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

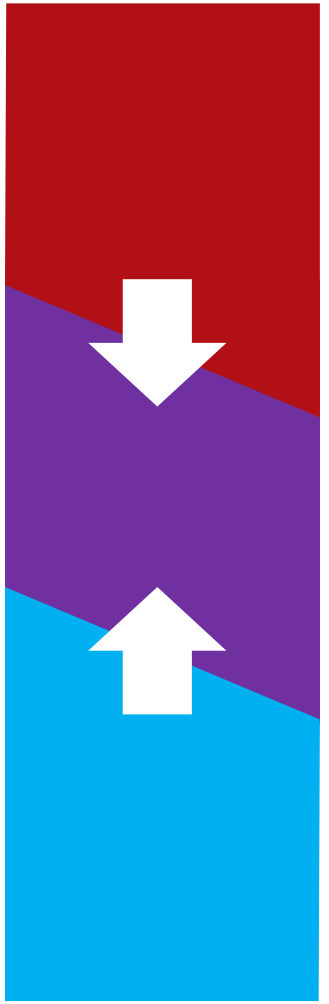
- **Definition:** the defenders in an organization entrusted with identifying and remediating attacks. Generally associated with Security Operations Center or Managed Security Service Provider (MSSP), Hunt Team, Incident Response, and Digital Forensics. Really, it is everyone's responsibility!
- **Goal:** 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

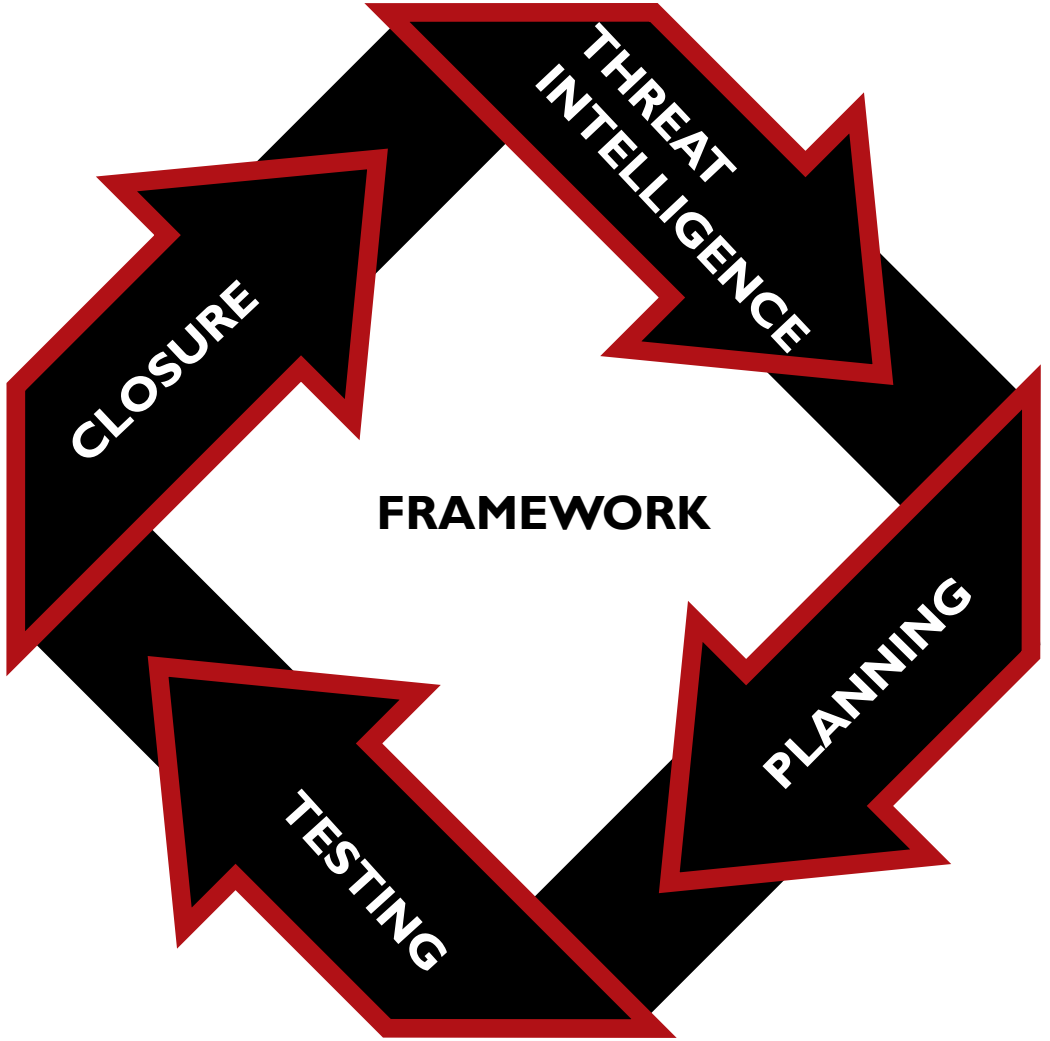
- **Definition:** A function, or virtual team, where red and blue work together to improve the overall security of the organization. Red Team does not focus on stealth as they normally would.
- **Goal:** Red Team emulates adversary TTPs while blue teams watch and improve detection and response policies,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



Framework for SEC564

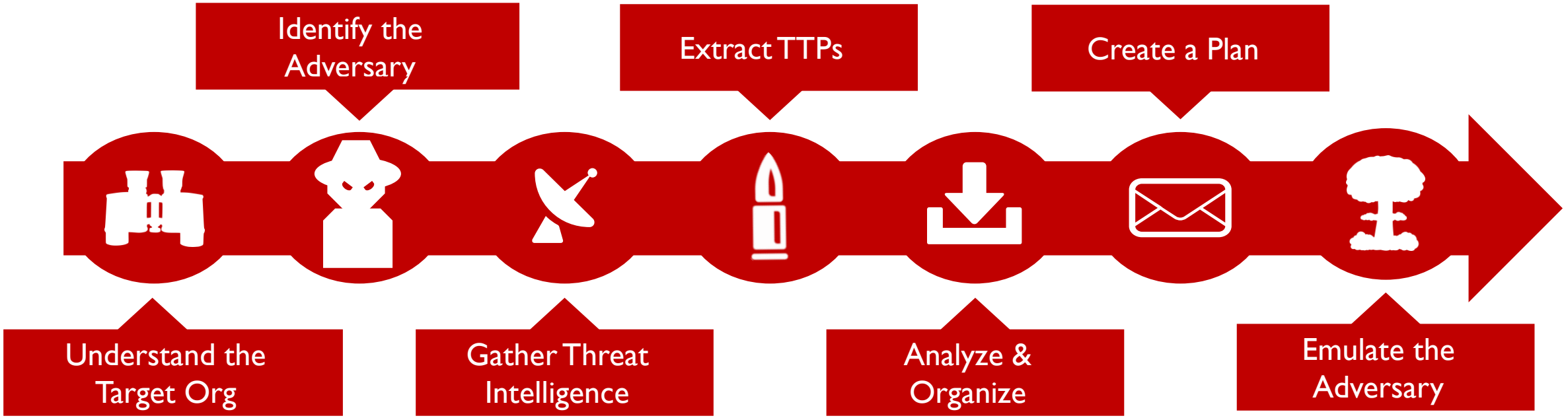
Like most organizations, this course will take a hybrid approach based on the frameworks and methodologies just introduced

- 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)**



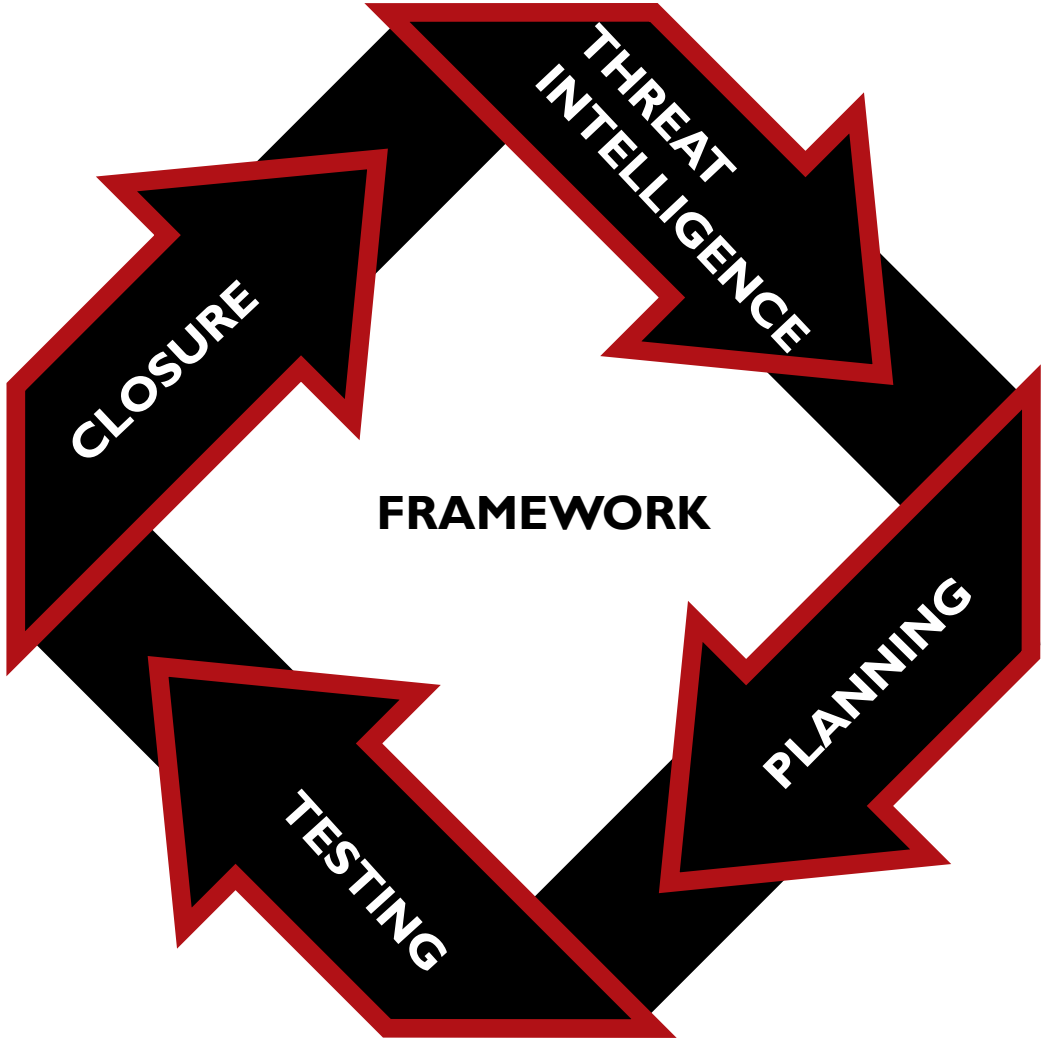
MITRE® ATT&CK™

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	AppInit 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	AppInit 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



Assumed Breach

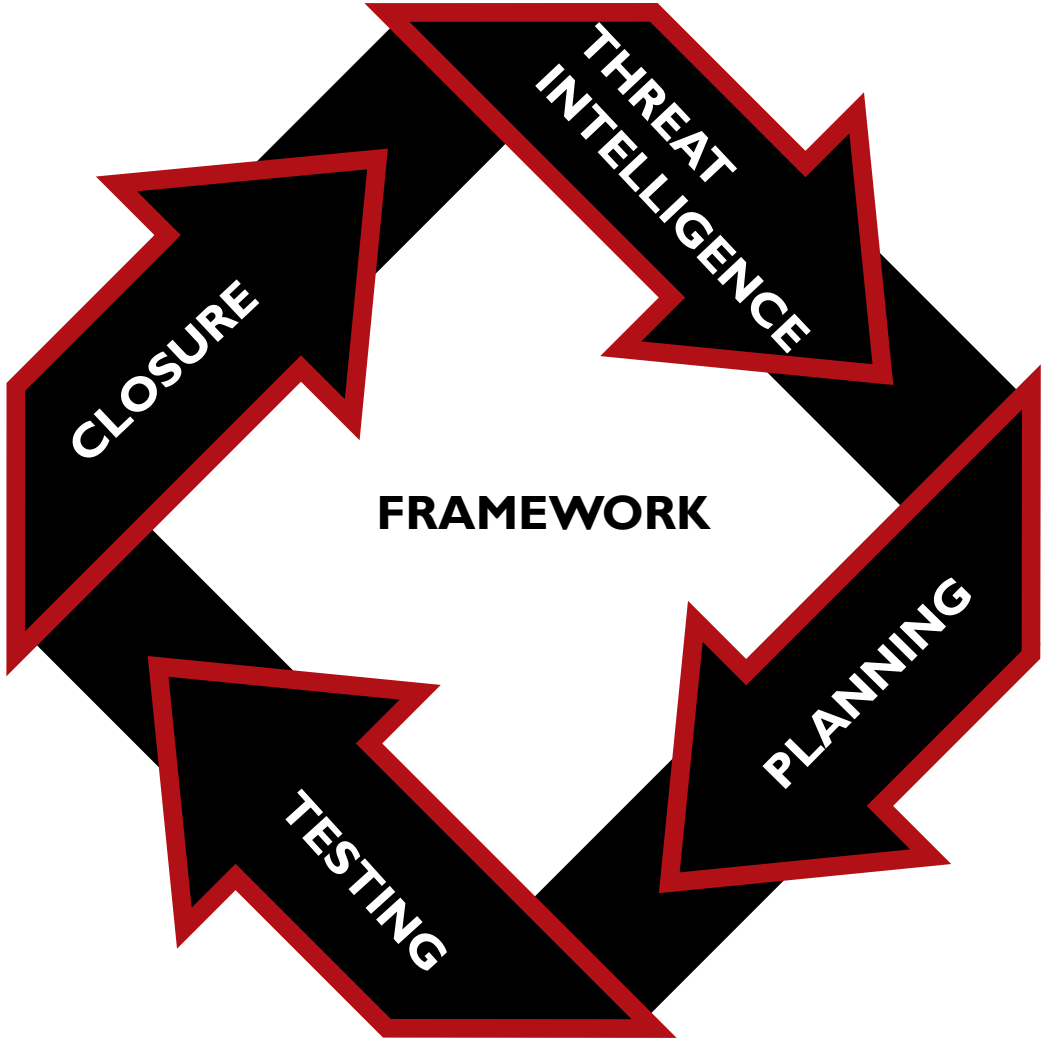
Philosophy and understanding one will be breached

- 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
Governance	Approve the attack scenario, the final report and remediation action items. Governance agents should also receive status updates throughout the exercise
Project Management	Coordinate entire Red Team Exercise including threat intelligence gathering; target reconnaissance; Testing Phase communication; and management of timeline and objectives
Threat Intelligence	Identify cyber threat actor(s) with the sophistication and desire to attack the organization; provide the group's technical and behavioral profile including TTPs
Risk Avoidance	Receive daily updates on all Red Team actions and are responsible for avoiding or reducing the material impact of the exercise to business operations
Action Item Remediation Owners	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



The C2 Matrix

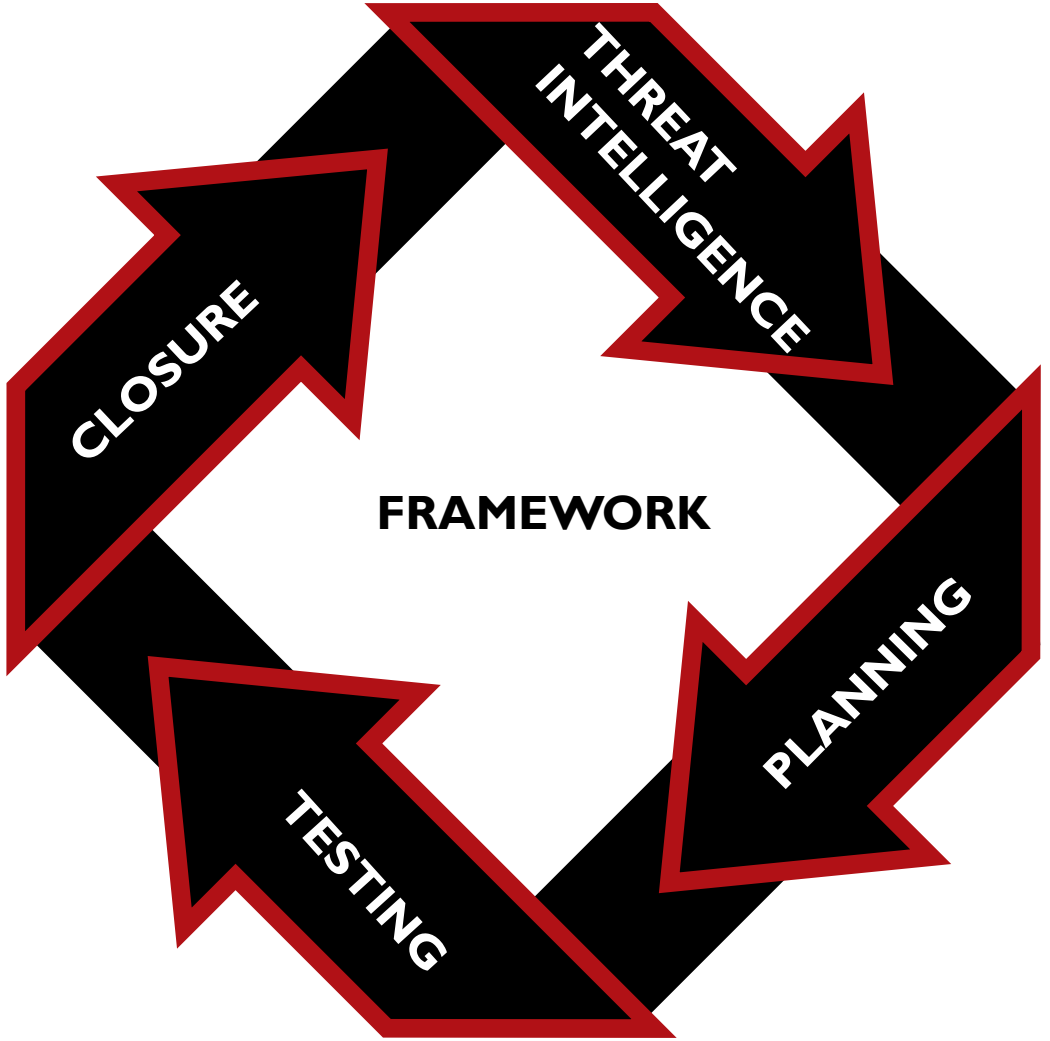
Matrix of command and control frameworks for Red Teamers

- 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
- howto.thec2matrix.com

				Language		UI			Agents			Channel						
Name	Slingshot	Kali	Server	Agent	Multi-User	UI	API	Windows	Linux	macOS	TCP	HTTP	HTTP2	HTTP3	DNS	DoH	ICMP
Apfell			Python	Python	Yes	Web	Yes	No	Yes	Yes	No	Yes	No	No	No	No	No
CALDERA			Python	Go	Yes	Web	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No
CHAOS	No		Go	Go	No	CLI	No	Yes	Yes	Yes	Yes	No	No	No	No	No	No
Cobalt Strike			Java	C	Yes	GUI	No	Yes	No	No	Yes	Yes	No	No	Yes	Yes	No
Covenant	Yes	Yes	C#	C#	Yes	Web	Yes	Yes	No	No	No	Yes	No	No	No	No	No
Dali			Python	Python	No	CLI	No	BYOI	BYOI	BYOI	No	Yes	No	No	No	No	No
Empire	Yes	Yes	Python	PowerShell	Yes	GUI	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No
EvilOSX		Yes	Python	Python	No	GUI	No	Yes	Yes	Yes	No	Yes	No	No	No	No	No
Faction C2	Yes	Yes	.NET	.NET	Yes	Web	Yes	Yes	No	No	Yes	Yes	No	No	No	No	No
FlyingAFalseFlag			Python	C++	No	CLI	No	Yes	No	No	No	Yes	No	No	No	No	No
FudgeC2		Yes	Python	Powershell	Yes	Web	No	Yes	No	No	No	Yes	No	No	No	No	No
godoh		Yes	Go	Go	No	CLI	No	Yes	Yes	Yes	No	No	No	No	Yes	Yes	No
HARS			Python	C#	No	CLI	No	Yes	No	No	No	Yes	No	No	No	No	No
ibombshell		Yes	Python	PowerShell	No	GUI	No	Yes	Yes	Yes	No	Yes	No	No	No	No	No
INNUENDO			Python	Python	Yes	Web	Yes	Yes	Yes	Yes	No	Yes	No	No	Yes	No	Yes
Koadic C3	Yes	Yes	Python	JScript/VBScript	No	GUI	No	Yes	No	No	No	Yes	No	No	No	No	No
MacShellSwift	Yes		Python	Swift	No	CLI	No	No	No	Yes	No	Yes	No	No	No	No	No
Merlin	Yes	Yes	Go	Go	No	CLI	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No	No
Metasploit			Ruby	C/Java/PHP/Python	Yes	CLI	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
Ninja			Python	C#/PowerShell	Yes	CLI	No	Yes	No	No	No	Yes	No	No	No	No	No
Nuages			Python	C#	Yes	GUI	Yes	Yes	No	No	No	Yes	No	No	No	No	No
Octopus			Python	PowerShell	No	GUI	No	Yes	No	No	No	Yes	No	No	No	No	No
PoshC2		Yes	Python	PowerShell/C#/Python	Yes	CLI	No	Yes	Yes	Yes	No	Yes	No	No	No	No	No
PowerHub		Yes	Python	PowerShell	Yes	Web	No	Yes	No	No	No	Yes	No	No	No	No	No
Prismatica			Javascript/Python	JScript/.NET/Rust	Yes	GUI	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
QuasarRAT			C#	C#	No	GUI	No	Yes	No	No	Yes	No	No	No	No	No	No
Red Team Toolkit			Python	C++	No	CLI	No	Yes	No	No	No	Yes	No	No	No	No	No
ReverseTCPShell			PowerShell	PowerShell	No	CLI	No	Yes	No	No	Yes	No	No	No	No	No	No
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

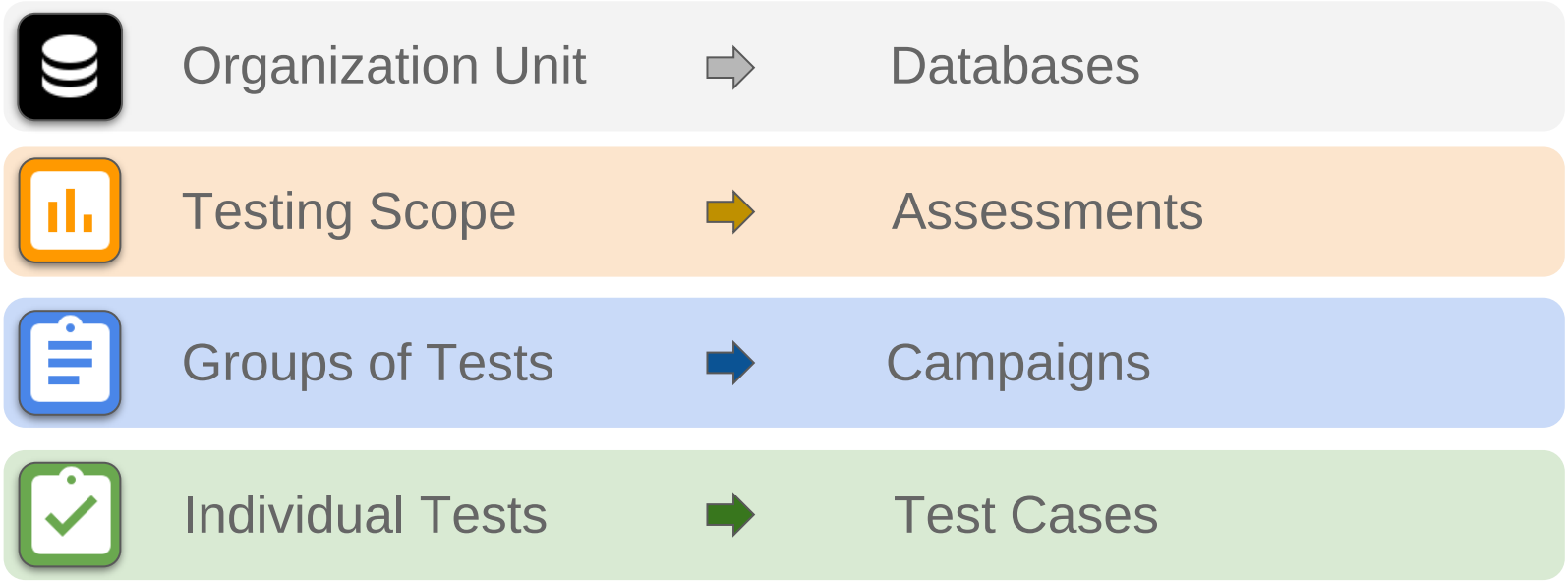
Common Use Cases for VECTR

- 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

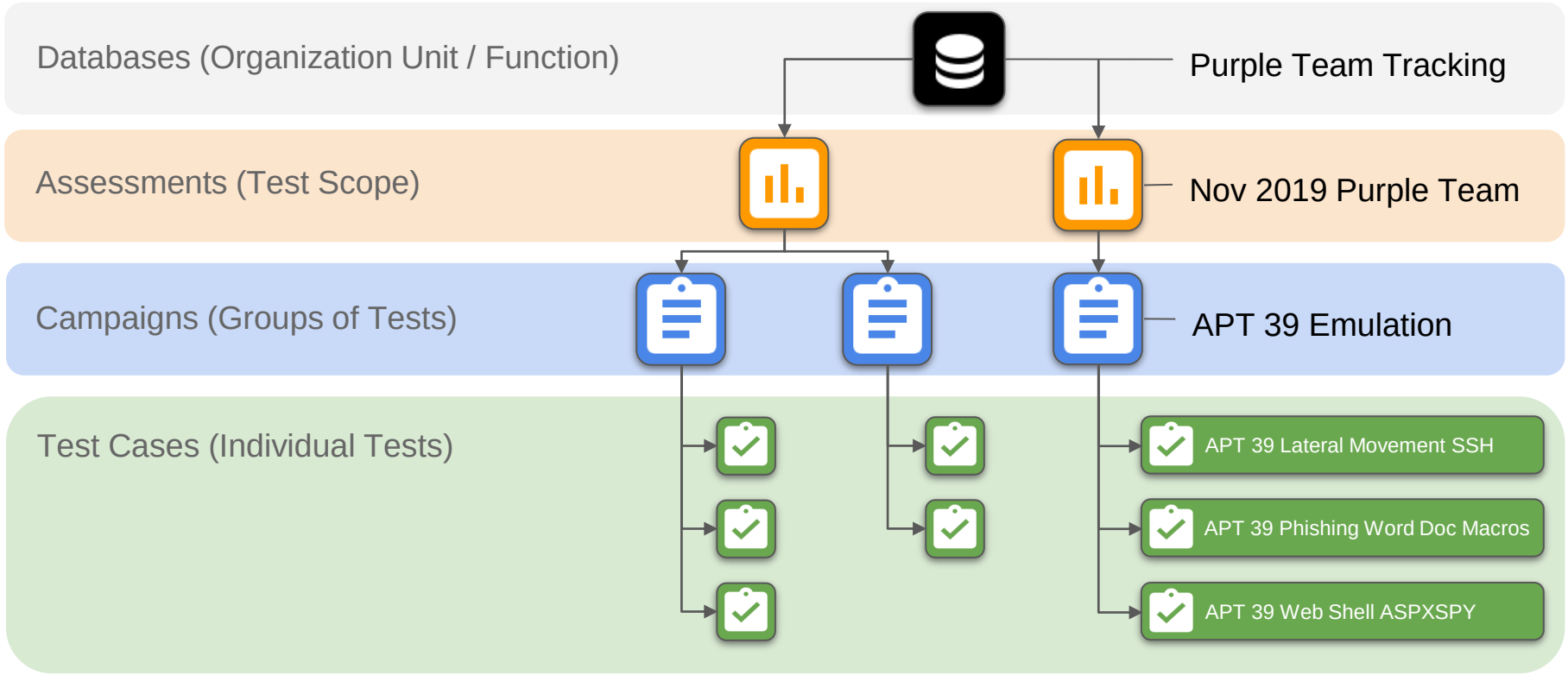
Getting Started

- 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 with questions & feedback

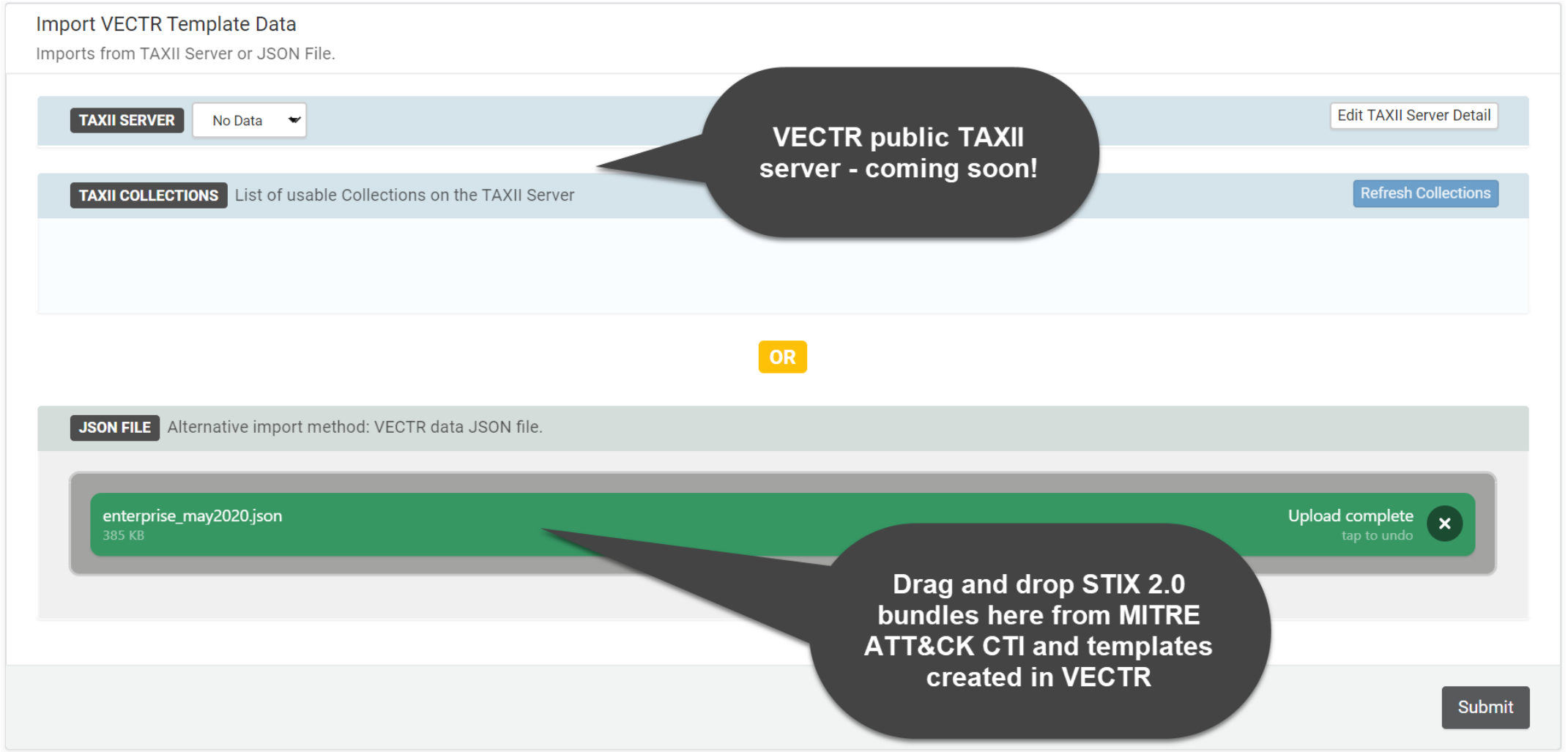
VECTR Concepts



Data Hierarchy

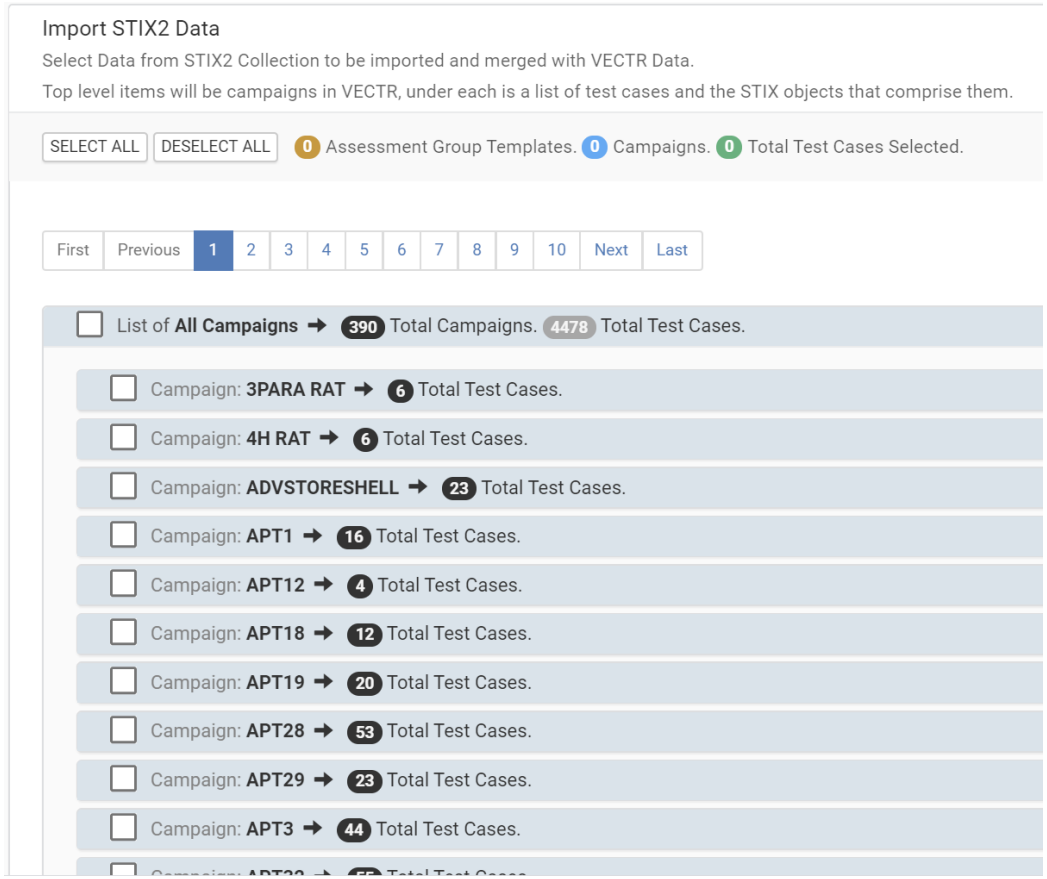


Importing Assessment Templates

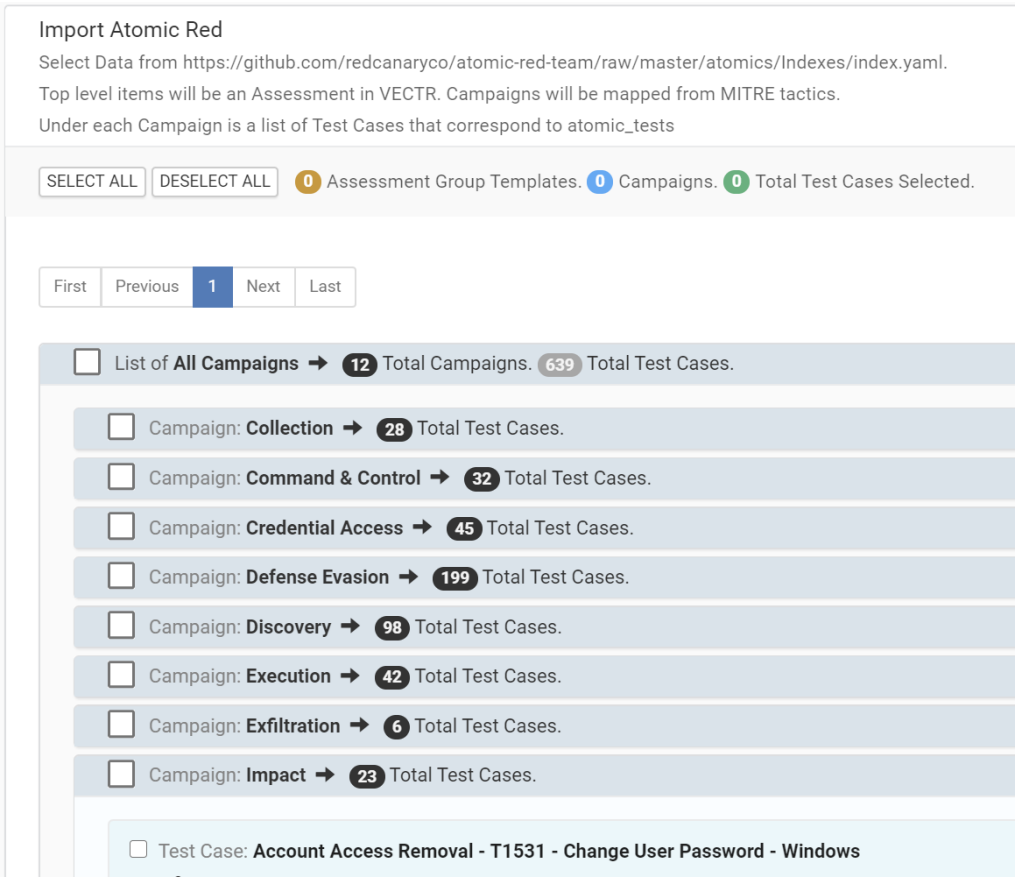


Importing Content from Third-party Sources

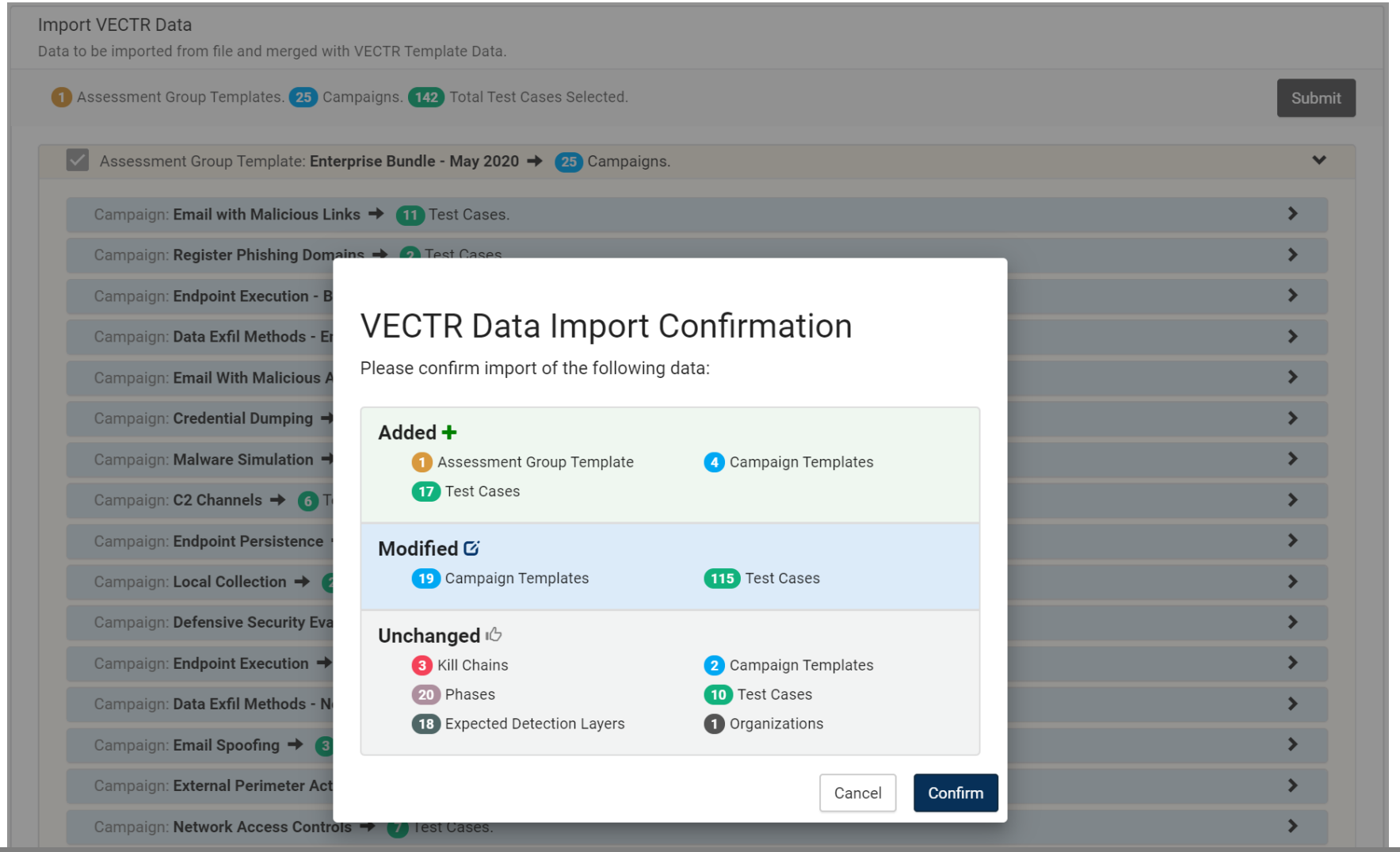
Import latest MITRE ATT&CK enterprise bundle



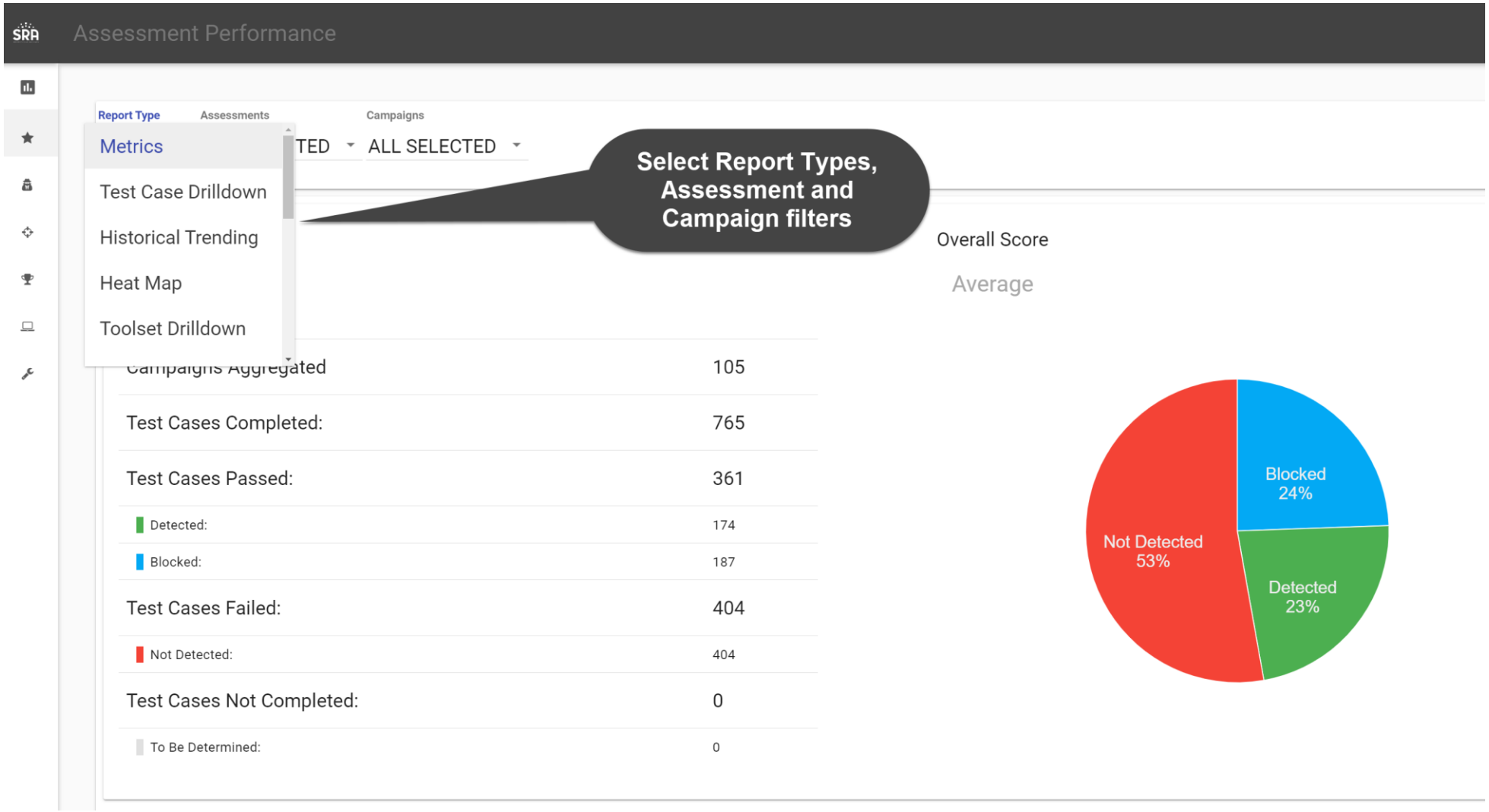
Import latest Red Canary Atomic Red index



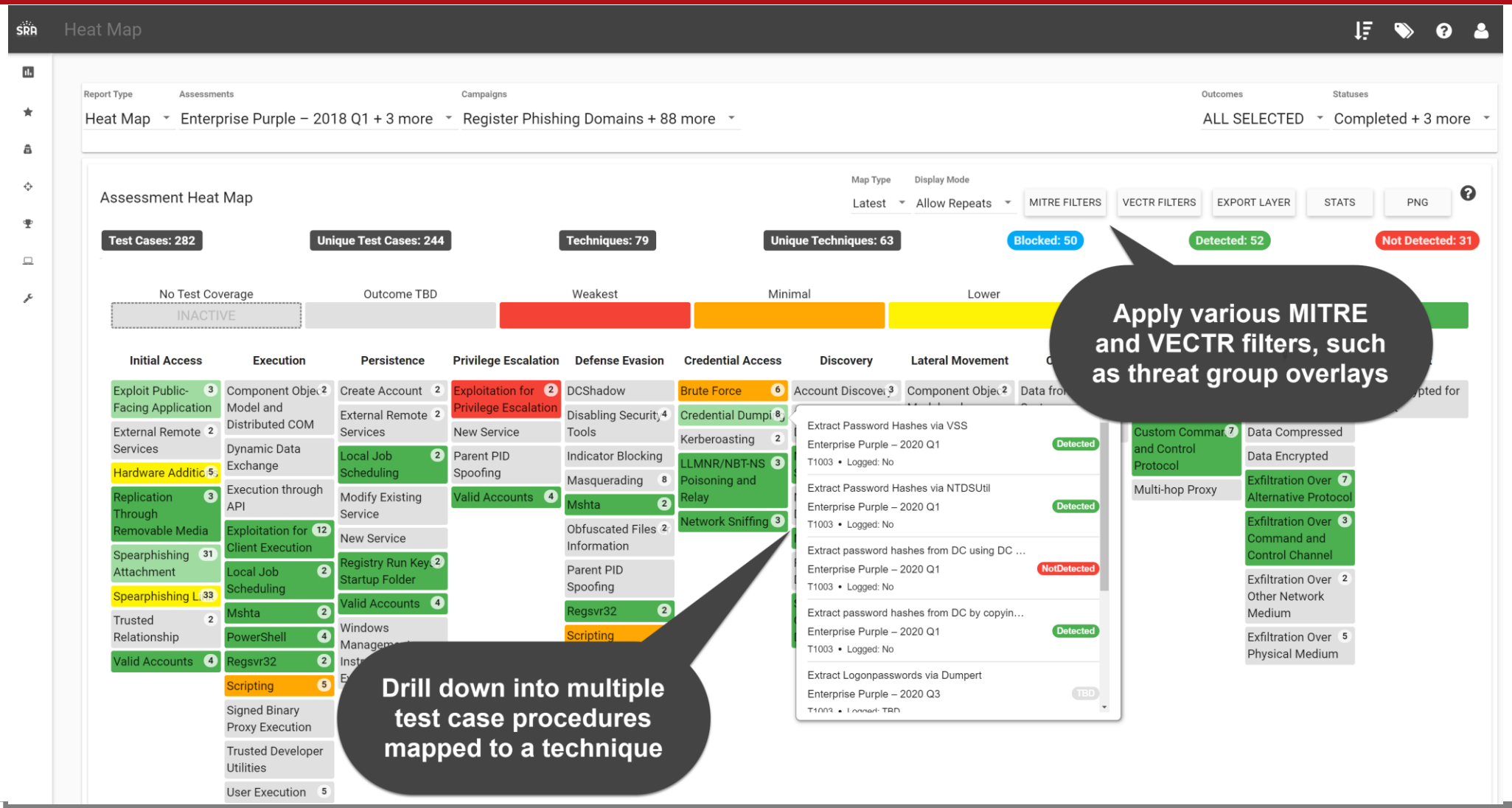
Importing Custom Assessments (VECTR-to-VECTR sharing)



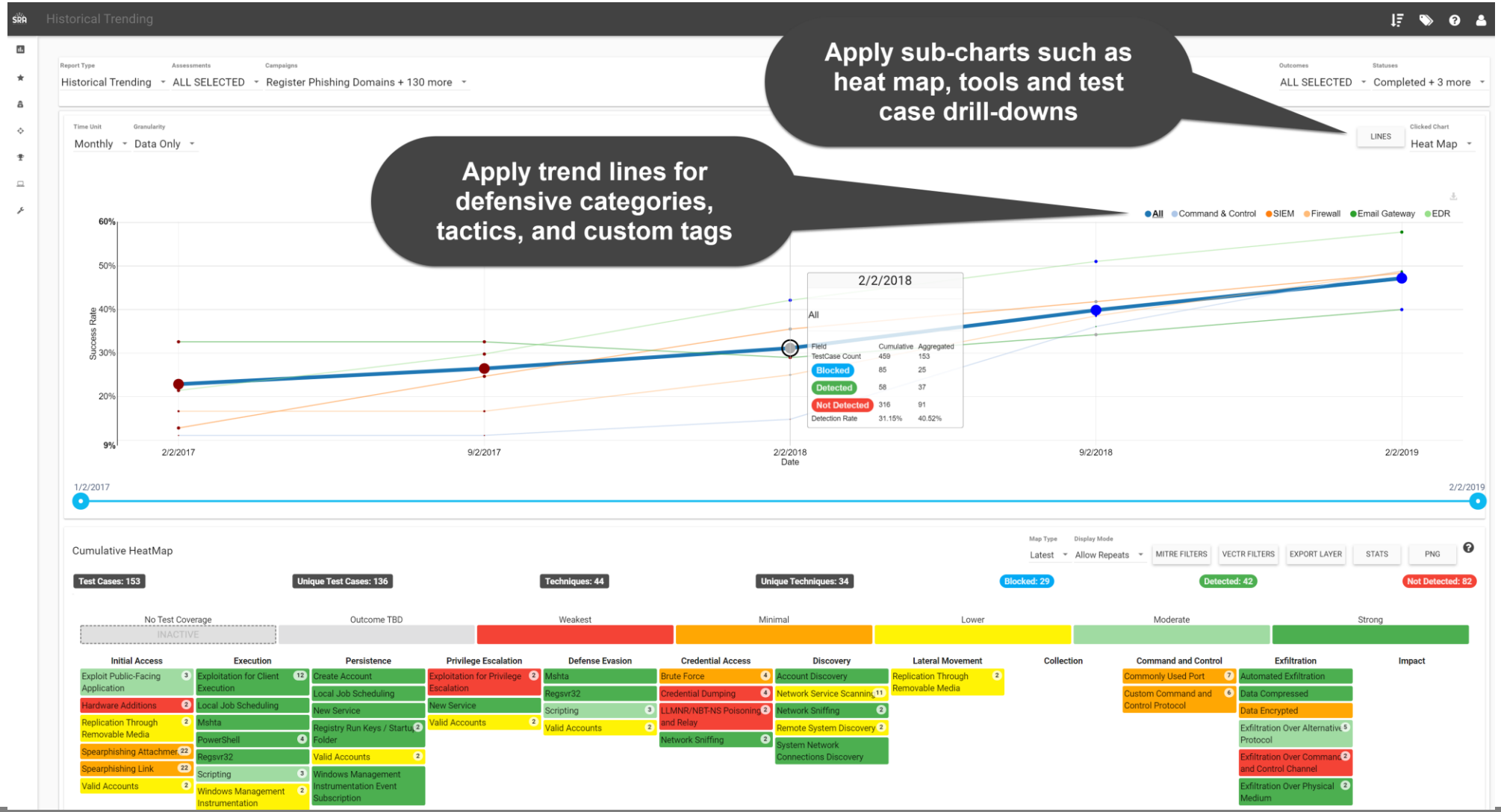
Reporting Dashboard



Dynamic Heat Map

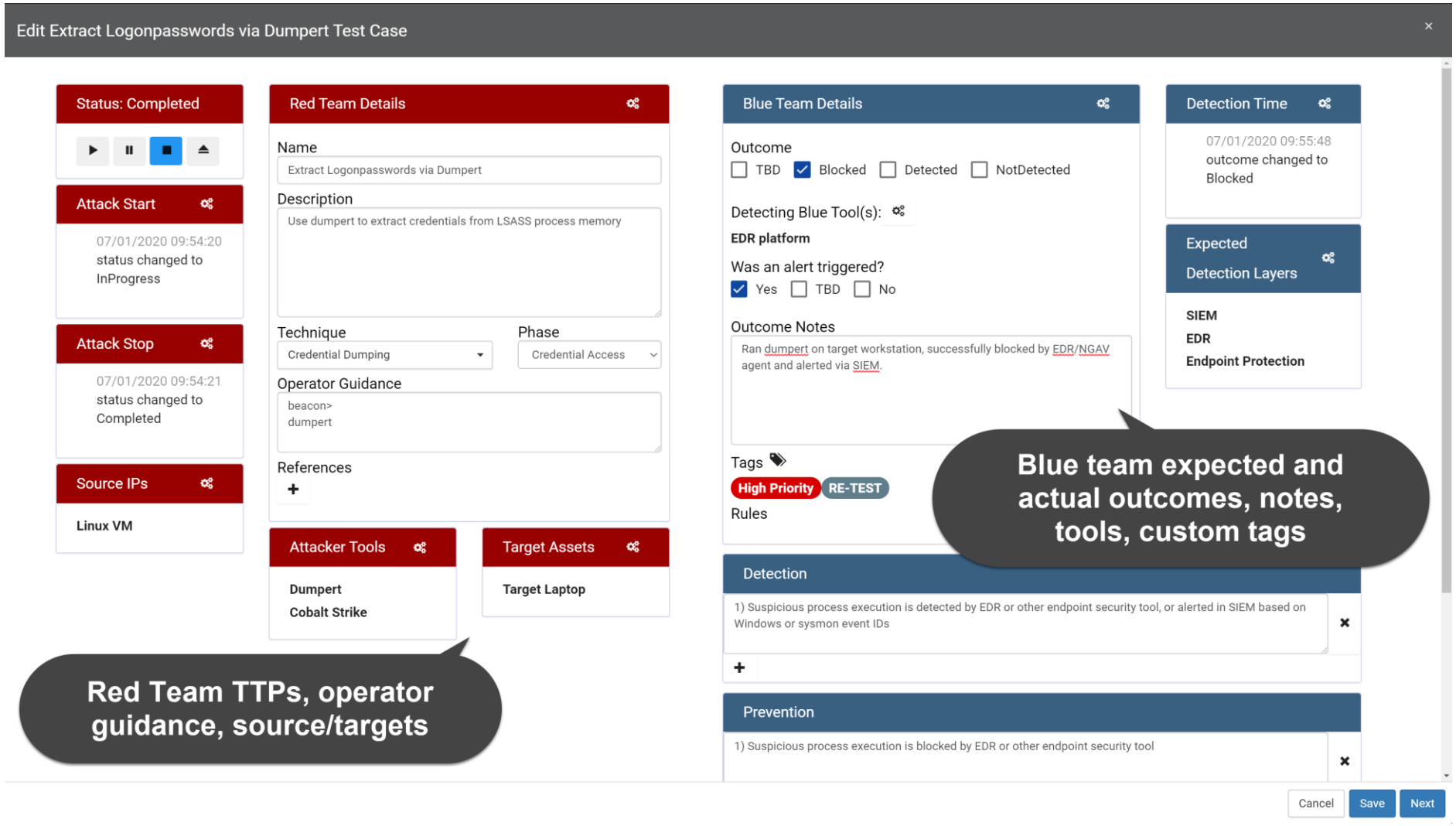


Historical Trending with sub-charts



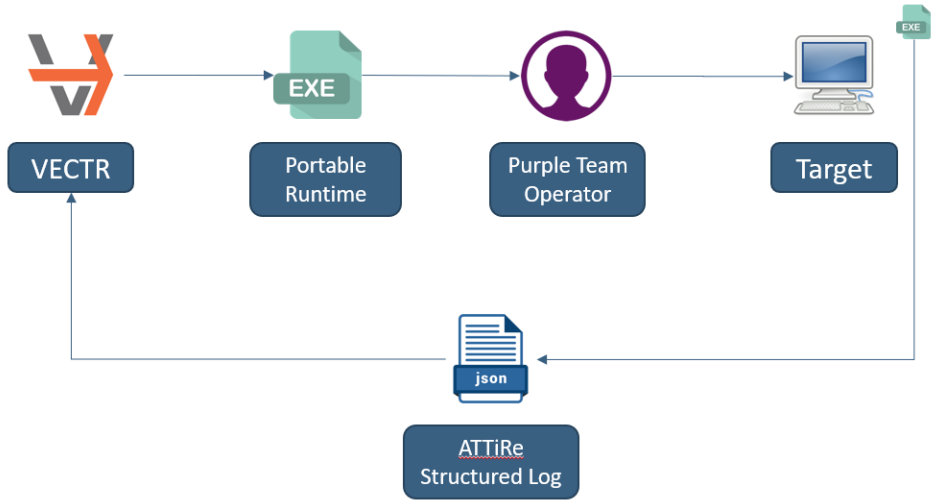
Campaign Dashboard

Test Case Panel



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 SCYTHE
- 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?