

PUBLIC



**SEPTEMBER 2020**

Sajid Nawaz Khan

# **Adversarial Threat Modelling: A Practical Approach to Purple Teaming in the Enterprise**

Presented at X33FCON

# HELLO

WELCOME TO THE WORKSHOP



Thank you for joining my workshop today, it's a pleasure to be presenting at X33FCON.

## *whoami*

- Sajid Nawaz Khan
- In finance sector 15+ years
- Senior Cyber Threat Intelligence Analyst, five years in security
- GIAC GREM, GDAT certified
- Mitre ATT&CK evangelist

## */etc*

Food, films, museums, science, origami and more.

# WORKSHOP AGENDA

OUR PLAN TODAY

1

## Presentation · 45 MINS

The problem, and our approach to intelligence-led Purple Teaming

2

## Demo · 15 MINS

A practical demonstration of Vectr; for analysts *and* managers

3

## Workshop · 2 HOURS

Hands-on session installing and configuring Vectr for Enterprise use

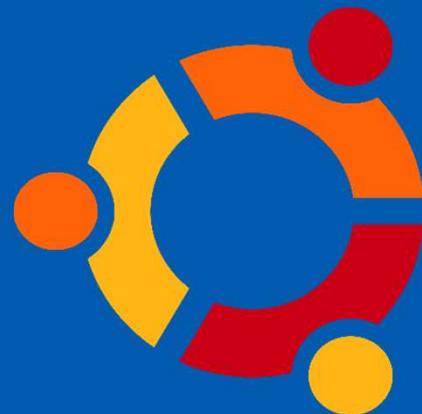


# REQUIREMENTS

PREPARING FOR SUCCESS



**VirtualBox** or equivalent, with Extension Pack, Guest Additions and fast internet connectivity



**Ubuntu 20.04.1 LTS**, with 4GB RAM, 20GB disk space and bi-directional clipboard and file sharing



**Vectr**, please follow the installation guide including dependencies at [docs.vectr.io](https://docs.vectr.io)

# IT'S BEEN A BUSY YEAR

LITTLE REST FOR DEFENDERS

## January

A suspected nation state targeted the Austrian foreign ministry as part of a cyber attack lasting several weeks

A Russian hacking group infiltrated a Ukrainian energy company

The FBI announced that nation state hackers had breached the networks of two U.S. municipalities

Mitsubishi announces that a suspected Chinese group had targeted the company as part of a massive cyberattack that compromised personal data of 8,000 individuals

Turkish government hackers targeted at least 30 organisations across Europe and the Middle East, including government ministries, embassies, security services, and companies

The UN was revealed to have covered up a hack into its IT systems in Europe conducted by an unknown but sophisticated hacking group

An Iranian hacking group launched an attack on the U.S. based research company

Iran announced that it has defended against a DDoS against its communications infrastructure that caused internet outages across the country

## February

Chinese hackers targeted Malaysian government officials to steal data related to government-backed projects in the region

A hacking group of unknown origin was found to be targeting government and diplomatic targets across Southeast Asia as part of a phishing campaign utilizing custom malware

The U.S. Defence Information Systems Agency announced it had suffered a data breach

Mexico's economy ministry announced it had detected a cyber attack launched against the ministry's networks

Source



Center for Strategic & International Studies (CSIS)

[www.csis.org/programs/technology-policy-program/significant-cyber-incidents](http://www.csis.org/programs/technology-policy-program/significant-cyber-incidents)

# IT'S BEEN A BUSY YEAR

LITTLE REST FOR DEFENDERS

SOURCE: CSIS

## March

Human rights activists and journalists in Uzbekistan were targeted by suspected state security hackers in a spear-phishing campaign intended to install spyware on their devices

A suspected nation state hacking group was discovered to be targeting industrial sector companies in Iran

Chinese hackers targeted over 75 organisations around the world in the manufacturing, media, healthcare, and non-profit sectors as part of a broad-ranging cyber espionage campaign

Saudi mobile operators exploited a flaw in global telecommunications infrastructure to track the location of Saudis traveling abroad

## April

Suspected state-sponsored hackers targeted Chinese government agencies and Chinese diplomatic missions abroad by exploiting a zero-day vulnerability in virtual private networks servers

Government and energy sector entities in Azerbaijan were targeted by an unknown group focused on the SCADA systems of wind turbines

Suspected Iranian hackers unsuccessfully targeted the command and control systems of water treatment plants, pumping stations, and sewage in Israel

Poland suggested the Russian government was behind a series of cyber attacks on Poland's War Studies University

## May

Operations at two Taiwanese petrochemical companies were disrupted by malware attacks

A suspected PLA hacking group targeted government-owned companies, foreign affairs ministries, & science and technology ministries across Australia, Indonesia, the Philippines, Vietnam, Thailand, Myanmar, and Brunei

Japan's Defence Ministry investigated a large-scale cyber attack against Mitsubishi Electric that could have compromised details of new state-of-the-art missile designs

Suspected Iranian hackers compromised the IT systems of at least three telecom companies in Pakistan

# IT'S BEEN A BUSY YEAR

LITTLE REST FOR DEFENDERS

SOURCE: CSIS

## June

Suspected North Korean hackers compromised at least two defence firms in Central Europe by sending false job offers to their employees while posing as representatives from major U.S. defence contractors

In the midst of escalating tensions between China and India over a border dispute in the Galwan Valley, Indian government agencies and banks reported being targeted by DDoS attacks reportedly originating in China

North Korean state hackers sent COVID-19-themed phishing emails to more than 5 million businesses and individuals in Singapore, Japan, the United States, South Korea, India, and the UK in an attempt to steal personal and financial data

The most popular of the tax reporting software platforms China requires foreign companies to download to operate in the country was discovered to contain a backdoor that could allow malicious actors to conduct network reconnaissance or attempt to take remote control of company systems

## July

Canada, the UK, and the U.S. announced that hackers associated with Russian intelligence had attempted to steal information related to COVID-19 vaccine development

The UK announced that it believed Russia had attempted to interfere in its 2019 general election by stealing and leaking documents related to the UK-US Free Trade Agreement

## August

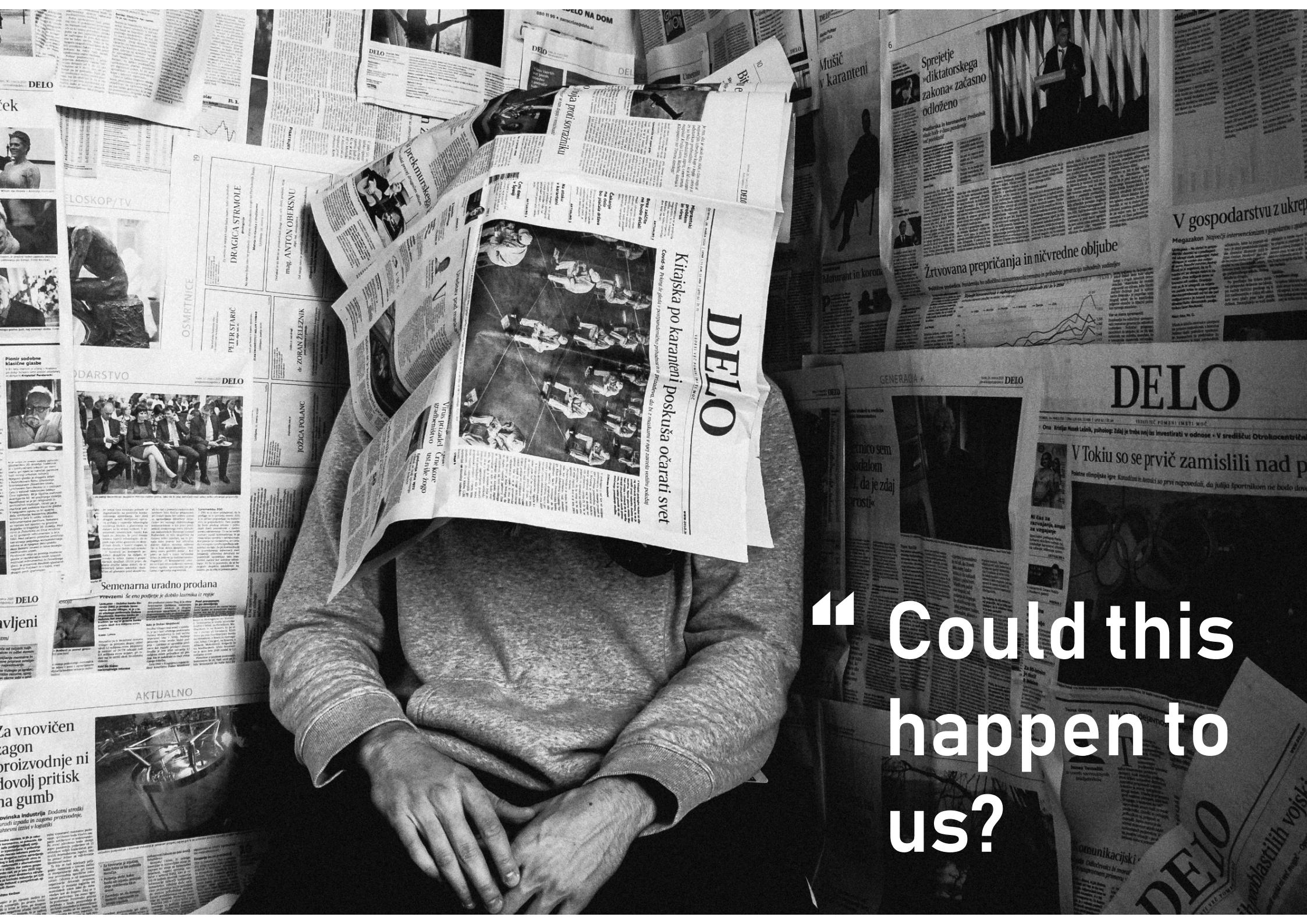
Pakistan announced that hackers associated with Indian intelligence agencies had targeted the mobile phones of Pakistani government officials and military personnel

An Iranian hacking group was found to be targeting major U.S. companies and government agencies by exploiting recently disclosed vulnerabilities in high-end network equipment to create backdoors for other groups to use

A Chinese espionage group targeted military and financial organisations across Eastern Europe

U.S. officials announced that North Korean government hackers had been operating a campaign focused on stealing money from ATMs around the world ...

" Could this  
happen to  
us?



“ Could  
this  
happen  
to us?

BEFORE

- “ ... defence in depth
- ... indicators ingested
- ... industry-leading controls
- ... visibility via peers and industry trust groups
- ... couldn't / wouldn't happen to us

...

“ Could  
this  
happen  
to us?

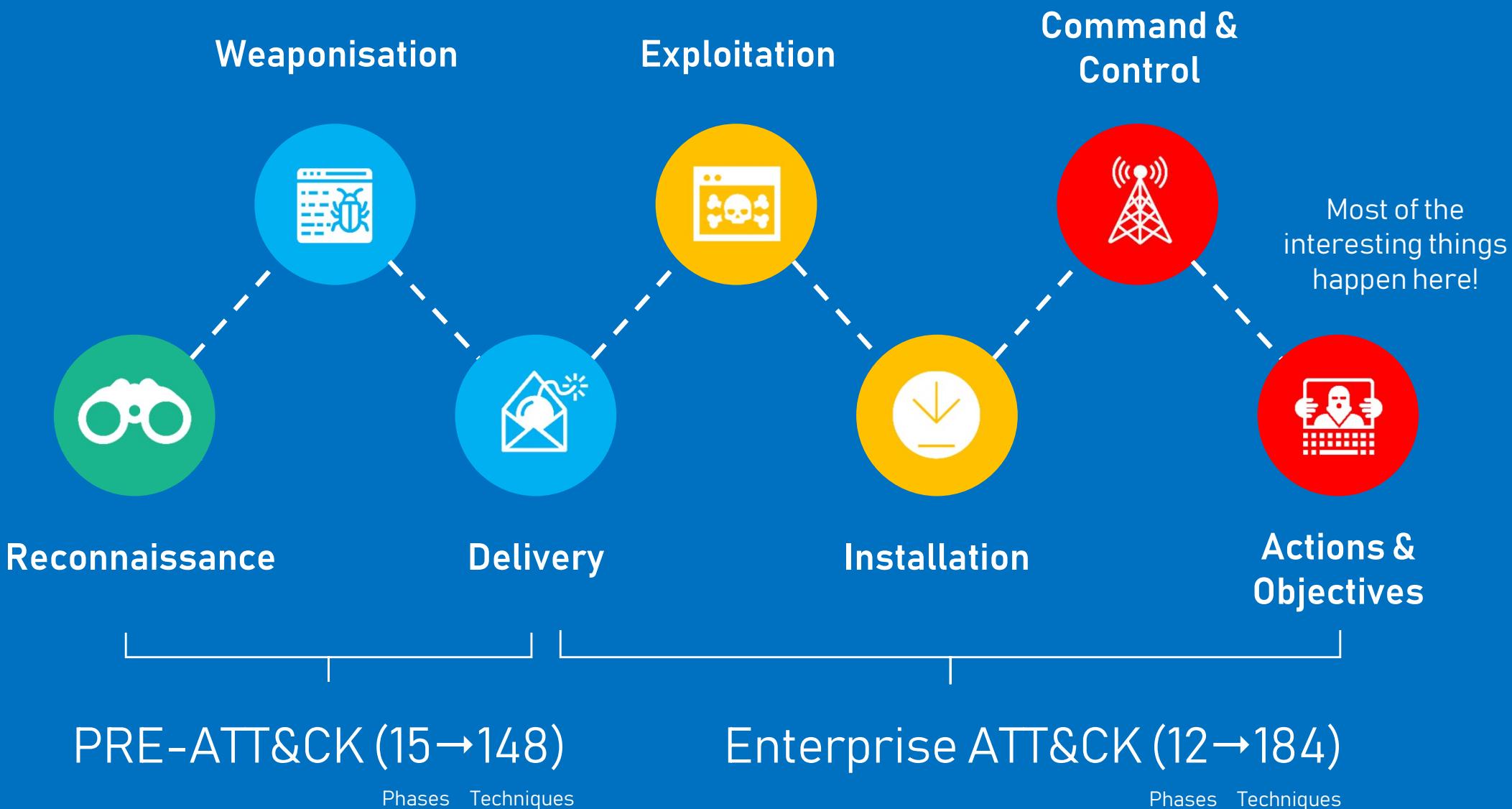
AFTER

■ Threat Intelligence are aware of *7 Tier One actors*, including *Lazarus*, using *Techniques A, B, C* in a number of successful attacks within the sector.

We therefore *strongly recommend* developing and deploying *ControlX* as a priority; to detect and mitigate any impact from this technique.

# HOW DID WE GET HERE?

MOVING BEYOND THE LOCKHEED MARTIN KILL CHAIN



# MITRE NAVIGATOR

VISUALISE THE ADVERSARY

The Mitre Navigator can be used to highlight techniques used by specific adversaries, create heat maps for heavily used techniques, or visualise your defensive coverage

Lazarus x +

selection controls layer controls technique controls

MITRE ATT&CK® Navigator ?

Initial Access	Execution	Persistence	Defense Evasion	Discovery	Collection	Command and Control	Exfiltration	Impact
1 techniques	2 techniques	1 techniques	1 techniques	8 techniques	2 techniques	3 techniques	1 techniques	4 techniques
Drive-by Compromise	Exploitation for Client Execution	Account Manipulation (0/0)	Obfuscated Files or Information (0/0)	Application Window Discovery	Archive Collected Data (0/2)	Fallback Channels	Exfiltration Over C2 Channel	Data Destruction
		Windows Management Instrumentation		File and Directory Discovery	Data from Local System	Ingress Tool Transfer		Resource Hijacking
				Process Discovery		Non-Standard Port		Service Stop
				Query Registry				System Shutdown/Reboot
				System Information Discovery				
				System Network Configuration Discovery				
				System Owner/User Discovery				
				System Time Discovery				

MITRE ATT&CK® Navigator v3.1

# IS MITRE ATT&CK ENOUGH?

MORE DETAIL == BETTER DECISIONS



Techniques & sub-techniques still don't often provide enough detail to replicate an attack †

Mitre knowledgebase is extensive, but only includes public information, which may not reflect reality

Techniques are not always distilled to individual toolkits or intrusions, so harder to identify trends

† GRANULAR PROCEDURE LEVEL INFORMATION IS IN THE MITRE ROADMAP

# PHISHING · T1566

HOW MANY WAYS CAN YOU THINK OF?



Macro  
Cobalt Strike  
Standard



Macro  
Cobalt Strike  
Standard as HREF



Macro  
Cobalt Strike  
as URL Rewrite



Macro  
WScript  
PowerShell



Macro  
Wscript  
leading to EXE



Macro  
WScript  
PowerShell XOR



Macro  
MMG WMI  
PowerShell



Macro LuckyStrike  
PowerShell  
CellEmbed



Macro  
MSBuild



DDE  
PowerShell



Macro  
Remote  
Template



Encrypted  
Archive



Password  
Protected  
Office Doc



Link  
Inside  
PDF



Link  
Inside Office  
Document



File:  
HTA



File:  
EXE



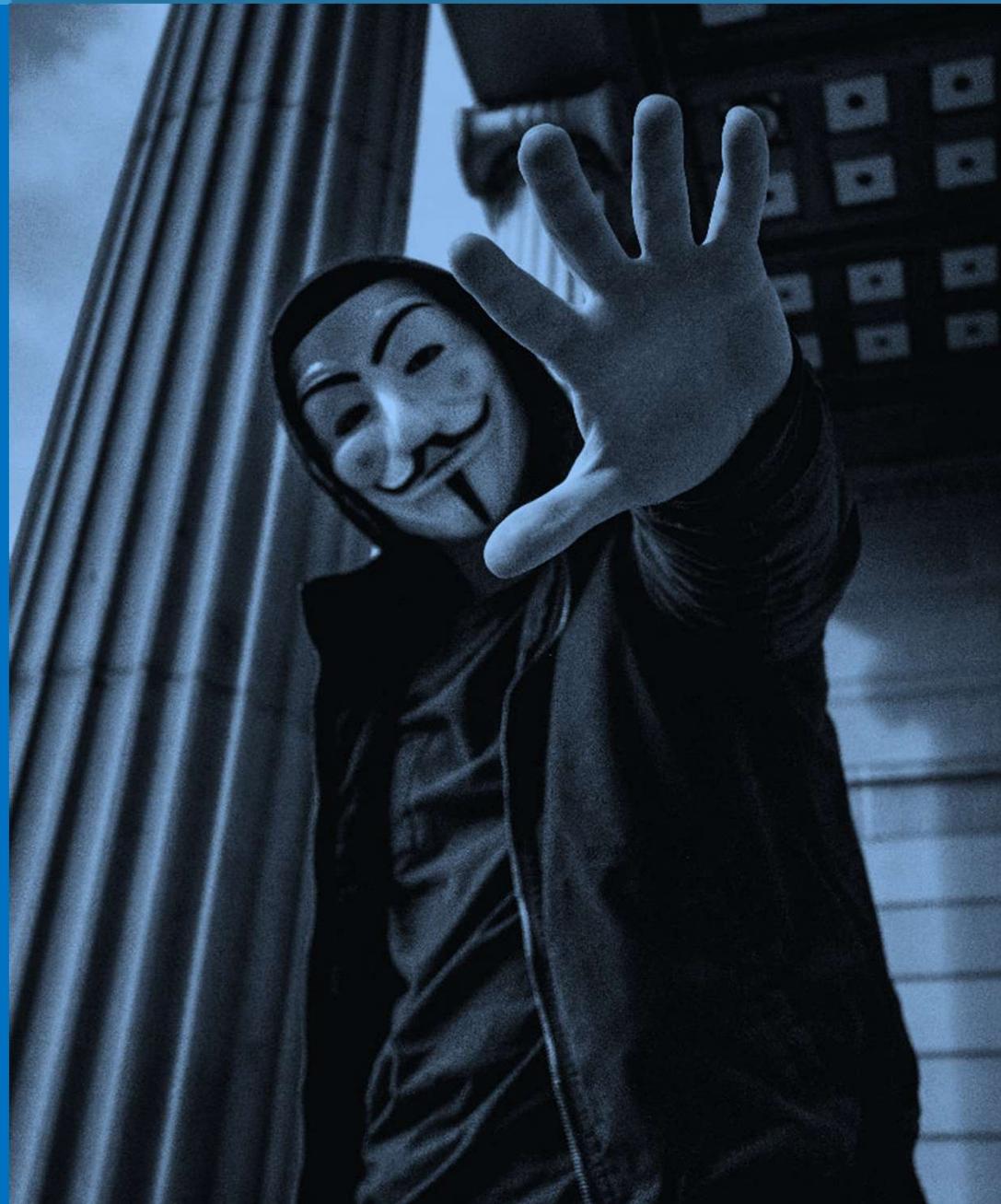
File:  
.BAT

# BECOMING THREAT-LED

AN ADVERSERIAL APPROACH TO PURPLE TEAMING

## What We Wanted to Achieve

- List of threat actors, associated campaigns and TTPs of interest to Standard Chartered and the Financial Services industry
- Granular level understanding of TTPs, and how specifically these can be detected and blocked in our environment
- Remove control-efficacy ambiguity from TTPs, and provide confidence and assurance that controls are effective, through atomic level testing
- A library of TTPs aligned to the Mitre Enterprise framework, which would be actively maintained by Threat Intelligence and security teams

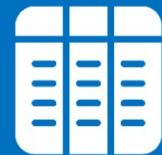


# BECOMING THREAT-LED

INTEGRATING INTELLIGENCE IN YOUR APPROACH

Using Threat Intelligence can bring focus to Purple Team initiatives, helping to prioritise those Threat Actors and TTPs that are likely to be the greatest threat to your organisation and technology stack. Your Cyber Threat Intelligence team will work with internal stakeholders, peers, trust groups and vendors to develop a detailed understanding of the threat landscape. Mitre's *Level 3* approach is detailed below:

## ADVERSARY EMULATION PLAN



**Gather**  
threat intelligence  
based on the  
threats to your  
organisation

**Extract**  
techniques and  
map to your  
preferred  
framework

**Analyse**  
.organise and  
diagram your  
analysis into an  
operational flow

**Develop**  
tools and  
procedures to help  
teams replicate  
the attack

**Emulate**  
the adversary,  
working closely  
with Blue Teams to  
identify gaps

### Essential Reading

[medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3](https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3)  
[medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f](https://medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f)

# OUR APPROACH

TPP CENTRIC, FOCUSING ON SPECIFIC INTRUSIONS

THREAT-LED



## Focus on TPPs

Our focus is on the top two tiers of the Pyramid of Pain



## Threat Actor

Understanding which adversaries are the greatest risk



## Cyber Attack

Prominent cyber attack or tool used by the adversary



## Specific TTP

Specific way a tool was used by the adversary

LAZARUS

BANK OF BANGLADESH

TTP1

FAR EASTERN INTERNATIONAL BANK

TTP 2

TROY OPERATION

TTP 3

DARKSEOUL OPERATION

TTP 4

SONY PICTURES

ETC

Malpedia and the Thai CERT Threat Actor Encyclopedia are a great place to start:

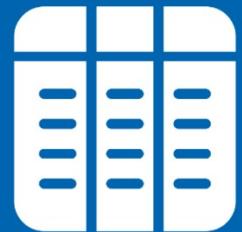
- [malpedia.caad.fkie.fraunhofer.de/actors](http://malpedia.caad.fkie.fraunhofer.de/actors)
- [apt.thaicert.or.th/cgi-bin/listgroups.cgi](http://apt.thaicert.or.th/cgi-bin/listgroups.cgi)

# OUR APPROACH

## OPERATIONALISING THREAT INTELLIGENCE

We wanted to industrialise the end-to-end pipeline between Threat Intelligence, Purple Teams, Detection Engineering, Threat Hunting and finally, Red/Blue teams for validation

### Threat Intelligence



**Research**  
Understanding the Threat Landscape and attacks to the Finance sector

### Purple Team, Detection Engineering



**Assess**  
Identifying how these TTPs might be detected via current controls

### Red & Blue Teams



**Enhance**  
Improving and prioritising detection capabilities

**Validate**  
Testing efficacy of controls and TTP detection via Red Teaming



# OUR REQUIREMENTS

## WHAT WE WANTED FROM A PLATFORM

To help fulfil our organisations' requirement to be threat-intelligence led, we wanted a platform that could help orchestrate teams across the security function. We needed:

### Flexibility

- Framework / Kill Chain agnostic
- Could meet our current and future requirements

### Standards Compliance

- STIX/TAXII compliant
- Easy to export data to re-use elsewhere

### Detail Orientated

- Ability to capture rich detail, both from a Red and Blue team perspective

### Encouraged Collaboration

- Encourage intra-business collaboration
- But also support sharing with peers and trust groups

### Single Tool Across Security

- A tool for analysts *as well as* management
- One tool, with multiple use cases (not just for CTI)





### Alert

The file format and extension of 'tables.xls' don't match. The file could be corrupted or unsafe. Unless you trust its source, don't open it. Do you want to open it anyway?

Yes

No

# TOOL REVIEWS

WHY WE PICKED VECTR

	Benefits	Considerations
<b>Excel</b> <i>Unsuitable</i>	<ul style="list-style-type: none"> <li>▪ No additional licensing required</li> <li>▪ Can theoretically be built and customised to your specific use case</li> </ul>	<ul style="list-style-type: none"> <li>▪ Not optimised for multiple users</li> <li>▪ Significant development time</li> <li>▪ Excel not optimised for this task</li> </ul>
<b>Custom Tooling</b> <i>Unsuitable</i>	<ul style="list-style-type: none"> <li>▪ Can be customised to meet all your development and productivity needs</li> <li>▪ Would be fully compliant with all your business / security requirements</li> </ul>	<ul style="list-style-type: none"> <li>▪ Cost / time for development</li> <li>▪ Would require ongoing development, to maintain alignment with changes to the Mitre framework</li> </ul>
<b>Unfetter</b> <i>Unsuitable</i>	<ul style="list-style-type: none"> <li>▪ Free for all uses, including Enterprise</li> <li>▪ Tool developed by the NSA, aiming to provide actor-centric security reviews</li> <li>▪ STIX compliant</li> </ul>	<ul style="list-style-type: none"> <li>▪ Development ceased in 2018, and so Mitre alignment off-kilter</li> <li>▪ Tool unstable and not very performant</li> <li>▪ Tool not as extensive as Vectr</li> </ul>
<b>Vectr</b> <i>Ideal</i>	<ul style="list-style-type: none"> <li>▪ Free for all uses, including Enterprise</li> <li>▪ Kill Chain / framework agnostic, but fully supports Mitre Enterprise</li> <li>▪ Actively maintained</li> <li>▪ STIX/TAXII compliant</li> <li>▪ Potential to automate testing in future</li> <li>▪ Facilitates collaboration between teams</li> </ul>	<ul style="list-style-type: none"> <li>▪ Not designed initially to be intel-led</li> <li>▪ Tool development driven by tool developers, with reduced influence to prioritise Enterprise features (but developers very receptive to feedback)</li> <li>▪ Self-hosted, technology stack may not be compatible with internal standards</li> </ul>

# VECTR

## CAMPAIGN AND ASSESSMENT TRACKER

**VECTR** is a platform designed to facilitate security teams through comprehensive threat simulation assessments. Attacks can be documented to gauge the effectiveness of defensive tools to help strengthen an organisations' security posture, and improve detection capabilities through historical performance tracking. Common campaigns and use cases include:

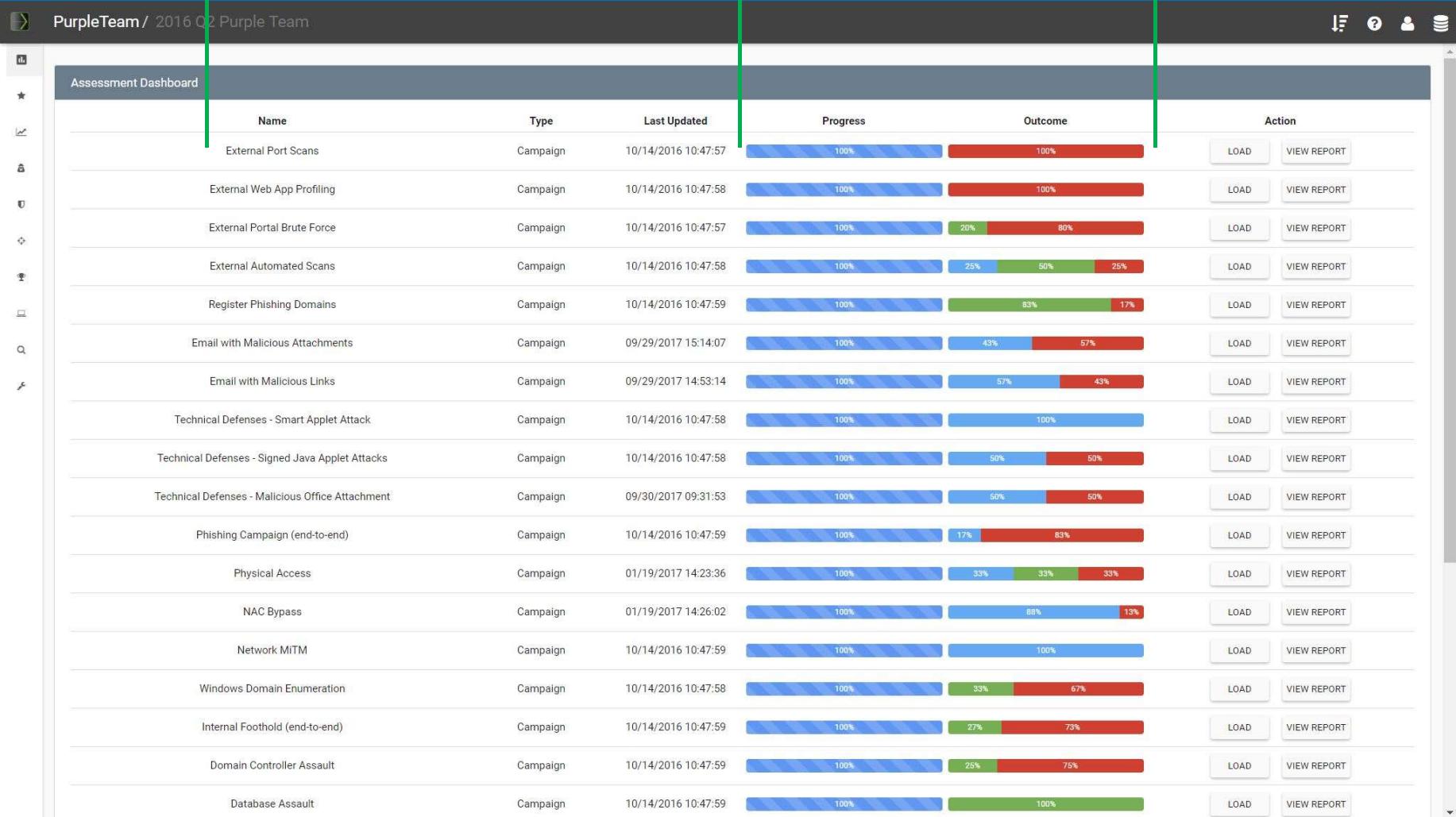
- Account abuse
- Spear phishing technical defences
- Malware detection and response
- Lateral movement and protected resources breach
- C2 and data exfiltration

- Ability to map prior attack methodologies in a consistent manner
- Measure progress across phases, campaign assessments, and outcomes
- Centralises Red Team and Blue Team techniques, allowing for control recommendations/tuning
- Ability to add custom test cases and target assets
- Produce summary and detailed reporting for campaign outcomes
- Provide historical trending of campaign exercises
- Rich management information; one tool for analysts and leaders

Each known cyber attack or attack type is loaded as a campaign

As TTPs are mapped and tested, the progress is updated

As a capability assessment is completed, the Outcome is updated



The screenshot shows the VECTR Assessment Dashboard for the PurpleTeam / 2016 Q2 Purple Team. The dashboard lists 17 different campaigns, each with a name, type (Campaign), last updated date, progress bar, outcome bar, and two action buttons: LOAD and VIEW REPORT.

Name	Type	Last Updated	Progress	Outcome	Action
External Port Scans	Campaign	10/14/2016 10:47:57	<div style="width: 100%;">100%</div>	<div style="width: 100%;">100%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
External Web App Profiling	Campaign	10/14/2016 10:47:58	<div style="width: 100%;">100%</div>	<div style="width: 100%;">100%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
External Portal Brute Force	Campaign	10/14/2016 10:47:57	<div style="width: 100%;">100%</div>	<div style="width: 20%;">20%</div> <div style="width: 80%;">80%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
External Automated Scans	Campaign	10/14/2016 10:47:58	<div style="width: 100%;">100%</div>	<div style="width: 25%;">25%</div> <div style="width: 50%;">50%</div> <div style="width: 25%;">25%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
Register Phishing Domains	Campaign	10/14/2016 10:47:59	<div style="width: 100%;">100%</div>	<div style="width: 83%;">83%</div> <div style="width: 17%;">17%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
Email with Malicious Attachments	Campaign	09/29/2017 15:14:07	<div style="width: 100%;">100%</div>	<div style="width: 43%;">43%</div> <div style="width: 57%;">57%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
Email with Malicious Links	Campaign	09/29/2017 14:53:14	<div style="width: 100%;">100%</div>	<div style="width: 57%;">57%</div> <div style="width: 43%;">43%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
Technical Defenses - Smart Applet Attack	Campaign	10/14/2016 10:47:58	<div style="width: 100%;">100%</div>	<div style="width: 100%;">100%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
Technical Defenses - Signed Java Applet Attacks	Campaign	10/14/2016 10:47:58	<div style="width: 100%;">100%</div>	<div style="width: 50%;">50%</div> <div style="width: 50%;">50%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
Technical Defenses - Malicious Office Attachment	Campaign	09/30/2017 09:31:53	<div style="width: 100%;">100%</div>	<div style="width: 50%;">50%</div> <div style="width: 50%;">50%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
Phishing Campaign (end-to-end)	Campaign	10/14/2016 10:47:59	<div style="width: 100%;">100%</div>	<div style="width: 17%;">17%</div> <div style="width: 83%;">83%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
Physical Access	Campaign	01/19/2017 14:23:36	<div style="width: 100%;">100%</div>	<div style="width: 33%;">33%</div> <div style="width: 33%;">33%</div> <div style="width: 33%;">33%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
NAC Bypass	Campaign	01/19/2017 14:26:02	<div style="width: 100%;">100%</div>	<div style="width: 88%;">88%</div> <div style="width: 12%;">12%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
Network MITM	Campaign	10/14/2016 10:47:59	<div style="width: 100%;">100%</div>	<div style="width: 100%;">100%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
Windows Domain Enumeration	Campaign	10/14/2016 10:47:58	<div style="width: 100%;">100%</div>	<div style="width: 33%;">33%</div> <div style="width: 67%;">67%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
Internal Foothold (end-to-end)	Campaign	10/14/2016 10:47:59	<div style="width: 100%;">100%</div>	<div style="width: 27%;">27%</div> <div style="width: 73%;">73%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
Domain Controller Assault	Campaign	10/14/2016 10:47:59	<div style="width: 100%;">100%</div>	<div style="width: 25%;">25%</div> <div style="width: 75%;">75%</div>	<button>LOAD</button> <button>VIEW REPORT</button>
Database Assault	Campaign	10/14/2016 10:47:59	<div style="width: 100%;">100%</div>	<div style="width: 100%;">100%</div>	<button>LOAD</button> <button>VIEW REPORT</button>

Swim lanes show an end-to-end view of an attack

Test Cases are specific implementations of a technique

Timeline and Outcome show the result of validation tests

SANS\_DEMO / Adversary Emulation 2020 / APT19

**APT19: Escalation Path**

**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

**Test Cases**

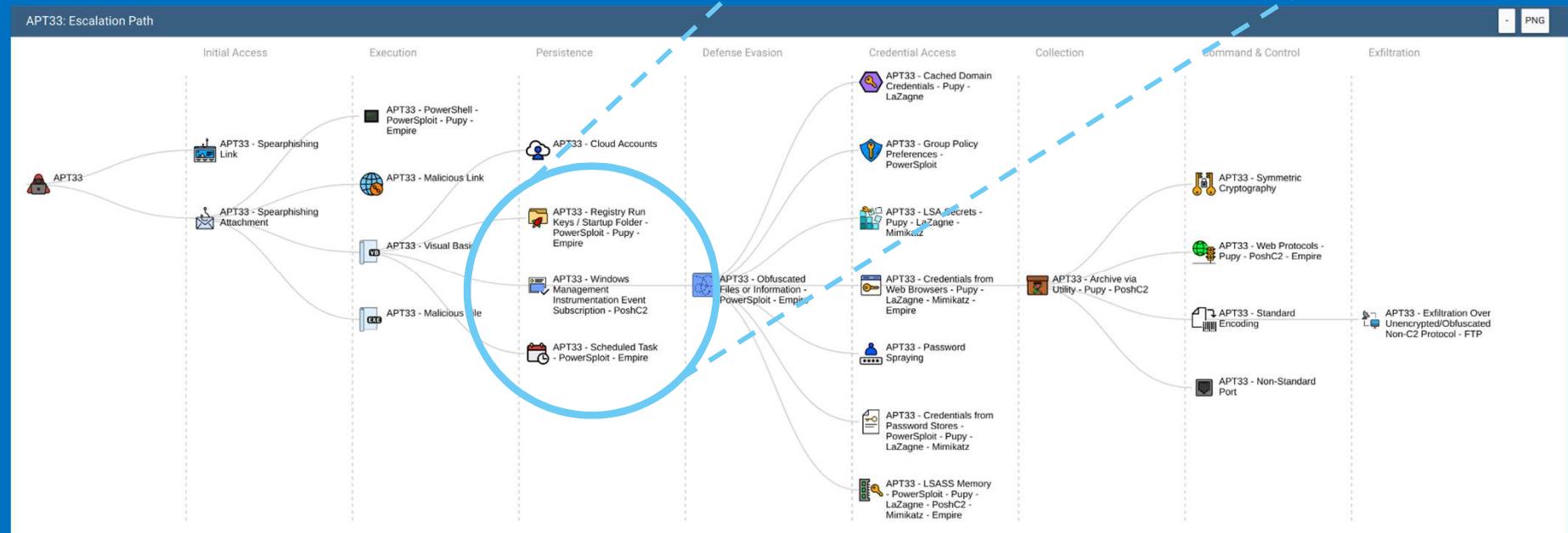
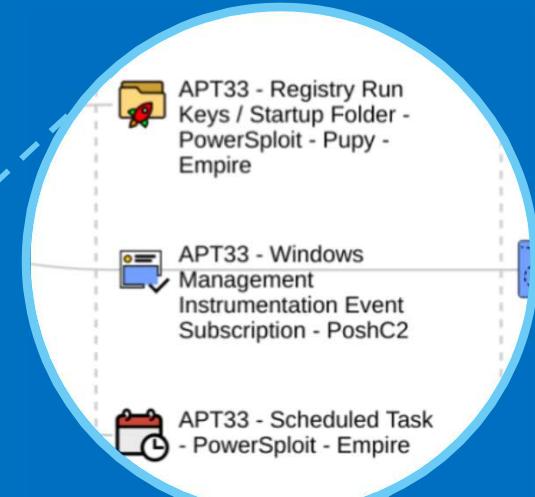
Phase	Technique	Test Case	Status	Outcome	Tags	Action
All	System Information Discovery	APT19 - System Information Discovery - Empire	Completed	Not Detected	High Priority	
Persistence	Registry Run Keys / Startup Folder	APT19 - Registry Run Keys / Startup Folder - Empire	Completed	Blocked		
Defense Evasion	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		

# VECTR

## ESCALATION PATH

A collection of Test Cases (TTPs) are used to illustrate an “Escalation Path”; which demonstrates the attacker’s movement across your preferred Kill Chain.

This is a simple, yet powerful way of summarising the adversary’s behaviour.



Red Team view shows specific offensive technique being tested

### Edit Extract Logonpasswords via Dumper 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 Dumper

**Description**: Use dumper to extract credentials from LSASS process memory

**Technique**: Credential Dumping    **Phase**: Credential Access

**Operator Guidance**: beacon>  
dumper

**References**: +

**Attacker Tools**: Dumper, Cobalt Strike

**Target Assets**: Target Laptop

Blue Team view shows specific defensive technique deployed

**Blue Team Details**

**Outcome**:  TBD  Blocked  Detected  NotDetected

**Detecting Blue Tool(s)**: ⚙️

**EDR platform**

Was an alert triggered?  
 Yes  TBD  No

**Outcome Notes**: Ran dumper 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 VIEW

ON THE OFFENSIVE

SAMPLE DATA

The screenshot displays the Red Team View application interface. On the left, a vertical timeline shows four main events:

- Status: Completed**: Includes icons for play, pause, stop, and up.
- Attack Start**: Occurred at 07/01/2020 09:54:20, status changed to InProgress.
- Attack Stop**: Occurred at 07/01/2020 09:54:21, status changed to Completed.
- Source IPs**: Associated with a Linux VM.

The central part of the interface is a detailed view of the second event (Attack Start). It includes the following fields:

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	+ [Add Reference]

Below this are two smaller sections: **Attacker Tools** (Dumpert, Cobalt Strike) and **Target Assets** (Target Laptop).

- TTP intent and description
- Map to Mitre (or your preferred framework or Kill Chain)
- Capture rich metadata
- Set TTP icon
- Add references
- Map to existing offensive toolkits
- Specify target/scope
- And more!

TIP

Consider adopting the Atomic Red Team YAML specification

# BLUE TEAM VIEW

CAPTURE THE DEFENCE

SAMPLE DATA

- Capture high level (vendor-agnostic) control
- TTP outcome
- Specific control responsible for detection or mitigation
- Add notes for defensive teams, including detection / prevention notes and corresponding evidence
- Map TTP directly to rules
- Tags to assist with work-flow
- And more!

**TIP**

Consider adopting the SIGMA specification

The screenshot displays the Blue Team View interface with a detailed incident report. The main panel shows 'Blue Team Details' with the following information:

- Outcome:** Blocked (checked), TBD, Detected, NotDetected.
- Detecting Blue Tool(s):** EDR platform.
- Was an alert triggered?** Yes (checked).
- Outcome Notes:** Ran dumpert on target workstation, successfully blocked by EDR/NGAV agent and alerted via SIEM.
- Tags:** High Priority, RE-TEST.
- Rules:** A section for listing detection rules.

On the right side, there are two vertical panels:

- Detection Time:** 07/01/2020 09:55:48, outcome changed to Blocked.
- Expected Detection Layers:** SIEM, EDR, Endpoint Protection.

At the bottom, a 'Detection' section lists rule 1: Suspicious process execution detected by EDR or other endpoint security tool, or alerted in SIEM based on Windows or sysmon event IDs.

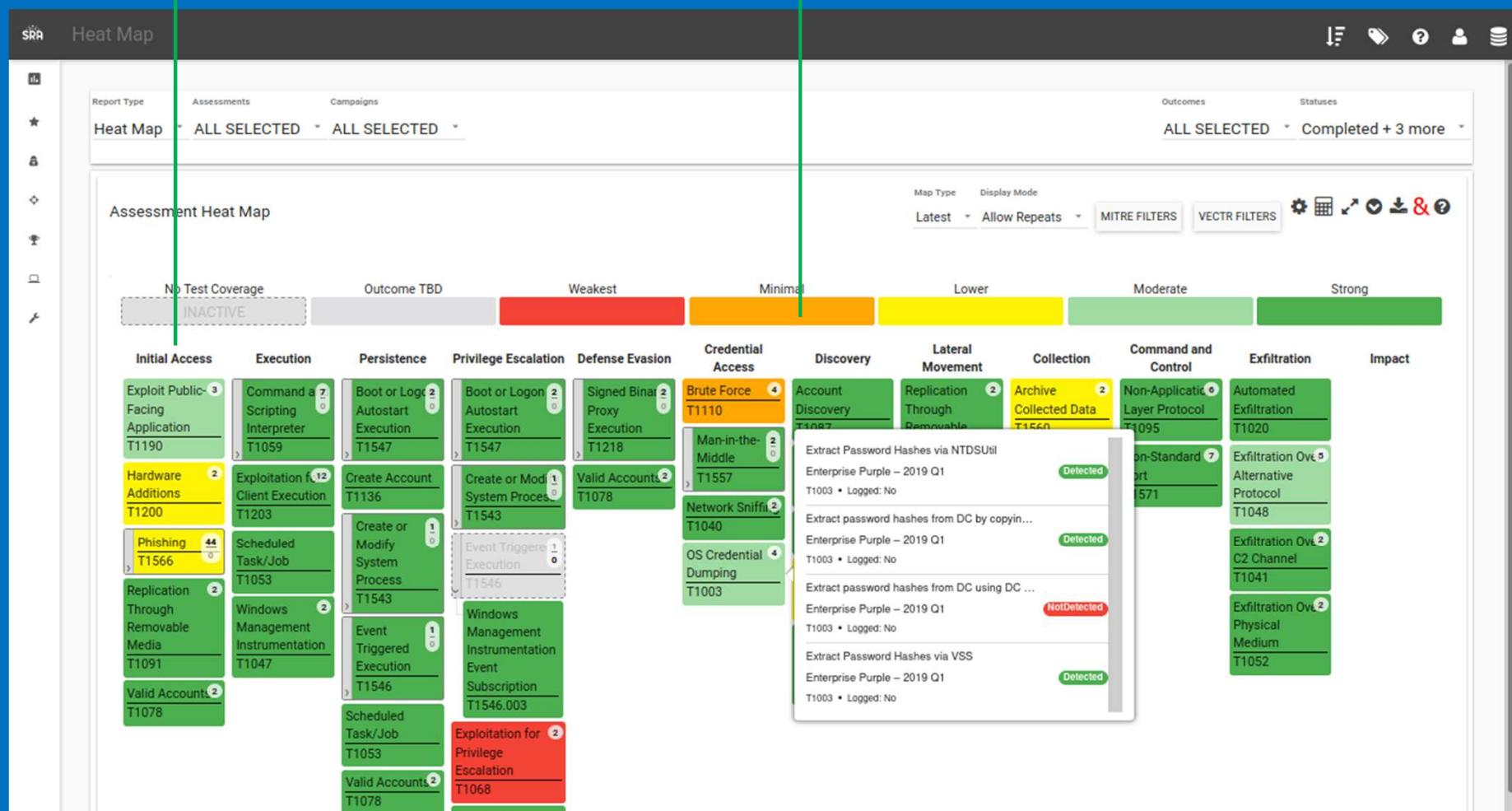
# HEAT MAP

## CONTROL EFFICACY HEATMAP VIEW

SAMPLE DATA

Heatmap view shows concentration of attacker TTPs grouped by tactic

Heatmap shows where controls are strongest, and opportunities for improvement



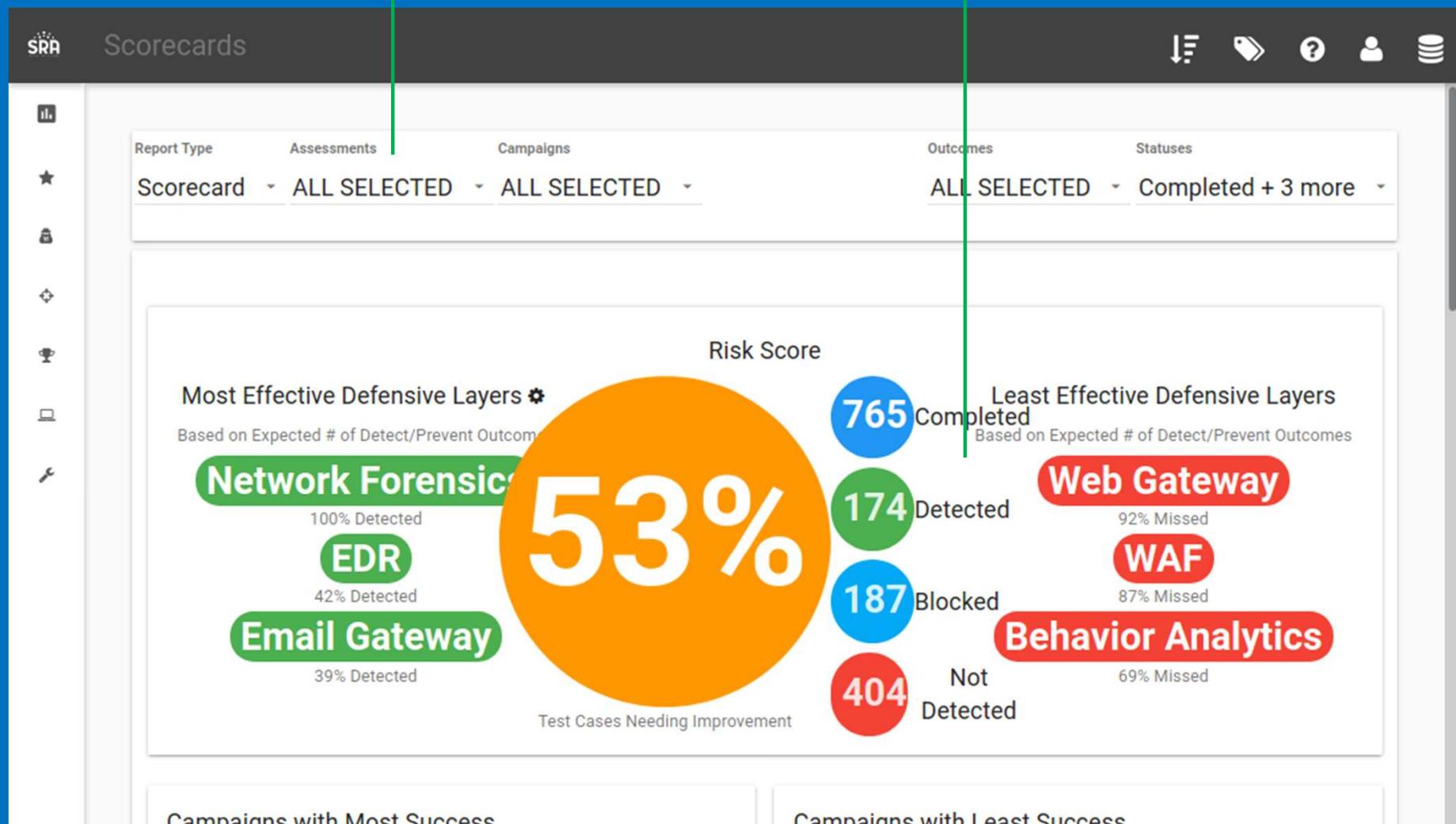
# MANAGEMENT INFORMATION

SAMPLE DATA

## CAMPAIGN ASSESSMENT DASHBOARD

Get a holistic view  
across all your tests, or  
specific campaigns

Campaign summary  
shows what you're good  
at, and what requires  
further development



# TOOLSET SUMMARY

## CONTROL EFFICACY REPORTING

SAMPLE DATA

Quickly see which specific controls are effective

Also see high-level, vendor-agnostic views of control posture



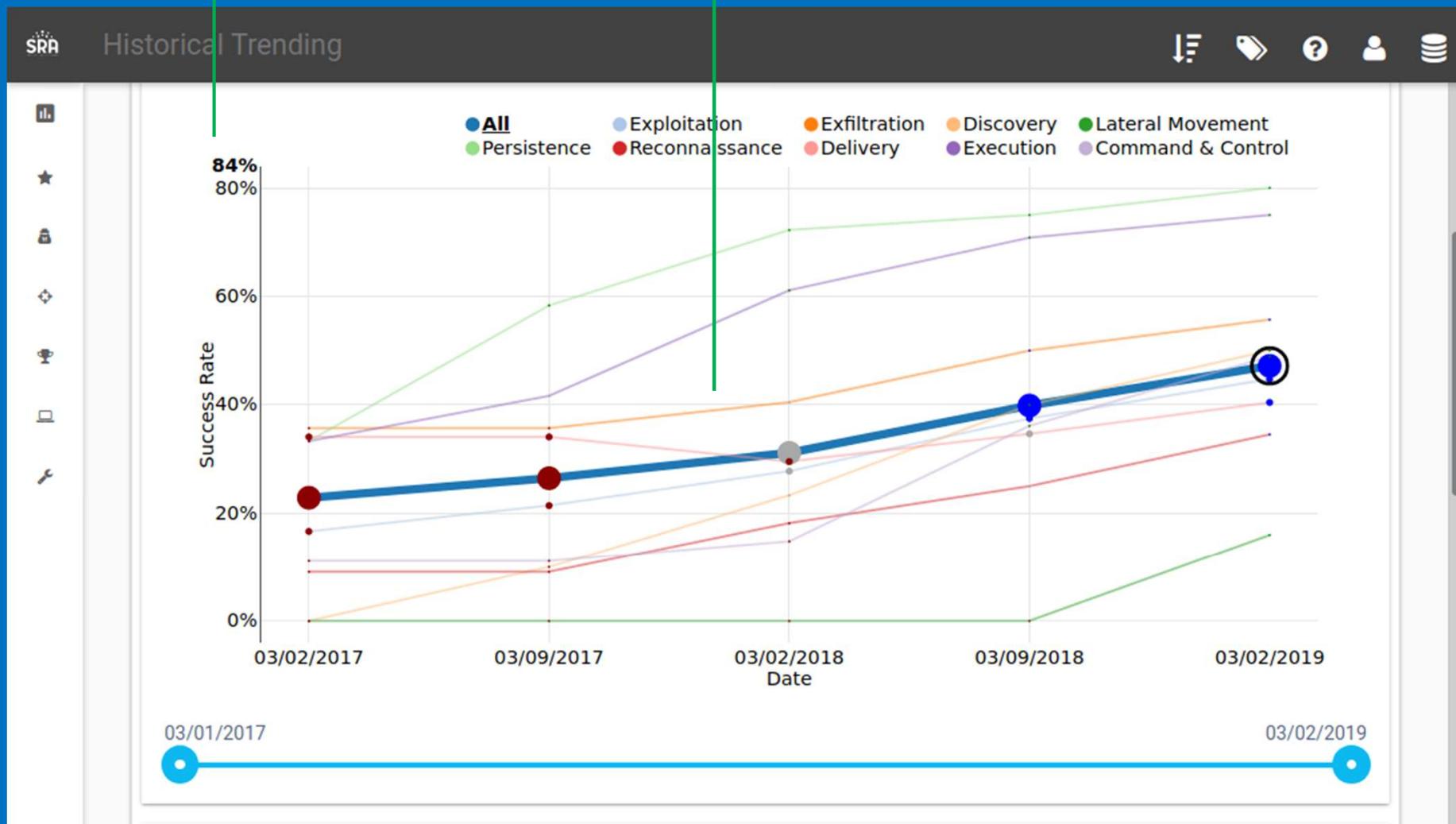
# PROGRESS REPORTING

## HISTORIC TRENDING VIEW

SAMPLE DATA

Over time,  
dashboards provide  
holistic view of  
improvements

Tactic view shows  
control efficacy by  
Kill Chain phase



# IMPORT

SUPPORTS YAML, JSON AND DIRECT IMPORT VIA TAXII SERVER

Supports importing directly from a STIX / TAXII server

Or manually, via YAML or JSON files

The screenshot shows the 'Import Data' interface. On the left is a vertical toolbar with icons for Home, Star, Collection, Refresh, Import, Export, and Help. The main area has a dark header bar with the SRA logo and 'Import Data' text, along with a download icon, a file icon, a question mark icon, a user icon, and a settings icon.

**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.  
Drag & Drop your files or Browse

# IMPORT

## ATOMIC RED TEAM

Flexibility to import  
one, some, or all  
intrusion sets

The screenshot shows the SRA (Security Research Assistant) interface with a dark header bar containing the SRA logo and various icons for file operations, help, and user profile.

The main content area has a title "Import Atomic Red" and instructions:

- Select Data from <https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/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.

Below these instructions are buttons for "SELECT ALL" and "DESELECT ALL", and status indicators: 0 Assessment Group Templates, 0 Campaigns, and 0 Total Test Cases Selected. A "Submit" button is also present.

A navigation bar below the status indicators includes "First", "Previous", "1" (highlighted in blue), "Next", and "Last".

The main list area displays a hierarchical structure of campaigns and their test cases:

- List of All Campaigns → 12 Total Campaigns. 677 Total Test Cases.
  - Campaign: Collection → 28 Total Test Cases.
  - Campaign: Command & Control → 32 Total Test Cases.
  - Campaign: Credential Access → 50 Total Test Cases.
  - Campaign: Defense Evasion → 211 Total Test Cases.
  - Campaign: Discovery → 102 Total Test Cases.
  - Campaign: Execution → 45 Total Test Cases.

# IMPORT

## MITRE CTI BUNDLE

Flexibility to import  
one, some, or all  
intrusion sets

The screenshot shows the VECTR application interface with a dark header bar containing the SRA logo and various icons for file operations, user management, and help.

The main content area has a title "Import STIX2 Data" and a sub-instruction: "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."

Below this, there are buttons for "SELECT ALL" and "DESELECT ALL", and status indicators: "0 Assessment Group Templates", "0 Campaigns", and "0 Total Test Cases Selected". A "Submit" button is also present.

A navigation bar at the bottom of the content area includes links for "First", "Previous", "1" (selected), "2", "3", "4", "5", "6", "7", "8", "9", "10", "Next", and "Last".

The main list area displays a table of campaigns:

Campaign	Total Test Cases
List of All Campaigns	447
Campaign: 3PARA RAT	4
Campaign: 4H RAT	6
Campaign: ABK	7
Campaign: ADVSTORESHELL	24
Campaign: APT-C-36	8
Campaign: APT1	16
Campaign: APT12	5

Each row in the table includes a checkbox for selecting individual campaigns and a right-pointing arrow icon for viewing details.

# COLLABORATE

ACCELERATE ANALYSIS WITH PEERS

Export full intrusion campaigns to share with peers

The screenshot displays the GoldStandard Admin Assessment Configuration interface. On the left, the 'Manage Campaigns' panel shows a list of campaigns with columns for Name, Organization, Import Date, and Action. It includes entries for 'SRA', 'BBSRAT' (MITRE, 01 Sep 2020), and 'CrossRAT' (MITRE, 01 Sep 2020). An 'Export to JSON File' button is located at the bottom right of this panel. A vertical green line separates this from the 'BBSRAT Details' panel on the right. The 'BBSRAT Details' panel lists various intrusion techniques categorized by Phase, Technique, Variant, and Action. The techniques include Persistence (Windows Service, BBSRAT - Windows Service), Command & Control (Web Protocols, BBSRAT - Web Protocols), Defense Evasion (Process Hollowing, BBSRAT - Process Hollowing), Command & Control (Commonly Used Port, BBSRAT - Commonly Used Port), Persistence (Registry Run Keys / Startup Folder, BBSRAT - Registry Run Keys / Startup Folder), Command & Control (Symmetric Cryptography, BBSRAT - Symmetric Cryptography), Defense Evasion (Deobfuscate/Decode Files or Information, BBSRAT - Deobfuscate/Decode Files or Information), Discovery (System Service Discovery, BBSRAT - System Service Discovery), Discovery (Process Discovery, BBSRAT - Process Discovery), and Defense Evasion (File Deletion, BBSRAT - File Deletion). Each entry has a gear icon for configuration and a download icon for sharing.

Name	Organization	Import Date	Action
SRA			
BBSRAT	MITRE	01 Sep 2020	
CrossRAT	MITRE	01 Sep 2020	

Export to JSON File

Phase	Technique	Variant	Action
Persistence	Windows Service	BBSRAT - Windows Service	
Command & Control	Web Protocols	BBSRAT - Web Protocols	
Defense Evasion	Process Hollowing	BBSRAT - Process Hollowing	
Command & Control	Commonly Used Port	BBSRAT - Commonly Used Port	
Persistence	Registry Run Keys / Startup Folder	BBSRAT - Registry Run Keys / Startup Folder	
Command & Control	Symmetric Cryptography	BBSRAT - Symmetric Cryptography	
Defense Evasion	Deobfuscate/Decode Files or Information	BBSRAT - Deobfuscate/Decode Files or Information	
Discovery	System Service Discovery	BBSRAT - System Service Discovery	
Discovery	Process Discovery	BBSRAT - Process Discovery	
Defense Evasion	File Deletion	BBSRAT - File Deletion	

# COLLABORATE

ACCELERATE ANALYSIS WITH PEERS

Supports importing directly from a STIX / TAXII server

Flexibility to import one, some, or all intrusion sets

The screenshot shows the VECTR web application's 'Import VECTR Data' feature. At the top, there's a header with the SRA logo and various navigation icons. Below the header, the main content area has a title 'Import VECTR Data' and a sub-instruction 'Data to be imported from file and merged with VECTR Template Data.' A summary bar at the top right indicates '1 Assessment Group Templates, 7 Campaigns, 162 Total Test Cases Selected.' A large checkbox is checked next to 'Assessment Group Template: Iranian TTP Bundle → 7 Campaigns.' Below this, a list of campaigns is shown with their respective test case counts: CopyKittens (6), OilRig (APT34) (44), MuddyWater (31), Collection of Iranian TTPs from US-CERT AA20-006A (15), APT39 (18), Magic Hound (27), and APT33 (21). Each campaign entry includes a right-pointing arrow icon and a 'Submit' button at the bottom right of the main content area.

EXPORTING CAMPAIGN TEMPLATES ONLY SHARES THE RED VIEW

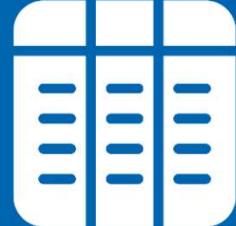
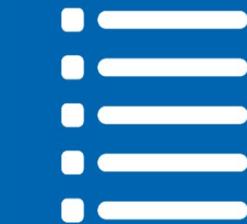
# VECTR CONCEPTS

ADAPTING VECTR FOR ADVERSARIAL MODELLING

VECTR VISION



**Database**  
For logical separation of assessments



**Assessment**  
Typically after a period of time, such as Q1 2020

**Campaign**  
Usually focussing around a specific TTP sprint

**Test Case**  
A specific atomic test to be completed

OUR VISION



**Team Use Case**  
One database per team within security



**Threat Actor**  
To track specific threat actors of interest



**Cyber Attack**  
Prominent cyber attack or tool used by the adversary



**Specific Test**  
Specific way a tool was used by the adversary

# VECTR CONCEPTS

PREPARING FOR ADVERSARY EMULATION

THREAT-LED



## Team Use Case

One database per team within security



## Threat Actor

To track specific threat actors of interest



## Cyber Attack

Prominent cyber attack or tool used by the adversary



## Specific Test

Specific way a tool was used by the adversary

THREAT RESEARCH

LAZARUS

BANK OF BANGLADESH

TTP1

FAR EASTERN INTERNATIONAL BANK

TTP 2

TROY OPERATION

TTP 3

DARKSEOUL OPERATION

TTP 4

SONY PICTURES

ETC

Not sure which threat actors or events are relevant? Read Chapter 7 “*Threat Intelligence for Risk Analysis*” by Recorded Future (free):

[go.recordedfuture.com/book](http://go.recordedfuture.com/book)

# VECTR-FY EVERYTHING

VECTR HERE, VECTR THERE, VECTR EVERYWHERE!



## Threat Intelligence

Threat Intelligence teams can use Vectr to collate and organise known truths about a threat actor, and their TTPs



## Internal Incidents

Incident Responders can log novel incidents such as Phishing campaigns into Vectr, and use its powerful reporting views



## Formal Engagements

Formal engagements, such as Pen Tests, can be loaded and actioned within Vectr

AND MUCH, MUCH MORE!

# LESSONS LEARNT

PREPARING FOR SUCCESS

1

## Get Buy-In

For best results, get support from your teams as early as possible

2

## Agree Responsibilities

Define clearly the roles of each area, to help industrialise outcomes

3

## Create a Framework

Develop your own framework detailing research standards

“

The best preparation for tomorrow is doing your best today

— H. Jackson Brown Jr

# DEMO

# QUESTIONS?

# BREAK

After the break:  
Hands-on workshop

# HANDS-ON LAB



Access a copy of this presentation, complete with  
set-up guides, helper scripts and more at:

<https://github.com/ssnkhan/x33fcon>

# INSTALLATION

PLEASE ACCEPT ALL DEFAULTS

```
sudo mkdir -p /opt/vectr  
cd /opt/vectr
```

TERMINAL

```
sudo wget  
https://github.com/SecurityRiskAdvisors/VECTR/releases/download/ce-5.7.0/sra-vectr-runtime-5.7.0-ce.zip
```

```
sudo unzip sra-vectr-runtime-5.7.0-ce.zip
```

```
sudo docker-compose -p sravectr up -d  
sudo nano /etc/hosts // and add fQDN for vectr
```

TIP

For demonstration purposes, please use default configuration options.  
Installation can take some time, so please start the process now

# LAUNCHING VECTR

## HELPER SCRIPTS

```
# Launch Vectr
cd /opt/vectr
sudo docker-compose up -d
sleep 30
firefox "https://sravectr.internal:8081/sra-purpletools-
webui/app/#"
```

TERMINAL

```
# Shutdown Vectr
cd /opt/vectr
sudo docker-compose down
```

TIP

Save these as `start_vectr.sh` and `shutdown_vectr.sh` in your home folder to quickly launch and safely shutdown your Vectr instance. Remember to `chmod +x`

# SET UP: UNDERSTANDING SCOPE

## LOCAL VS GLOBAL SCOPE

Configuration of offensive and defensive tooling (Vendor & Tools) as well as specific controls (Defensive Layers) can be set either locally for the current database, or globally; where they become available across all databases.

- **Local Scope** – Use this when you do not wish to persist customisations (including Test Cases) across other databases (e.g., where each database might represent a specific client)
- **Global Scope** – Use this if you wish to make your changes available across all your databases. This is best if your Vectr instance will be used entirely by your organisation

Local Scope

Global Scope

The screenshot shows the Vectr application interface. On the left is a navigation sidebar with the following structure:

- SRA
- VECTR
- HOME
- ASSESSMENTS
- REPORTING
- VENOR & TOOLS
- DEFENSIVE LAYERS
- TARGET ASSETS
- SOURCE IPs
- ADMINISTRATION
  - GROUP TEMPLATES
  - CAMPAIGN TEMPLATES
  - TEST CASES
  - VENOR & TOOLS
  - DEFENSIVE LAYERS
  - PHASES
  - ORGANIZATIONS
  - KILL CHAINS
  - TAGGING
  - DETECTION RULES
  - IMPORT DATA
  - USER MANAGEMENT

On the right, there is a table titled "ASSESSMENTS" with the following data:

Name	Create Date
Enterprise Purple – 2017 Q1	01/03/2017
Enterprise Purple – 2017 Q3	08/03/2017
Enterprise Purple – 2018 Q1	01/03/2018
Enterprise Purple – 2018 Q3	08/03/2018
Enterprise Purple – 2019 Q1	01/03/2019

At the bottom of the screen is the SRA logo.

# SET UP: ORGANISATIONS

## CONFIGURING VECTR

Organisations allow you to capture and attribute the source of research or analysis within Vectr. It is sensible to create a separate organisation for any key contributor, such as:

- Teams within your organisation (such as Threat Intelligence, your SOC or Red Teams)
- Specific Trust Groups
- Vendors, where analysis is made available in STIX / TAXII format

**TIP**

If a business area has their own database, they should have their own organisation too

ADMINISTRATION > ORGANIZATIONS

New Organization

Name:	<input type="text"/>
Description:	<input type="text"/>
Abbreviation:	<input type="text"/>
Url:	<input type="text"/>
Members:	<input type="button" value="+"/>

# SET UP: DATABASES

## CONFIGURING VECTR

In Vectr, Session Databases are designed as a means of logically separating a collection of work or research.

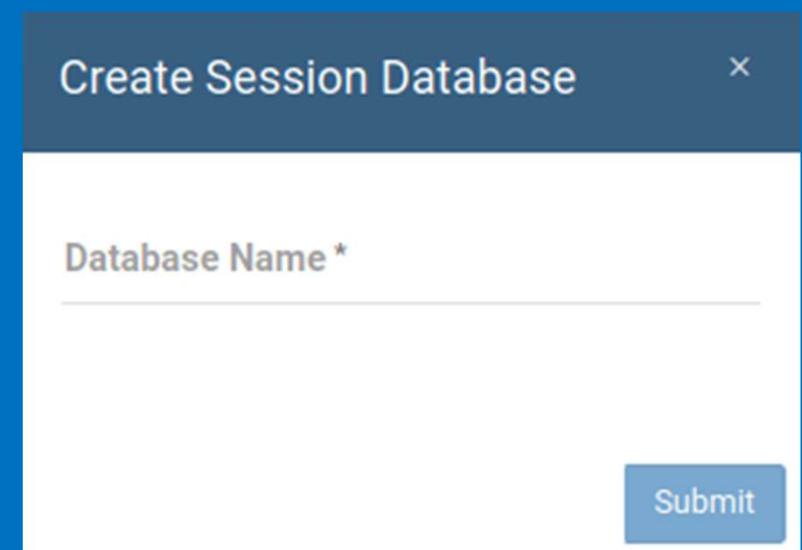
For instance, you may wish to create individual databases for:

- Threat intelligence led research
- Internal security Incidents
- Formal Pen Test findings
- Red Team Wiki
- Trust Groups / Collaboration

TIP

When considering a new database, think of the reporting implications

DB MENU > SELECT SESSION DATABASE



# SET UP: PHASES

CONFIGURING VECTR

In Vectr, Phases are the term used to organise and configure specific frameworks that you may wish to use. Your chosen framework will then be accessible when capturing Test Cases, and for illustrating the Escalation Path. Good candidates include:

- Mitre ATT&CK
- Unified Kill Chain
- Lockheed Martin Kill Chain
- Your bespoke Kill Chain

TIP

The order of Phases determines the way in which the Escalation Path is drawn

ADMINISTRATION > PHASES

## Mitre ATT&CK

INITIAL ACCESS   EXECUTION   PERSISTENCE  
PRIVILEGE ESCALATION   DEFENSE EVASION  
CREDENTIAL ACCESS   DISCOVERY  
LATERAL MOVEMENT   COLLECTION  
COMMAND AND CONTROL   EXFILTRATION   IMPACT

## Lockheed Martin Kill Chain

RECONNAISSANCE   WEAPONISATION   DELIVERY  
EXPLOITATION   INSTALLATION  
COMMAND AND CONTROL   ACTIONS ON OBJECTIVES

# SET UP: TAGS

## CONFIGURING VECTR

Tags are a powerful way of orchestrating actions within Vectr, and can serve as a helpful prompt to other teams within your organisation. For instance, you can use Tags to:

- Set the status of a piece of analysis
- Identify teams responsible for some output or analysis
- Set priorities for specific Test Cases
- Capture other internal metadata unique to your organisation or workflows

### TIP

Consider including Tags as part of your workflow standards documents

ASSESSMENTS > MENU > TAGGING

CAMPAIGN > MENU > TAGGING

TEST CASES > CONFIGURE TAGS

### Suggestions

QUEUED FOR ANALYSIS ANALYSING COMPLETE

ARCHIVED

QUEUED FOR ANALYSIS ANALYSING ENHANCING

CONTROL REVIEW VALIDATING COMPLETE

CTI SIEM TEAM FORENSICS MALWARE

ARCHITECTURE NETWORKS THREAT HUNTING

# SET UP: VENDORS & TOOLS

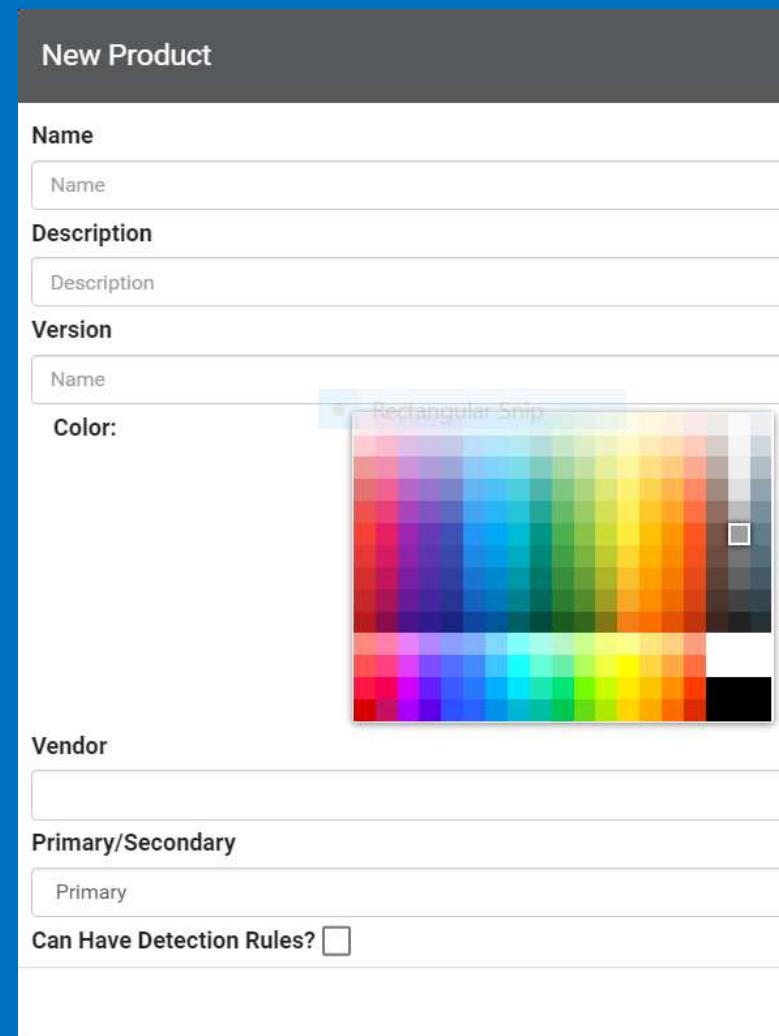
## CONFIGURING VECTR

A lot of the value in using Vectr is being able to understand which specific controls are responsible for detecting and blocking specific techniques. Setting these correctly ensures your controls receive the appropriate kudos.

- **Defensive Layers** – These should be high-level, vendor agnostic controls (e.g., Web Proxy)
- **Vendors & Tools** – These should represent the specific controls in your environment (e.g., FireEye EX)

### TIP

Remember to set your Vendor tool appropriately under “Can Have Detection Rules”

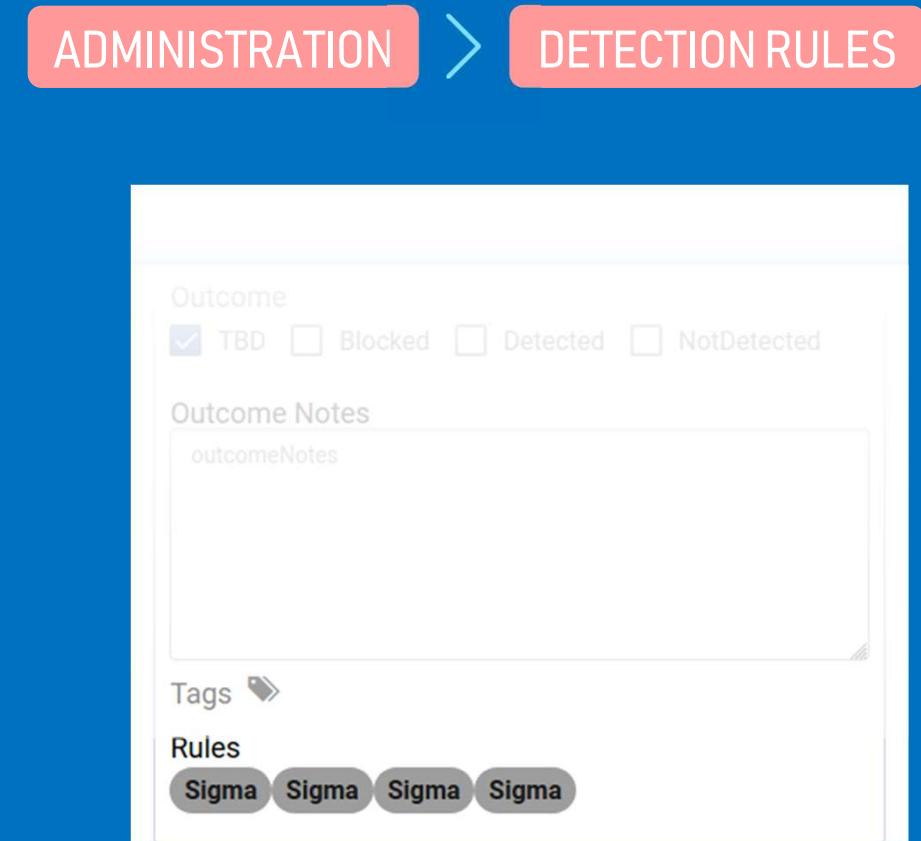


# SET UP: DETECTION RULES

## CONFIGURING VECTR

Detection rules allow signatures to be mapped to specific TTP Test Cases; to help continue developing a full view of the TTPs effect in your environment, and can support Threat Hunting initiatives.

- **Data Sources** – Reflect the various telemetry which underpins your ability to develop detections
- **Generic Sources** – Vendor agnostic, such as JA3, Sigma or YARA
- **Generic Rules** – The actual rules
- **Analysis Rules** – Vendor specific rules, such as Splunk, Tanium Signals
- **Behaviours** – Behaviours are the mechanism which link your rules to their corresponding TTPs



The following video demonstrates the process:  
[youtu.be/Xt2JsbNnUCA](https://youtu.be/Xt2JsbNnUCA)

# TIPS & TRICKS

GET THE MOST OUT OF VECTR

## Actor Naming

- Hidden Cobra, Lazarus, Bluenoroff, Labyrinth Chollima or ...? Agree on a common naming taxonomy:

APT38 · Lazarus · Hidden Cobra

## Campaign Naming

- Consider prefixing all campaigns with date serialisation to quickly sort chronologically: **YYYYMMDD Campaign:**

20160204 Bank of Bangladesh

## Abort FYI Use Cases

- To prevent polluting your management information with “FYI” only Test Cases, abort them in the Red Team view:

Assessment → Campaign → Test Case → 

## Key-Value Pairs

- In both Red and Blue team views, establish standardised key-value pairs to capture data:

md5:value sha1:value leadTester:staffID

# EXERCISES: IMPORT

PRACTICAL EXAMPLES TO GET YOU UP AND RUNNING

1

## Mitre CTI Bundle

[github.com/mitre/cti/blob/master/enterprise-attack/enterprise-attack.json](https://github.com/mitre/cti/blob/master/enterprise-attack/enterprise-attack.json)

2

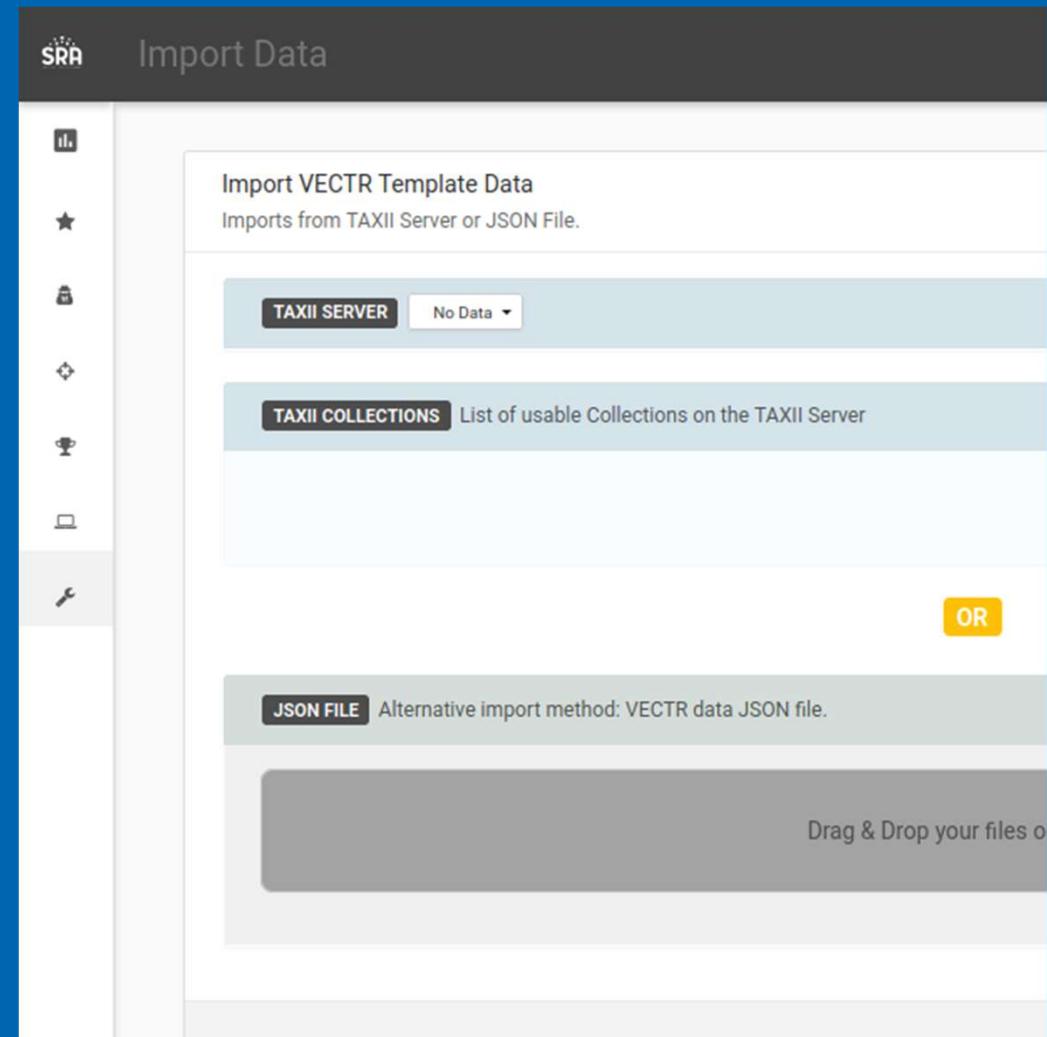
## Atomic Red Team

[github.com/redcanaryco/atomic-red-team/blob/master/atomics/indexes/index.yaml](https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/indexes/index.yaml)

3

## SRA Iran Analysis

[github.com/SecurityRiskAdvisors/VECTR/tree/master/cti](https://github.com/SecurityRiskAdvisors/VECTR/tree/master/cti)



# EXERCISES: THREAT LIBRARY

PRACTICAL EXAMPLES TO GET YOU UP AND RUNNING

The rest of the session will be used to complete a few exercises to help develop your confidence and familiarity with Vectr – [pan-unit42.github.io/playbook\\_viewer/](https://pan-unit42.github.io/playbook_viewer/)

The screenshot shows a web-based application titled "PLAYBOOK VIEWER". On the left sidebar, there is a navigation menu with various threat names listed: UNIT 42, PLAYBOOK WALKTHROUGH, VIEW HOME, VIEW MAP, FILTER PLAYBOOKS, CLEAR FILTERS, OILRIG, SOFACY (which is highlighted in orange), PICKAXE, PATCHWORK, DARKHYDRUS, REAPER, RANCOR, TICK, DRAGONOK, MENUPASS, EMISSARY PANDA, and MIRRORTED. The main content area has a title "PLAYBOOK VIEWER" and a section for "SOFACY". It displays four time periods: October 2018 to November 2018, October 2018 to October 2018, March 2018 to March 2018, and February 2018 to February 2018. Below this, it shows an "Intrusion Set: Sofacy" with "Campaigns: 4", "Indicators: 51", and "Attack Patterns: 34". It also lists "Industries: [Icons]", "Regions: [Flags]", and "Malware Used: Cannon, Zebrocy". A table titled "Select Kill Chain [Lockheed Martin]" is shown, with columns for Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, and Actions on Objectives. The Delivery column contains the entry "T1566.001: Spearphishing Attachment" with a count of 27. The Installation column contains "T1047: Windows Management Instrumentation" with a count of 1. The Command & Control column contains "T1071: Application Layer Protocol" with a count of 7. The Actions on Objectives column contains "T1113: Screen Capture" with a count of 0. The bottom of the page includes a footer with the text "Created by Palo Alto Networks - Unit 42" and "Mitre Attack TTX 2.0".

# QUESTIONS?

HERE TO HELP



## Thank You for Participating

Tweet me at [@snkhhan](https://twitter.com/snkhhan), or send a message via LinkedIn at [linkedin.com/in/sajidnawazkhan](https://linkedin.com/in/sajidnawazkhan).

## Come Work for Us

[www.sc.com/en/careers/jobseekers/](http://www.sc.com/en/careers/jobseekers/)

## Getting Involved

SRA are currently developing a TTP Index for various industry sectors, including Finance. To get involved, and provide your input and expertise, please contact SRA at:

[vectr@sra.io](mailto:vectr@sra.io)



PHOTOS FROM UNSPLASH