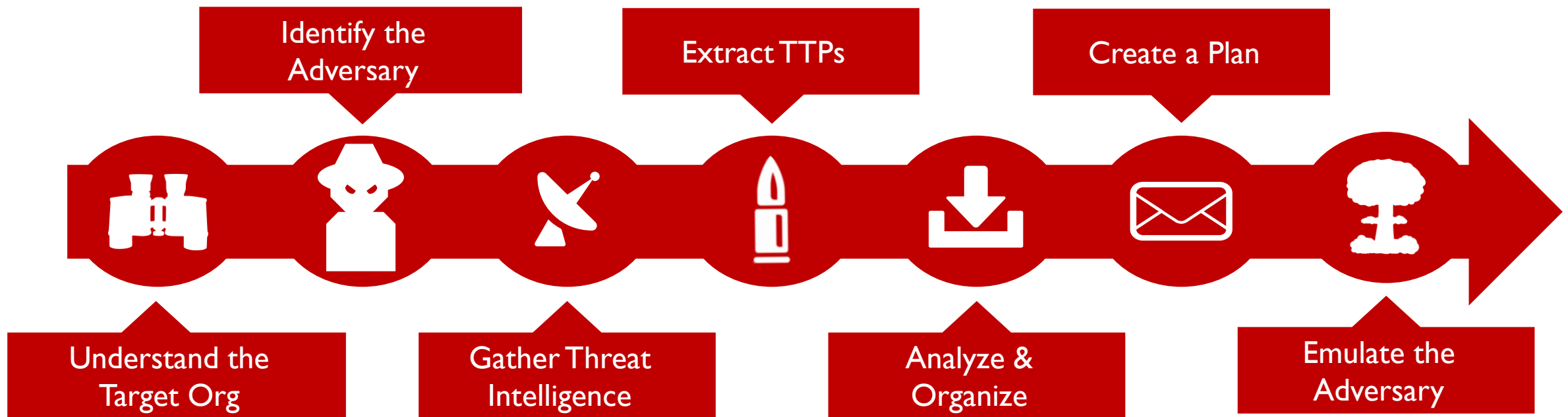
**Like most organizations, this course will take a hybrid approach based on the frameworks and methodologies just introduced**

- Threat Intelligence
- Planning
- Testing
  - Red Team Exercise Execution
- Closure
  - Analysis and Response
  - Report
  - Remediation and Action Plan



# Threat Intelligence for Red Team & Purple Team Exercises

***"Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard." (Gartner)***

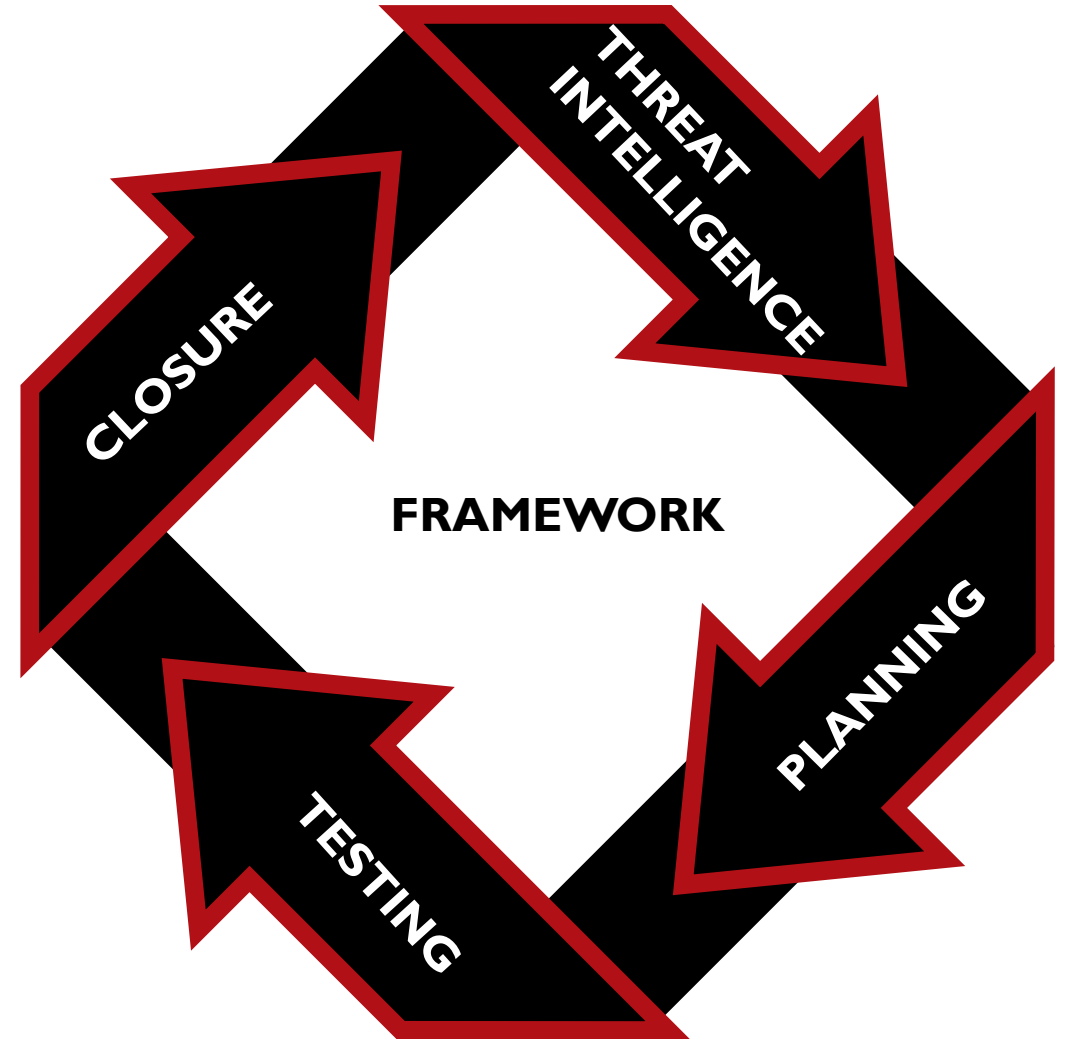


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	Applnit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	Applnit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption

## Planning

### The planning phase covers test preparation activities

- Triggers
- Objectives
- Scope
- Trusted Agents
- Roles and Responsibilities
- Rules of Engagement



### Philosophy and understanding one will be breached

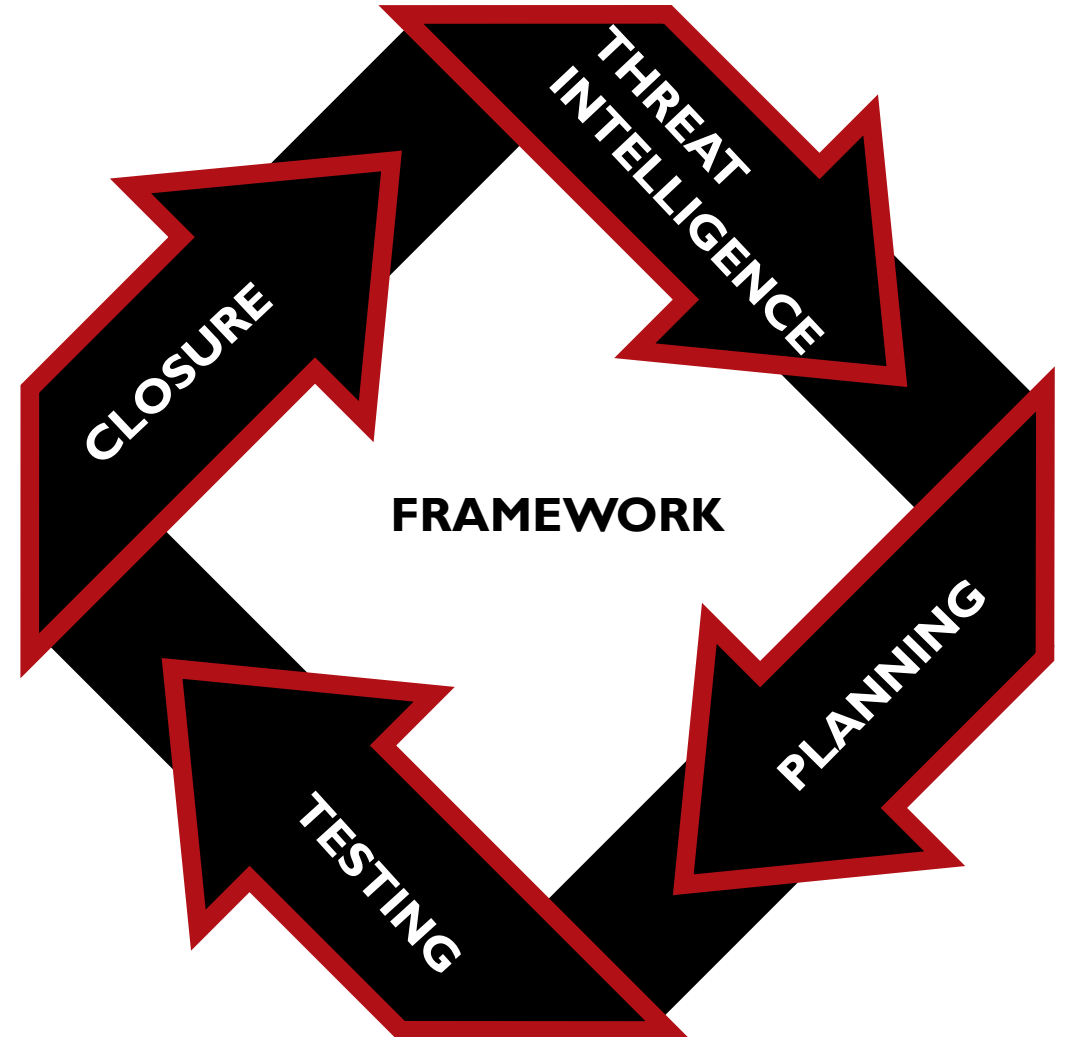
- Based on assumption an endpoint is already compromised
- Answers “what can attacker do with this initial access”
  - Tests for malicious insider threat as well
- Start with a base build of OS and account just like a new hire
- Simulate a user being compromised, then emulate an adversary
- All other ATT&CK™ Tactics are in play
- See Red Siege’s Mike Saunders presentation



Role	Responsibilities
<b>Governance</b>	Approve the attack scenario, the final report and remediation action items. Governance agents should also receive status updates throughout the exercise
<b>Project Management</b>	Coordinate entire Red Team Exercise including threat intelligence gathering; target reconnaissance; Testing Phase communication; and management of timeline and objectives
<b>Threat Intelligence</b>	Identify cyber threat actor(s) with the sophistication and desire to attack the organization; provide the group's technical and behavioral profile including TTPs
<b>Risk Avoidance</b>	Receive daily updates on all Red Team actions and are responsible for avoiding or reducing the material impact of the exercise to business operations
<b>Action Item Remediation Owners</b>	Own actions related to remediation plan. Owners of Technology related findings will be privy to more briefings and overall action items than those that fall in the Exercise and Process categories as the need to know becomes lower and the risk of knowledge transfer becomes higher

## Red Team Planning

- Red Team Planning
  - Fill any planning gaps
  - Attack Infrastructure/C2
  - Reconnaissance
  - Social Engineering
  - Weaponization
- Initial Access/Foothold
- Network Propagation
- Action on Objectives



### Matrix of command and control frameworks for Red Teamers

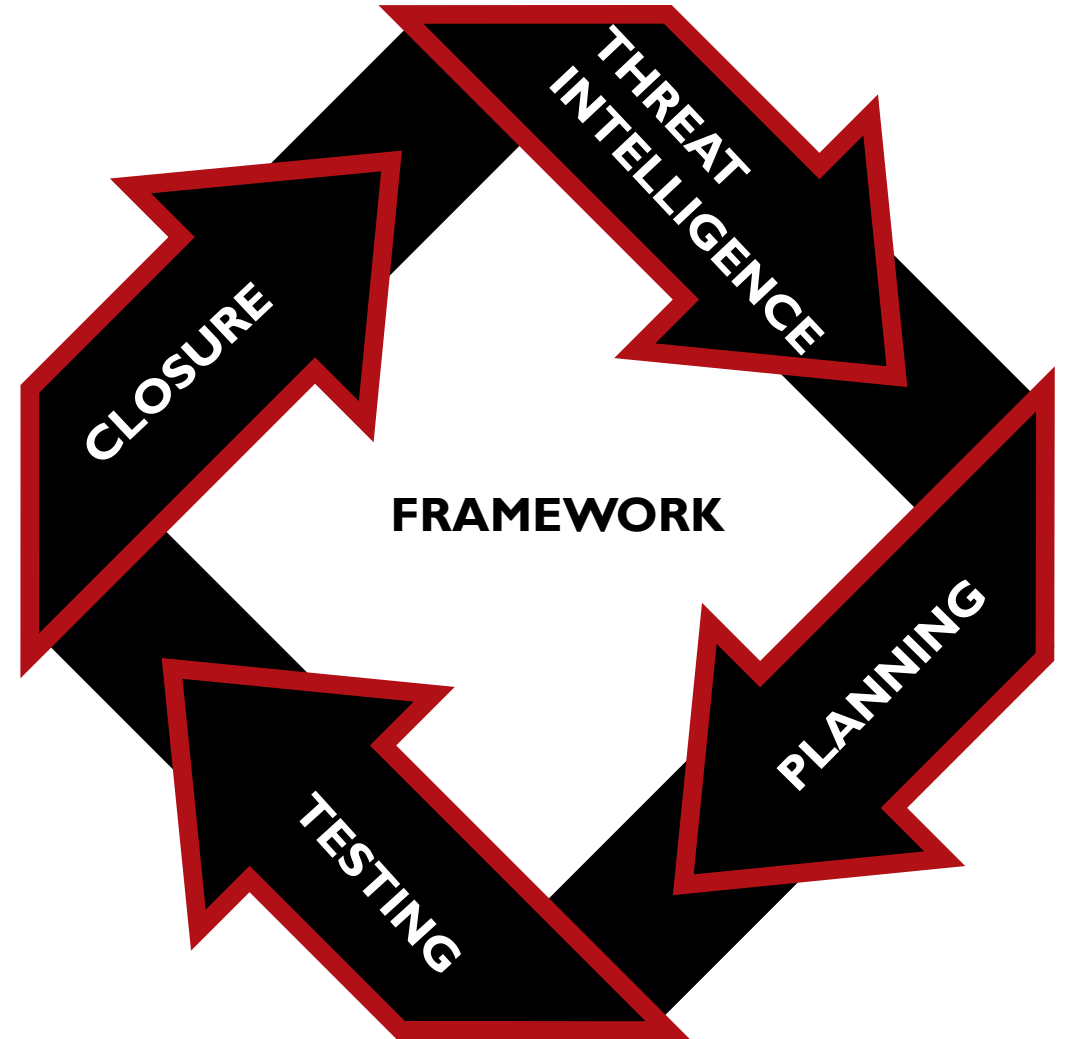
- Google doc of most C2 frameworks
- Documents various capabilities of each framework
- There is no right or wrong, better or worse framework
- Find ideal C2 for your current objective
- Wizard like UI to select which one
- [www.thec2matrix.com](http://www.thec2matrix.com)
- [howto.thec2matrix.com](http://howto.thec2matrix.com)



1			Language	UI	Agents	Channel												
2	Name	Slingshot	Kali	Server	Agent	Multi-User	UI	API	Windows	Linux	macOS	TCP	HTTP	HTTP2	HTTP3	DNS	DoH	ICMP
3	Apfell			Python	Python	Yes	Web	Yes	No	Yes	Yes	No	Yes	No	No	No	No	No
7	CALDERA			Python	Go	Yes	Web	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No
8	CHAOS	No		Go	Go	No	CLI	No	Yes	Yes	Yes	Yes	No	No	No	No	No	No
9	Cobalt Strike			Java	C	Yes	GUI	No	Yes	No	No	Yes	Yes	No	No	Yes	Yes	No
10	Covenant	Yes	Yes	C#	C#	Yes	Web	Yes	Yes	No	No	No	Yes	No	No	No	No	No
11	Dali			Python	Python	No	CLI	No	BYOI	BYOI	BYOI	No	Yes	No	No	No	No	No
12	Empire	Yes	Yes	Python	PowerShell	Yes	GUI	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No
13	EvilOSX		Yes	Python	Python	No	GUI	No	Yes	Yes	Yes	No	Yes	No	No	No	No	No
14	Faction C2	Yes	Yes	.NET	.NET	Yes	Web	Yes	Yes	No	No	Yes	Yes	No	No	No	No	No
15	FlyingAFalseFlag			Python	C++	No	CLI	No	Yes	No	No	No	Yes	No	No	No	No	No
16	FudgeC2		Yes	Python	Powershell	Yes	Web	No	Yes	No	No	No	Yes	No	No	No	No	No
17	godoh		Yes	Go	Go	No	CLI	No	Yes	Yes	Yes	No	No	No	No	Yes	Yes	No
18	HARS			Python	C#	No	CLI	No	Yes	No	No	No	Yes	No	No	No	No	No
19	ibombshell		Yes	Python	PowerShell	No	GUI	No	Yes	Yes	Yes	No	Yes	No	No	No	No	No
20	INNUENDO			Python	Python	Yes	Web	Yes	Yes	Yes	Yes	No	Yes	No	No	Yes	No	Yes
21	Koadic C3	Yes	Yes	Python	JScript/VBScript	No	GUI	No	Yes	No	No	No	Yes	No	No	No	No	No
22	MacShellSwift	Yes		Python	Swift	No	CLI	No	No	No	Yes	No	Yes	No	No	No	No	No
23	Merlin	Yes	Yes	Go	Go	No	CLI	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No	No
24	Metasploit			Ruby	C/Java/PHP/Python	Yes	CLI	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
26	Ninja			Python	C#/PowerShell	Yes	CLI	No	Yes	No	No	No	Yes	No	No	No	No	No
28	Nuages			Python	C#	Yes	GUI	Yes	Yes	No	No	No	Yes	No	No	No	No	No
29	Octopus			Python	PowerShell	No	GUI	No	Yes	No	No	No	Yes	No	No	No	No	No
31	PoshC2		Yes	Python	PowerShell/C#/Python	Yes	CLI	No	Yes	Yes	Yes	No	Yes	No	No	No	No	No
32	PowerHub		Yes	Python	PowerShell	Yes	Web	No	Yes	No	No	No	Yes	No	No	No	No	No
33	Prismatica			Javascript/Python	JScript/.NET/Rust	Yes	GUI	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
36	QuasarRAT			C#	C#	No	GUI	No	Yes	No	No	Yes	No	No	No	No	No	No
37	Red Team Toolkit			Python	C++	No	CLI	No	Yes	No	No	No	Yes	No	No	No	No	No
39	ReverseTCPShell			PowerShell	PowerShell	No	CLI	No	Yes	No	No	Yes	No	No	No	No	No	No
40	SCYTHE			Python	C	Yes	Web	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	No	No

## Show Value

- Analysis and Response
  - Red Team Reveal
  - Replay
  - Purple Team
- Reporting
- Remediation and Action Plan
  - People
  - Process
  - Technology



## What is VECTR?

- Free platform for planning and tracking red team and purple team assessments
- Heavy focus on collaborative testing between red & blue teams with tracking of specific red team activities and defensive outcomes
- Designed to promote transparency and education between red team operators, security operations, engineering, threat intel & hunt teams



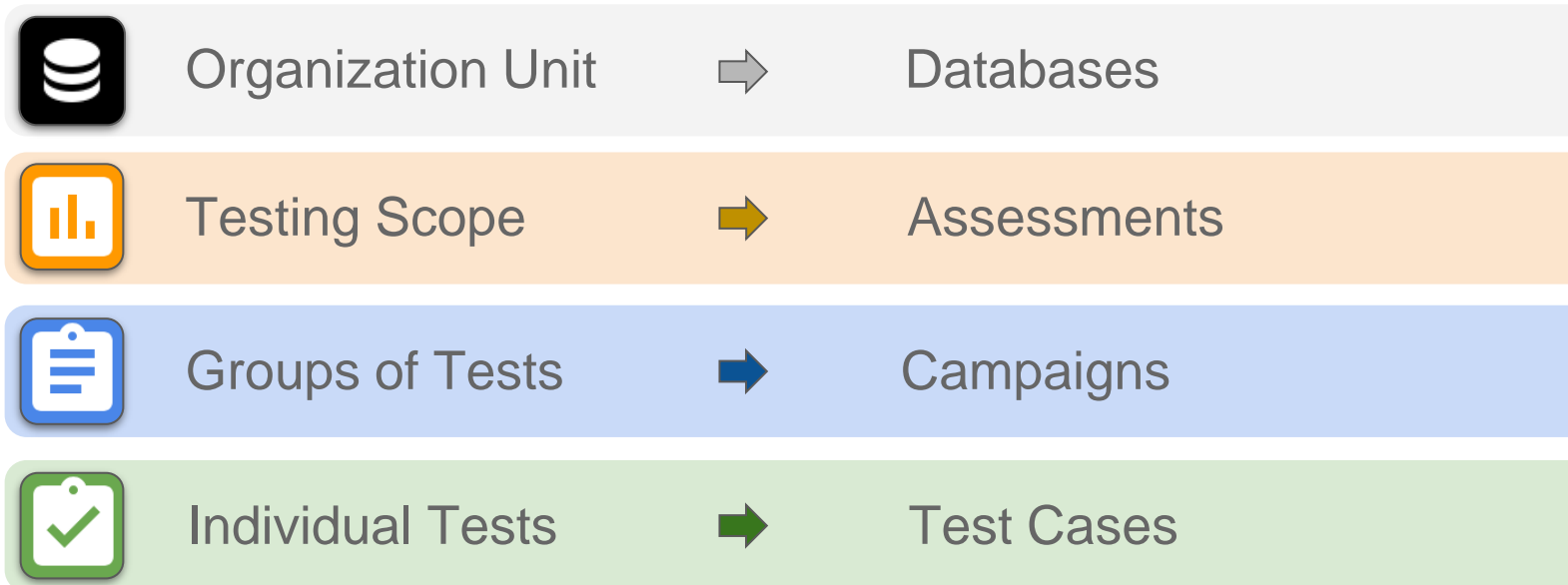
## Common Use Cases for VECTR

- Measure enterprise defenses across the MITRE ATT&CK framework
- Structured testing and evaluations for existing and PoC security tools in the environment
- Import structured CTI (STIX 2.0 bundles) for adversary emulation planning
- Create custom assessments, campaigns, and test case templates for repeatable testing across multiple environments and targets
- Report on executive summary level or drill-down into assessment results, visualize with dynamic heat map, historical trending, and detailed reporting views

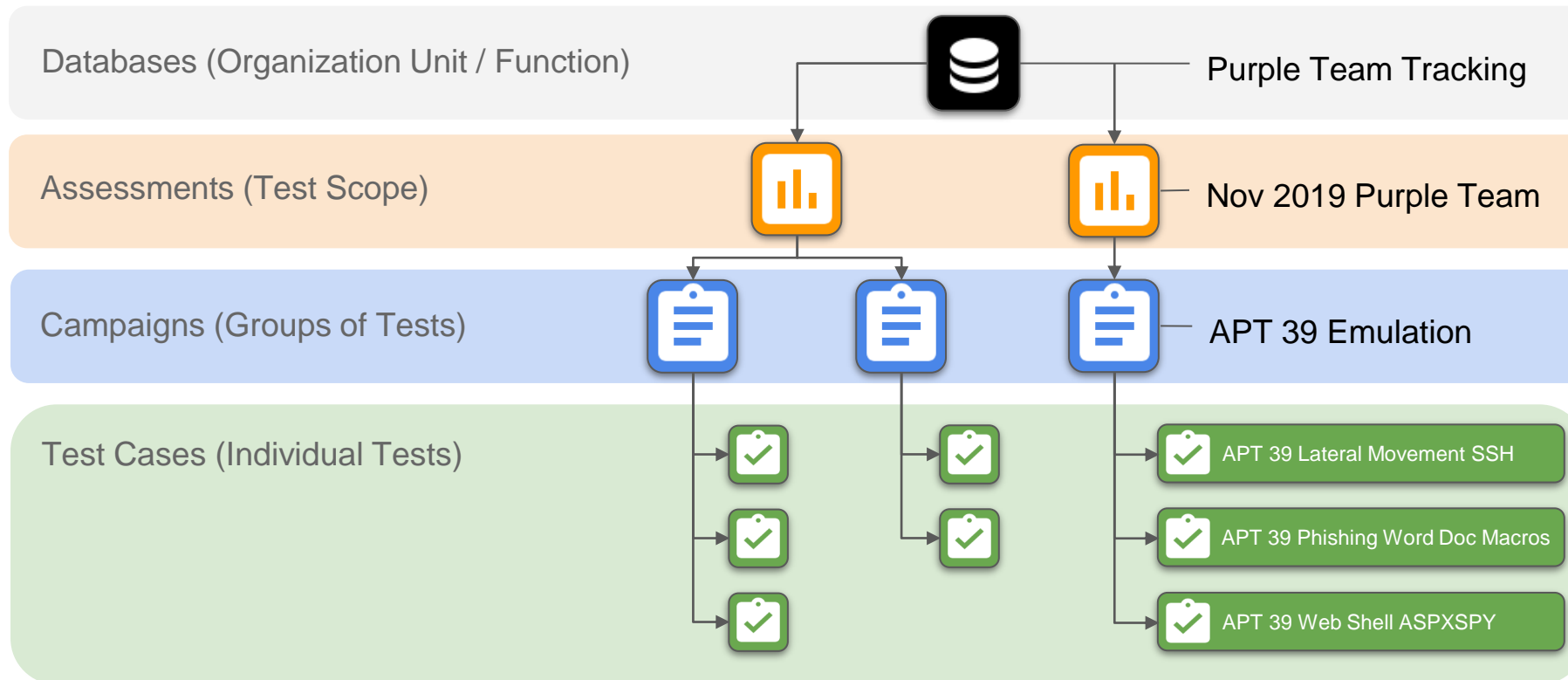
## Getting Started

- Download VECTR at <https://github.com/SecurityRiskAdvisors/VECTR>
- Read the docs: <https://docs.vectr.io>
- Join the community: <https://vectr.io>
- Contact the team at [vectr@sra.io](mailto:vectr@sra.io) with questions & feedback

# VECTR Concepts



# Data Hierarchy



# Importing Assessment Templates

Import VECTR Template Data  
Imports from TAXII Server or JSON File.

**TAXII SERVER** No Data ▼ Edit TAXII Server Detail

**TAXII COLLECTIONS** List of usable Collections on the TAXII Server Refresh Collections

OR

**JSON FILE** Alternative import method: VECTR data JSON file.

enterprise\_may2020.json  
385 KB Upload complete tap to undo ✕

**Submit**

**VECTR public TAXII server - coming soon!**

**Drag and drop STIX 2.0 bundles here from MITRE ATT&CK CTI and templates created in VECTR**

# Importing Content from Third-party Sources

## Import latest MITRE ATT&CK enterprise bundle

Import STIX2 Data  
Select Data from STIX2 Collection to be imported and merged with VECTR Data.  
Top level items will be campaigns in VECTR, under each is a list of test cases and the STIX objects that comprise them.

0 Assessment Group Templates. 0 Campaigns. 0 Total Test Cases Selected.

First Previous **1** 2 3 4 5 6 7 8 9 10 Next Last

- List of **All Campaigns** → 390 Total Campaigns. 4478 Total Test Cases.
- Campaign: **3PARA RAT** → 6 Total Test Cases.
- Campaign: **4H RAT** → 6 Total Test Cases.
- Campaign: **ADVSTORESHELL** → 23 Total Test Cases.
- Campaign: **APT1** → 16 Total Test Cases.
- Campaign: **APT12** → 4 Total Test Cases.
- Campaign: **APT18** → 12 Total Test Cases.
- Campaign: **APT19** → 20 Total Test Cases.
- Campaign: **APT28** → 53 Total Test Cases.
- Campaign: **APT29** → 23 Total Test Cases.
- Campaign: **APT3** → 44 Total Test Cases.

## Import latest Red Canary Atomic Red index

Import Atomic Red  
Select Data from <https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/Indexes/index.yaml>.  
Top level items will be an Assessment in VECTR. Campaigns will be mapped from MITRE tactics.  
Under each Campaign is a list of Test Cases that correspond to atomic\_tests

0 Assessment Group Templates. 0 Campaigns. 0 Total Test Cases Selected.

First Previous **1** Next Last

- List of **All Campaigns** → 12 Total Campaigns. 639 Total Test Cases.
- Campaign: **Collection** → 28 Total Test Cases.
- Campaign: **Command & Control** → 32 Total Test Cases.
- Campaign: **Credential Access** → 45 Total Test Cases.
- Campaign: **Defense Evasion** → 199 Total Test Cases.
- Campaign: **Discovery** → 98 Total Test Cases.
- Campaign: **Execution** → 42 Total Test Cases.
- Campaign: **Exfiltration** → 6 Total Test Cases.
- Campaign: **Impact** → 23 Total Test Cases.
- Test Case: **Account Access Removal - T1531 - Change User Password - Windows**

# Importing Custom Assessments (VECTR-to-VECTR sharing)

Import VECTR Data  
Data to be imported from file and merged with VECTR Template Data.

1 Assessment Group Templates. 25 Campaigns. 142 Total Test Cases Selected. Submit

Assessment Group Template: Enterprise Bundle - May 2020 → 25 Campaigns.

- Campaign: Email with Malicious Links → 11 Test Cases.
- Campaign: Register Phishing Domains → 2 Test Cases.
- Campaign: Endpoint Execution - B
- Campaign: Data Exfil Methods - E
- Campaign: Email With Malicious A
- Campaign: Credential Dumping →
- Campaign: Malware Simulation →
- Campaign: C2 Channels → 6 T
- Campaign: Endpoint Persistence
- Campaign: Local Collection →
- Campaign: Defensive Security Eva
- Campaign: Endpoint Execution →
- Campaign: Data Exfil Methods - N
- Campaign: Email Spoofing → 3
- Campaign: External Perimeter Act
- Campaign: Network Access Controls → 7 Test Cases.

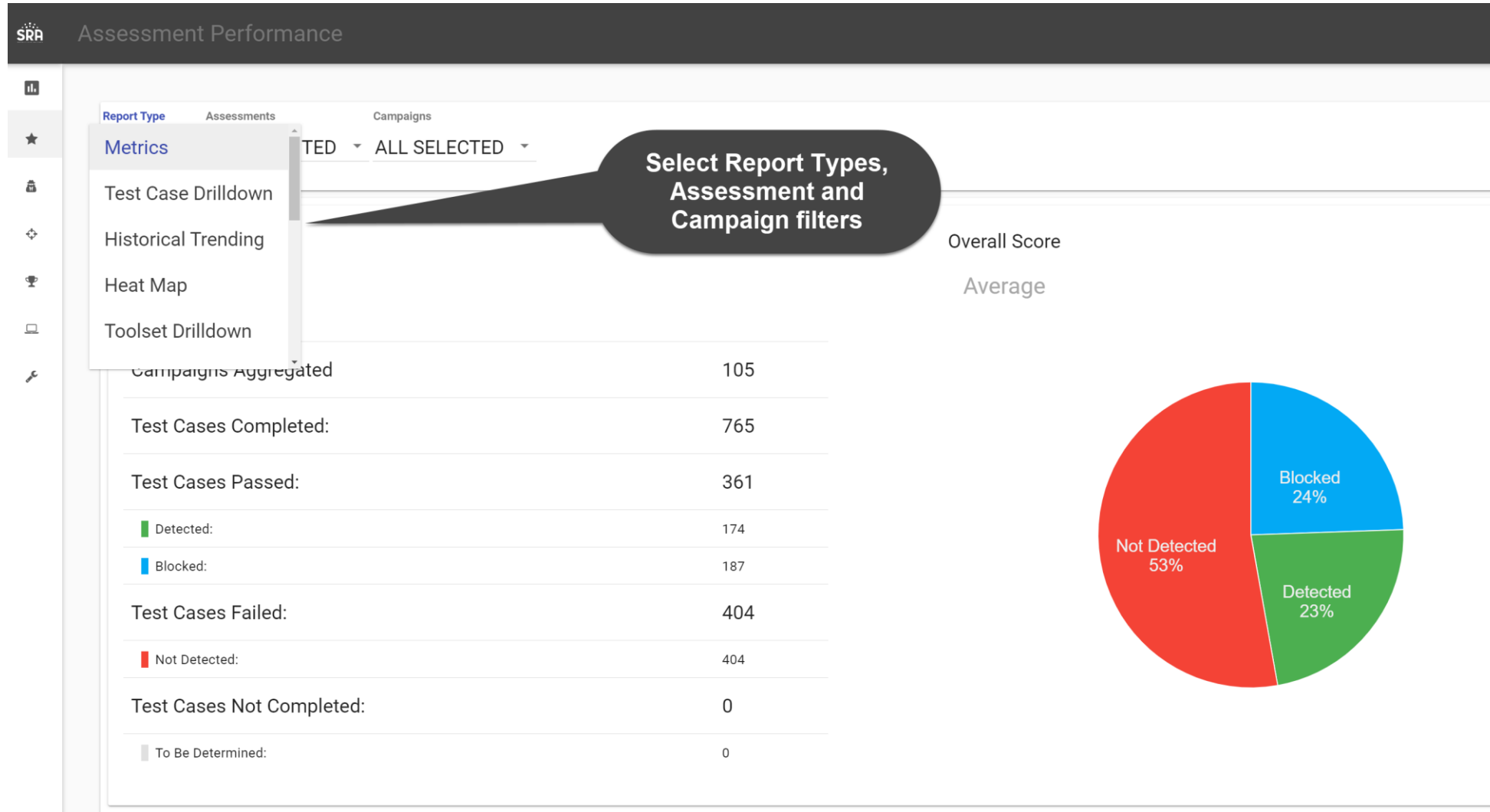
### VECTR Data Import Confirmation

Please confirm import of the following data:

<b>Added +</b>	
1 Assessment Group Template	4 Campaign Templates
17 Test Cases	
<b>Modified ↗</b>	
19 Campaign Templates	115 Test Cases
<b>Unchanged ↶</b>	
3 Kill Chains	2 Campaign Templates
20 Phases	10 Test Cases
18 Expected Detection Layers	1 Organizations

Cancel Confirm

# Reporting Dashboard



# Dynamic Heat Map

**Report Type:** Heat Map | **Assessments:** Enterprise Purple - 2018 Q1 + 3 more | **Campaigns:** Register Phishing Domains + 88 more | **Outcomes:** ALL SELECTED | **Statuses:** Completed + 3 more

**Assessment Heat Map**

Map Type: Latest | Display Mode: Allow Repeats | MITRE FILTERS | VECTR FILTERS | EXPORT LAYER | STATS | PNG

**Summary:** Test Cases: 282 | Unique Test Cases: 244 | Techniques: 79 | Unique Techniques: 63 | Blocked: 50 | Detected: 52 | Not Detected: 31

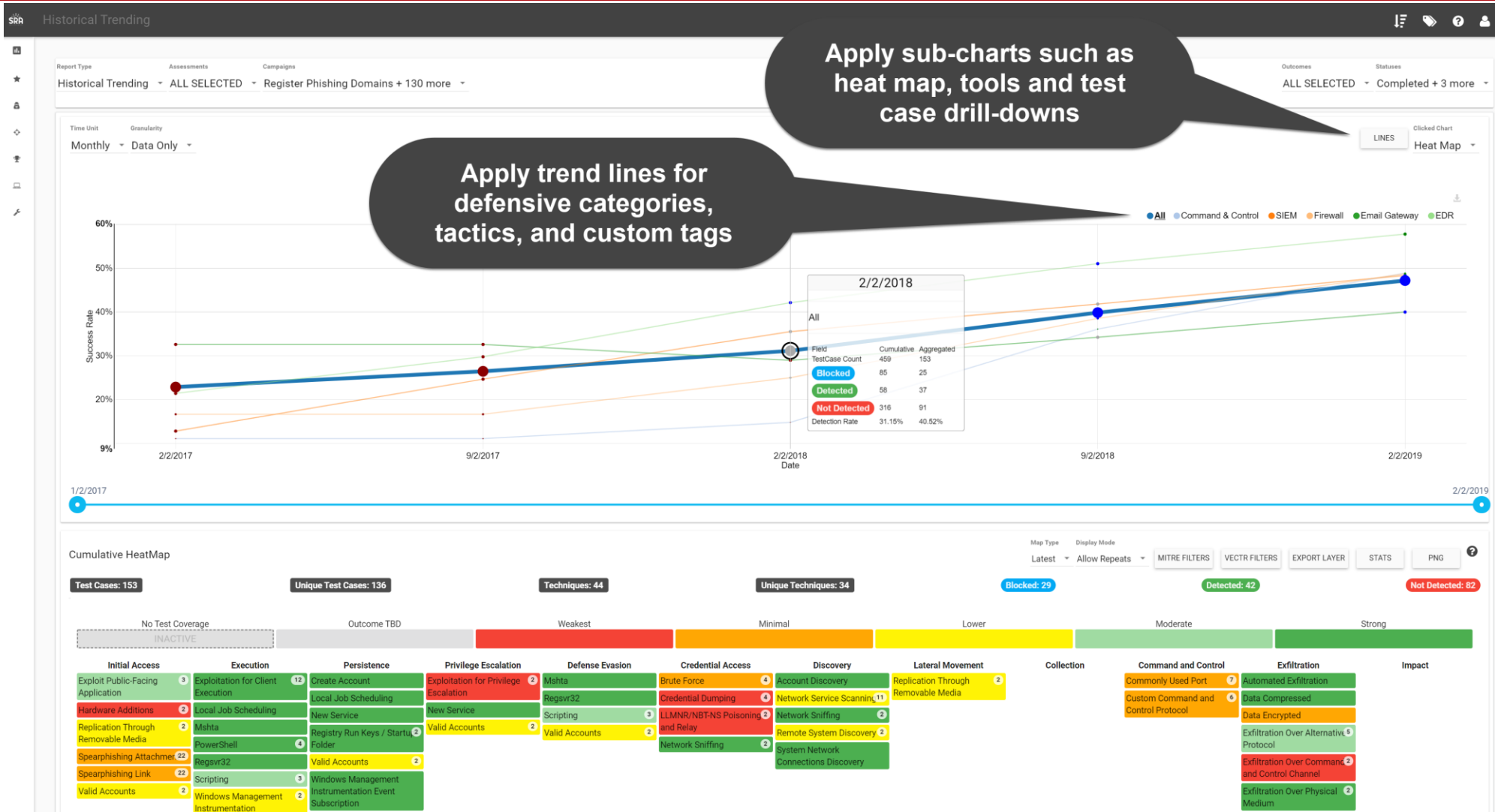
**Legend:** No Test Coverage (INACTIVE), Outcome TBD, Weakest, Minimal, Lower

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
Exploit Public-Facing Application (3)	Component Object Model and Distributed COM (2)	Create Account (2)	Exploitation for Privilege Escalation (2)	DCShadow	Brute Force (6)	Account Discovery (3)	Component Object Model (2)
External Remote Services (2)	Dynamic Data Exchange	External Remote Services	New Service	Disabling Security Tools (4)	Credential Dumping (8)	Extract Password Hashes via VSS (Enterprise Purple - 2020 Q1 T1003 • Logged: No) [Detected]	Data from ... (2)
Hardware Additive (5)	Execution through API	Local Job Scheduling (2)	Parent PID Spoofing	Indicator Blocking	Kerberoasting (2)	Extract Password Hashes via NTDSUtil (Enterprise Purple - 2020 Q1 T1003 • Logged: No) [Detected]	Custom Command and Control Protocol (7)
Replication Through Removable Media (3)	Exploitation for Client Execution (12)	Modify Existing Service	Valid Accounts (4)	Masquerading (8)	LLMNR/NBT-NS (3)	Extract password hashes from DC using DC ... (Enterprise Purple - 2020 Q1 T1003 • Logged: No) [NotDetected]	Multi-hop Proxy
Spearphishing Attachment (31)	Local Job Scheduling (2)	New Service	Registry Run Key (2)	Mshta (2)	Poisoning and Relay	Extract password hashes from DC by copyin... (Enterprise Purple - 2020 Q1 T1003 • Logged: No) [Detected]	Data Compressed (2)
Spearphishing L (33)	Mshta (2)	Registry Run Key (2)	Startup Folder	Obfuscated Files and Information (2)	Network Sniffing (3)	Extract Logonpasswords via Dumpert (Enterprise Purple - 2020 Q3 T1003 • Logged: TBD)	Data Encrypted (2)
Trusted Relationship (2)	PowerShell (4)	Valid Accounts (4)	Windows Management Instrumentation (4)	Parent PID Spoofing	Scripting (5)		Exfiltration Over Alternative Protocol (7)
Valid Accounts (4)	Regsvr32 (2)	Windows Management Instrumentation (4)	Scripting (5)	Regsvr32 (2)			Exfiltration Over Command and Control Channel (3)
	Signed Binary Proxy Execution	Scripting (5)		Scripting (2)			Exfiltration Over Other Network Medium (2)
	Trusted Developer Utilities			Scripting (2)			Exfiltration Over Physical Medium (5)
	User Execution (5)			Scripting (2)			

**Callout 1:** Apply various MITRE and VECTR filters, such as threat group overlays

**Callout 2:** Drill down into multiple test case procedures mapped to a technique

# Historical Trending with sub-charts



# Campaign Dashboard

SRR SANS\_DEMO / Adversary Emulation 2020 / APT19

APT19: Escalation Path

Initial Access Persistence Defense Evasion Command & Control Discovery

APT19 - Drive-by Compromise  
APT19 - Spearphishing Attachment  
APT19 - Registry Run Keys / Startup Folder - Empire  
APT19 - Modify Existing Service - Empire  
APT19 - DLL Side-Loading  
APT19 - Deobfuscate/Decode Files or Information  
APT19 - Obfuscated Files or Information - Empire  
APT19 - Hidden Window  
APT19 - Modify Registry  
APT19 - Standard Application Layer Protocol - Cobalt Strike - Empire  
APT19 - Commonly Used Port - Cobalt Strike - Empire  
APT19 - Data Encoding  
APT19 - System Information Discovery - Empire  
APT19 - System Network Configuration Discovery - Empire  
APT19 - System Owner/User Discovery

Timeline

- 07/01/2020 09:44:49 APT19 - Standard Application Layer Protocol - Cobalt Strike - Empire : outcome changed to Detected
- 07/01/2020 09:44:47 APT19 - Standard Application Layer Protocol - Cobalt Strike - Empire : status changed to Completed
- 07/01/2020 09:44:46 APT19 - Standard Application Layer Protocol - Cobalt Strike - Empire : status changed to InProgress
- 07/01/2020 09:44:36 APT19 - Drive-by Compromise : outcome changed to Blocked
- 07/01/2020 09:44:35 APT19 - Drive-by Compromise : status changed to Completed
- 07/01/2020 09:44:34 APT19 - Drive-by Compromise : status changed to InProgress

Escalation diagram, test cases aligned to kill chain phase or MITRE tactics

Test Cases

Phase	Technique	Test Case	Status	Outcome	Tags	Action
All	search ...	search ...	All	All	All	
Discovery	System Information Discovery	APT19 - System Information Discovery - Empire	Completed	Not Detected	High Priority	📄 ⚙️ 🗑️ ✖️
Persistence	Registry Run Keys / Startup Folder	APT19 - Registry Run Keys / Startup Folder - Empire	Completed	Blocked		📄 ⚙️ 🗑️ ✖️
Defense Evasion	DLL Side-Loading	APT19 - DLL Side-Loading	Completed	Not Detected	Medium Priority	📄 ⚙️ 🗑️ ✖️
Execution	Regsvr32	APT19 - Regsvr32	Completed	Detected		📄 ⚙️ 🗑️ ✖️
Initial Access	Drive-by Compromise	APT19 - Drive-by Compromise	Completed	Blocked		📄 ⚙️ 🗑️ ✖️
Command & Control	Standard Application Layer Protocol	APT19 - Standard Application Layer Protocol - Cobalt Strike - Empire	Completed	Detected		📄 ⚙️ 🗑️ ✖️

# Test Case Panel

Edit Extract Logonpasswords via Dumpert Test Case

**Status: Completed**

▶ || ■ ▲

**Attack Start**

07/01/2020 09:54:20  
status changed to InProgress

**Attack Stop**

07/01/2020 09:54:21  
status changed to Completed

**Source IPs**

Linux VM

**Red Team Details**

Name  
Extract Logonpasswords via Dumpert

Description  
Use dumpert to extract credentials from LSASS process memory

Technique  
Credential Dumping

Phase  
Credential Access

Operator Guidance  
beacon>  
dumpert

References  
+

**Attacker Tools**

Dumpert  
Cobalt Strike

**Target Assets**

Target Laptop

**Blue Team Details**

Outcome  
 TBD  Blocked  Detected  NotDetected

Detecting Blue Tool(s):

EDR platform

Was an alert triggered?  
 Yes  TBD  No

Outcome Notes  
Ran dumpert on target workstation, successfully blocked by EDR/NGAV agent and alerted via SIEM.

Tags  
**High Priority** **RE-TEST**

Rules

**Detection**

1) Suspicious process execution is detected by EDR or other endpoint security tool, or alerted in SIEM based on Windows or sysmon event IDs

**Prevention**

1) Suspicious process execution is blocked by EDR or other endpoint security tool

**Detection Time**

07/01/2020 09:55:48  
outcome changed to Blocked

**Expected Detection Layers**

SIEM  
EDR  
Endpoint Protection

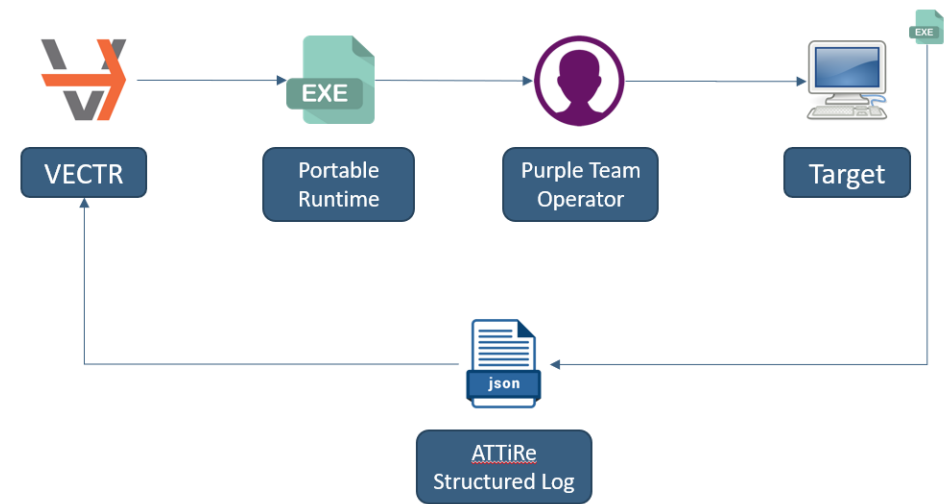
**Red Team TTPs, operator guidance, source/targets**

**Blue team expected and actual outcomes, notes, tools, custom tags**

Cancel Save Next

## VECTR: On Deck Features

- New auth layer with SSO and MFA support
- VECTR Portable Runtime Automation and structured logging format
  - ATTiRe – Attack Tool Timing and Reporting
  - Support import of data from SCYTHER
- Test Case Panel re-design
- Detection Rules re-design
- Reporting View updates and more customization
- More granular RBAC than current roles
- Public API & TAXII Server



SANS

Thank You!  
Questions?