black hat®
ARSENAL 2023

AUGUST 9-10
MANDALAY BAY/LAS VEGAS

THREAT PATROL

BLUE TEAM

UniSuper

ThreatPatrol – Protecting your Environment with Intelligence

VIRAL MANIAR

WHOAMI

- 12+ years of experience in the field of information security and management
- Passionate about offensive and defensive security
- Lead Security Specialist at UniSuper in Australia
- Runs a boutique consultancy firm - Preemptive Cybersecurity
- In my spare time, I develop security tools
- Presented at BlackHat USA, RootCon, DEF CON, OWASP meets and (ISC)2 local chapter.
- Outside of Infosec land – I like photography

https://github.com/Viralmaniar

https://twitter.com/maniarviral

https://www.linkedin.com/in/viralmaniar/

https://viralmaniar.github.io/

Information Classification: General

black hat ARSENAL 2023

AGENDA

01 Threat Landscape & Cybersecurity Incidents

- Problem Statement
- Statistics on cyber attacks (Q1 2023)
- Introduction to Threat Intelligence & Threat Hunting

02 Threat Intelligence Lifecycle

- Collection to Dissemination
- CTI Levels
- Reactive vs Proactive CTI program
- Types of Threat Intelligence

03 Using Threat Intelligence for Situational Awareness

- Race to Initial Access
- Usual Campaign Process
- Signal collection
- Pyramid of Pain
- CTI Maturity model

04 Cyber Threat Intelligence Frameworks

- CTI Frameworks & Diamond Model
- CTI for Blue, Red & Purple Team
- Traffic Light Protocols
- TAXII & STIX

05 Identifying and Profiling Threat Actors

- Identifying and Intro to Threat Actor Types
- Profiling Threat Actors
- Setting up Profiling Methodologies without Tools.

06 Threat Intelligence Reporting & Dissemination

- Types of Reports
- CTI Sharing
- SIGMA & YARA
- Where to Disseminate Reports & Intelligence

07 Open-Source Threat Intelligence Platform

- MISP
- OpenCTI
- IntelOwl
- YETI

08 Other Community Projects on TTPs

- Living Off The Land Binaries, Scripts and Libraries (LOLBAS)
- GTFOBins
- Living Off The Land Drivers
- FileSec
- Unprotect.it
- C2 Matrix

09 ThreatPatrol - Demo

- Architecture Design
- Features & Focus of the ThreatPatrol project
- Live demo
- Roadmap

Information Classification: General

Threat Landscape

Information Classification: General

Rising Tide of Cyber Attacks on Global Organisations

Cyber attacks against organisations worldwide, regardless of their size or geography, are growing in a sustained way, and every day we see more news about security breaches.

Need for Threat Intelligence

Breaches and Records

Between January 1, 2005 & December 31, 2022, there were 12,789 breaches and just in the second half of 2022 about 40 billion records were exposed.

Rising Breaches

Security breaches have increased by 72% in the last 5 years, and according to McAfee research *the hidden costs of cybercrime*, the monetary loss was around 1 trillion dollars.

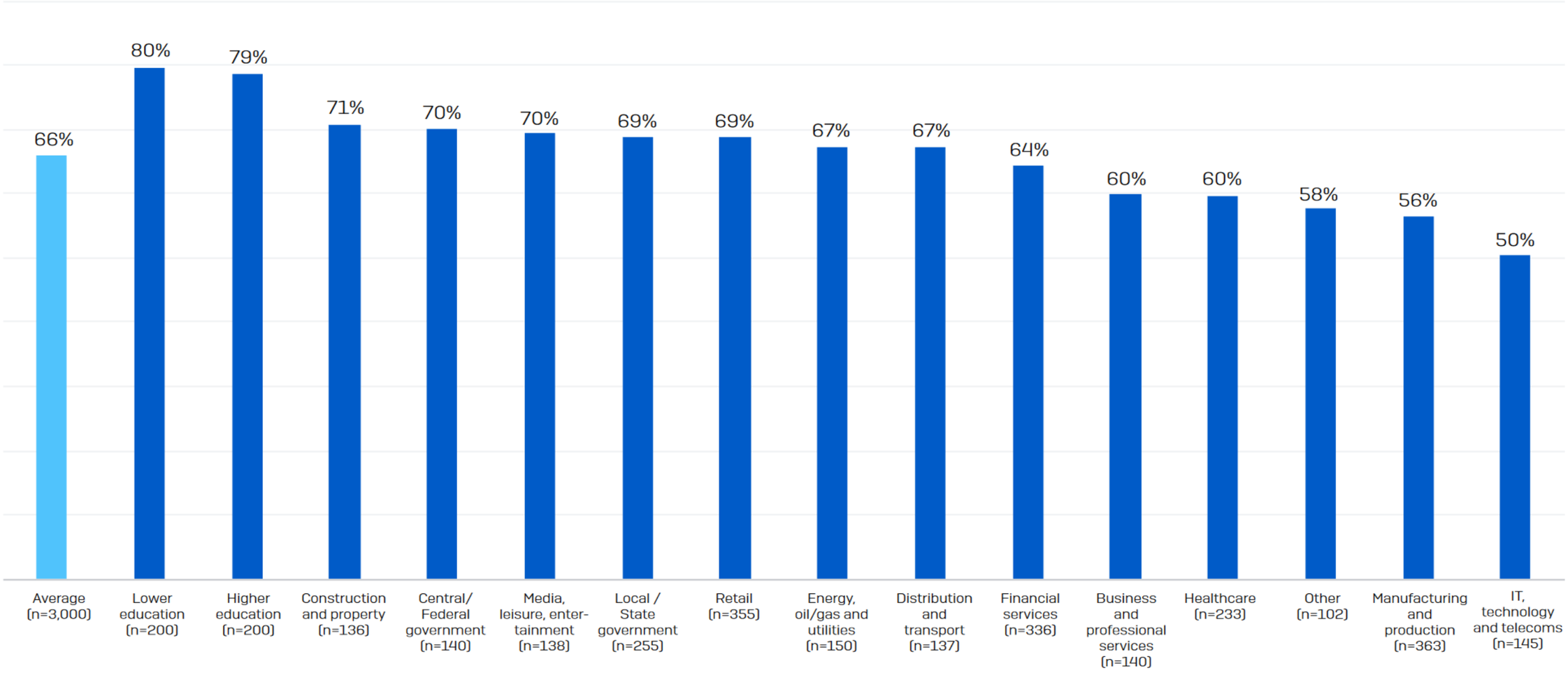
COVID-19 Impact

In August 2020, Interpol published the report *Cybercrime: COVID-19 Impact,* the key cyber threats were phishing and scam fraud, accounting 59% of incidents, malware & ransomware – 36% , Malicious domains – 22% and fake news – 14%

Information Classification: General

In the last year, has your organisation been hit by cyber attack? Base: 3,000 respondents.

(THE STATE OF RANSOMWARE 2023) – Sophos white paper



Information Classification: General

Data Breach at UPS Canada Disclosed: Some Stolen Customer Information Was Abused in SMS Phishing Attempts

itnews NEWS GOVERNMENT SECURITY REPORTS RESOURCES PODCAST LOG IN SUBSCRIBE

Australia had five data breaches that hit 1 million or more people

BLEEPINGCOMPUTER

NEWS DOWNLOADS VPNS VIRUS REMOVAL GUIDES TUTORIALS

Home > News > Security > American Airlines, Southwest Airlines disclose data breaches affecting pilots

American Airlines, Southwest Airlines disclose data breaches affecting pilots

The Register

Oreo cookie maker says crooks gobbled up staff info

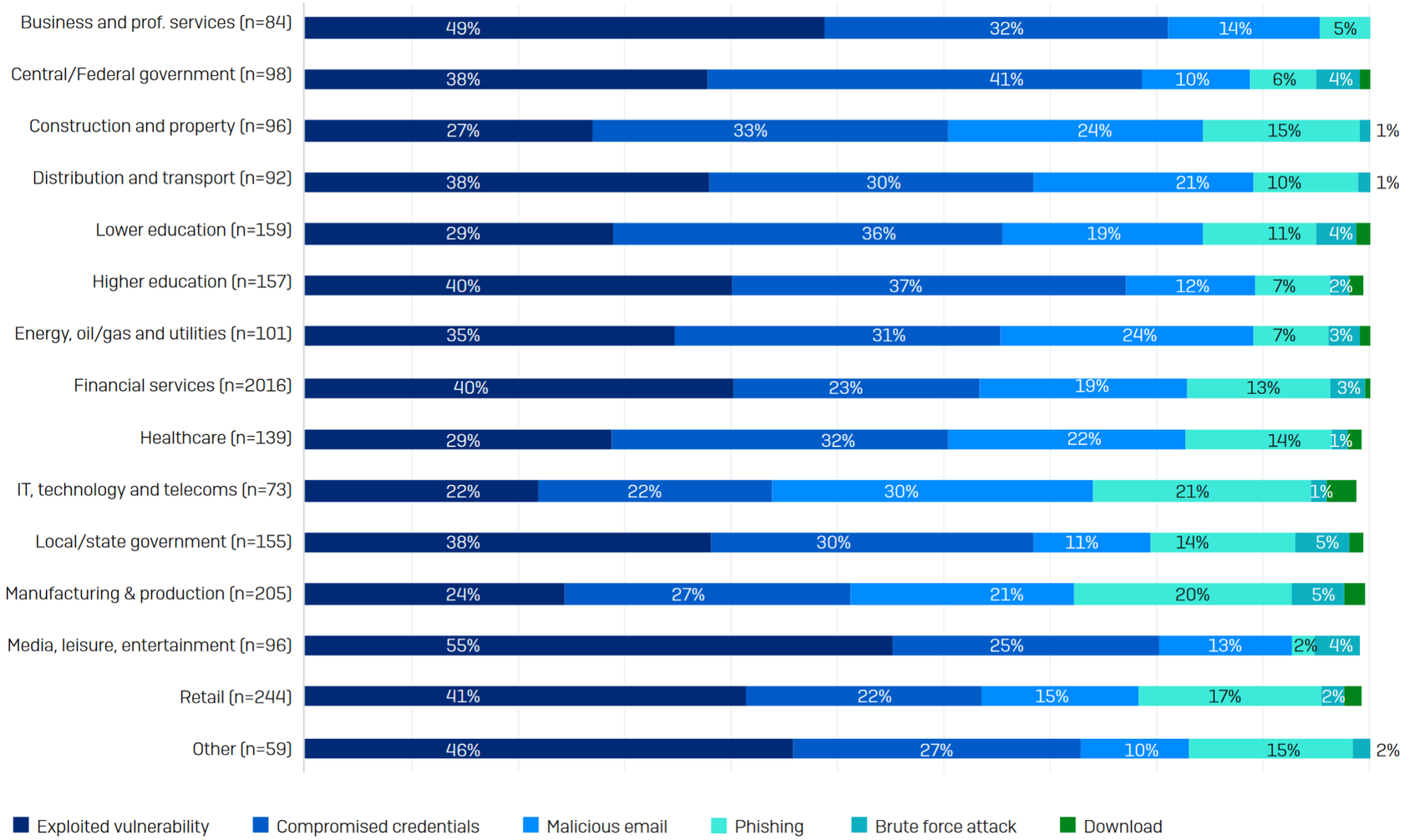
50K-plus employees' personal info swiped after law firm rolled

Jessica Lyons Hardcastle Tue 20 Jun 2023 / 21:01 UTC

Mondelez International has warned 51,000 of its past and present employees that their personal information has been stolen from a law firm hired by the Oreo and Ritz cracker giant.

Do you know the root cause of the cyber attack your organisation experienced in the last year? Base: 3,000 respondents.

(THE STATE OF RANSOMWARE 2023) – Sophos white paper



Information Classification: General

Threat Intelligence & Threat Hunting

Threat intelligence refers to the information collected, analysed, and utilised to identify and mitigate potential cybersecurity threats.

It provides organisations with actionable insights into the tactics, techniques, and procedures (TTPs) used by threat actors, enabling proactive defense measures.

Threat intelligence helps organisations stay ahead of emerging threats, make informed decisions, and strengthen their overall security posture.

Threat hunting involves actively searching for hidden threats and indicators of compromise (IOCs) within an organisation's network or systems.

It goes beyond traditional security measures and focuses on proactively identifying threats that may have evaded existing security controls.

Threat hunting combines human expertise, advanced analytics, and threat intelligence to identify malicious activities and potential breaches.

Information Classification: General

Threat Intelligence Lifecycle

Information Classification: General

Extracting valuable insights by analysing collected data, utilising techniques like correlation, pattern recognition, and behavioral analysis, to identify potential threats and understand the tactics, techniques, and procedures (TTPs) employed by threat actors.

Processing & Analysis

Integration & Enrichment

Combining the processed threat intelligence with internal data sources, such as indicators of compromise (IOCs) and existing threat intelligence feeds, to provide contextual information and enhance its value for more effective threat detection and response.

Gathering data from diverse sources, such as open-source intelligence (OSINT), commercial threat feeds, government sources, and internal security data, to acquire relevant information for analysis.

Collection

Dissemination & Feedback

Timely sharing of analysed threat intelligence with stakeholders, internally and externally, for proactive defense and coordinated response to emerging threats. Gathering feedback for ongoing improvement and alignment with evolving security needs.

Planning & Direction

Establishing the objectives, scope, and key stakeholders involved in the threat intelligence program.

Information Classification: General

Unprepared & Passive

Organisation lacking necessary insights to take action upon. Unprepared CTI maturity lacks readiness, while passive CTI maturity lacks proactive engagement.

Reactive

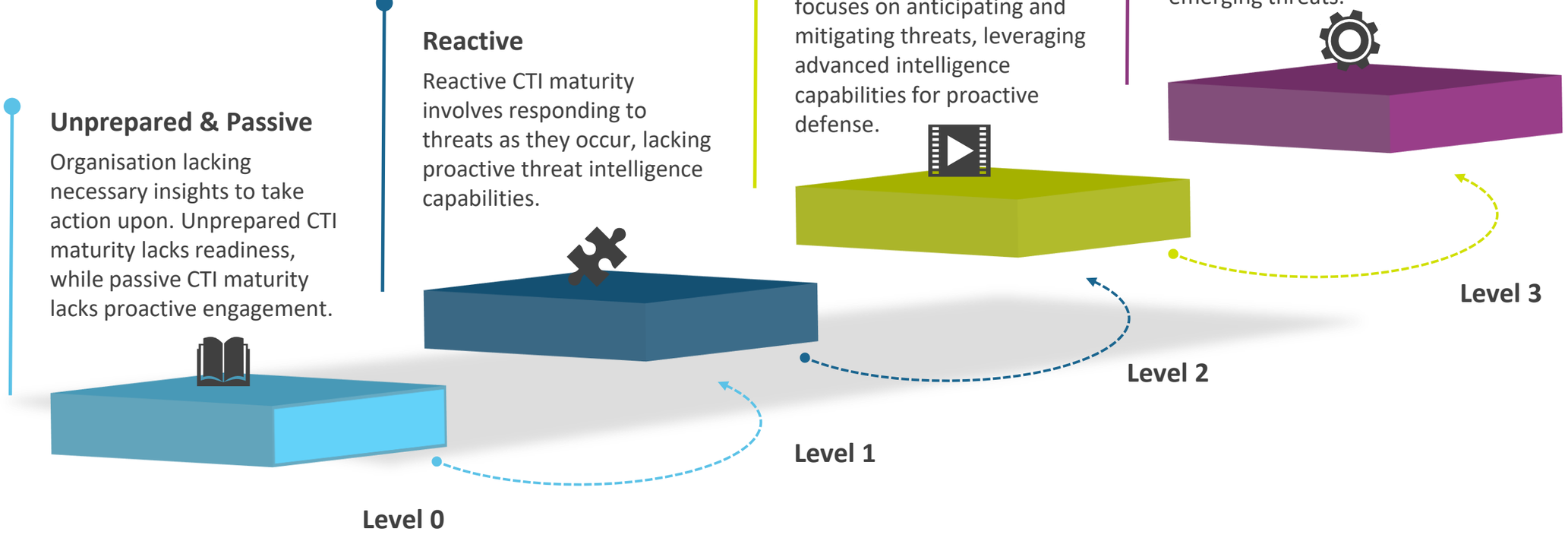
Reactive CTI maturity involves responding to threats as they occur, lacking proactive threat intelligence capabilities.

Proactive

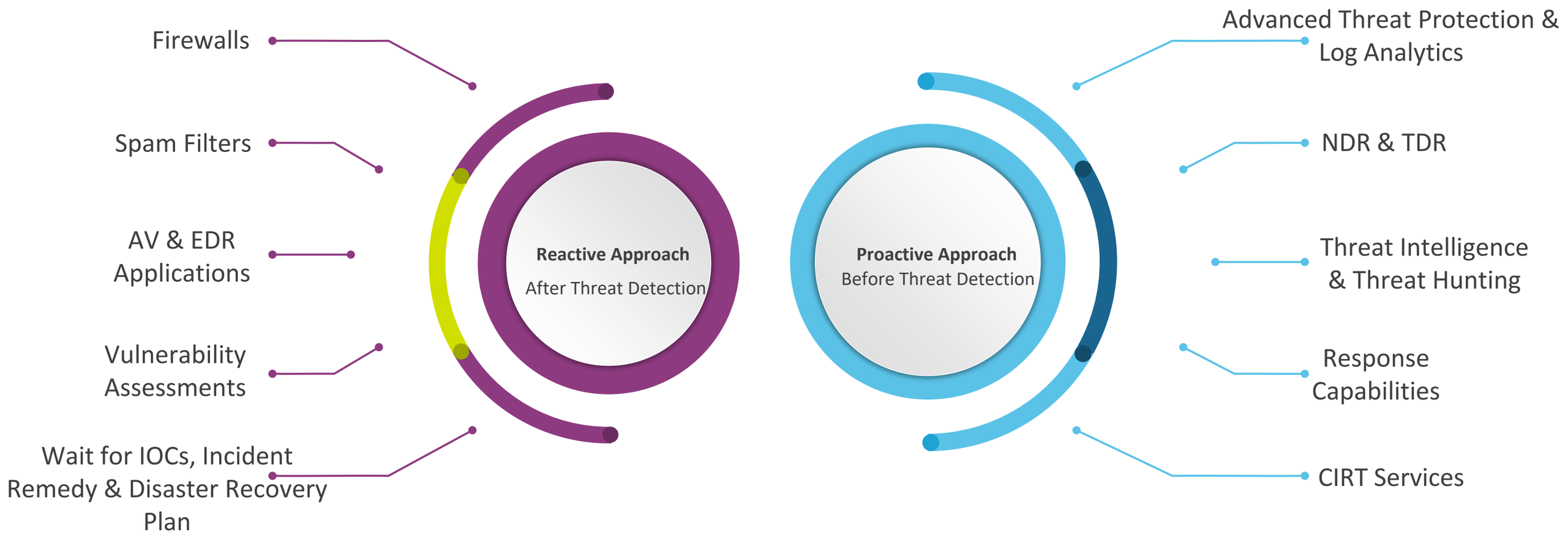
Proactive CTI maturity focuses on anticipating and mitigating threats, leveraging advanced intelligence capabilities for proactive defense.

Predictive & Anticipatory

Predictive and anticipatory CTI maturity involves leveraging advanced analytics and intelligence to forecast and proactively mitigate emerging threats.



Information Classification: General

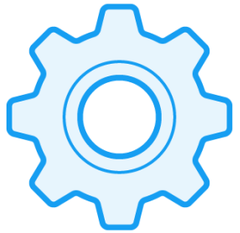


Information Classification: General

SHORT-TERM USE

LONG-TERM USE

SHORT-TERM USE



LONG-TERM USE

TECHNICAL

Indicator of Compromise

SOC Analyst
L1 support
Network Support
InfraOps

TACTICAL

Attacker TTPs

SOC Analyst
SIEM
Firewall
Endpoints
IDS/IPS

OPERATIONAL

Incoming Attacks

Threat Hunter
SOC Analyst
Vulnerability Management
Incident Response
Insider Threat

STRATEGICAL

High Level Information on Risks

CISO
CIO
CTO
Executive Board

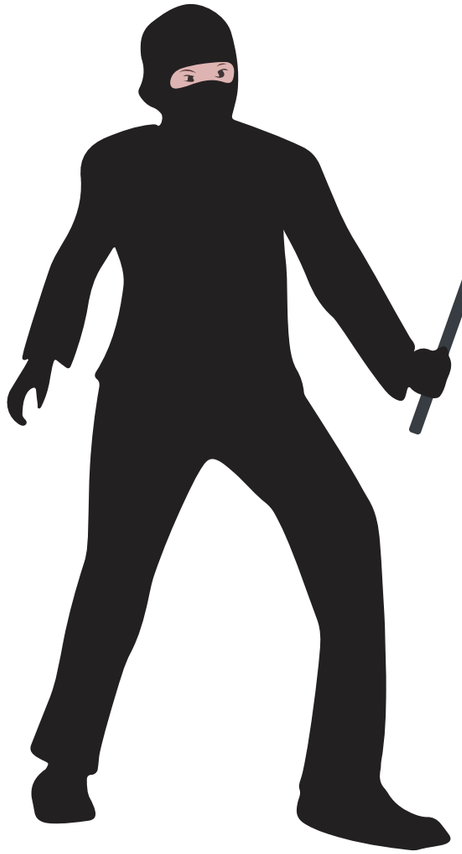
LOW-LEVEL

HIGH-LEVEL

Information Classification: General

Using Threat Intelligence for Situational Awareness

Information Classification: General



Race for Initial Access

In a high-stakes scenario, an attacker cunningly crafts a deceptive email, posing as the IT department, in an attempt to phish a user and gain unauthorised access to an organisation's internal resources. The unsuspecting user unknowingly stands at the brink of becoming a gateway for the attacker's malicious intentions.

- ❑ Exploit vulnerability
- ❑ Phishing
- ❑ Vishing / Smishing
- ❑ Malicious attachment
- ❑ Business Email Compromise
- ❑ Credential stuffing
- ❑ Password Brute force

Information Classification: General

Easiest Attack Vector

Typosqatted Domain

Campaign Design

Good ROI for Attackers

Fully working Phishing page

Drop Malware

Information Classification: General

Signals: Attacker vs. Victim Indicators

Attacker Signals: Attackers emit a plethora of signals in their quest for unauthorised access, including port scanning, suspicious login activities, exfiltration attempts, command-and-control traffic, and the presence of malicious artifacts. These signals are invaluable for threat hunting and intelligence analysis, enabling security teams to detect, investigate, and mitigate potential threats effectively.

Victim Signals: Victims also emit signals indicative of potential compromises. These signals encompass anomalous network traffic patterns, system crashes, unexpected log entries, unauthorised access attempts, and unusual user behavior. By analysing these signals, security professionals can proactively identify ongoing attacks, respond promptly, fortify defenses, and derive valuable insights for future incident prevention.

Initial Connection

IP Address, Netblock, ASN, ISP, Recon details on WAF, Port scans alerts, Regular offenders

Campaign Creation

Email Provider, Subject Line, Email Body, Headers, Attachments, Links, Timestamps

Other Infrastructure

Transit IP & Netblocks, Transit ASN, Transit Times, Traceroute

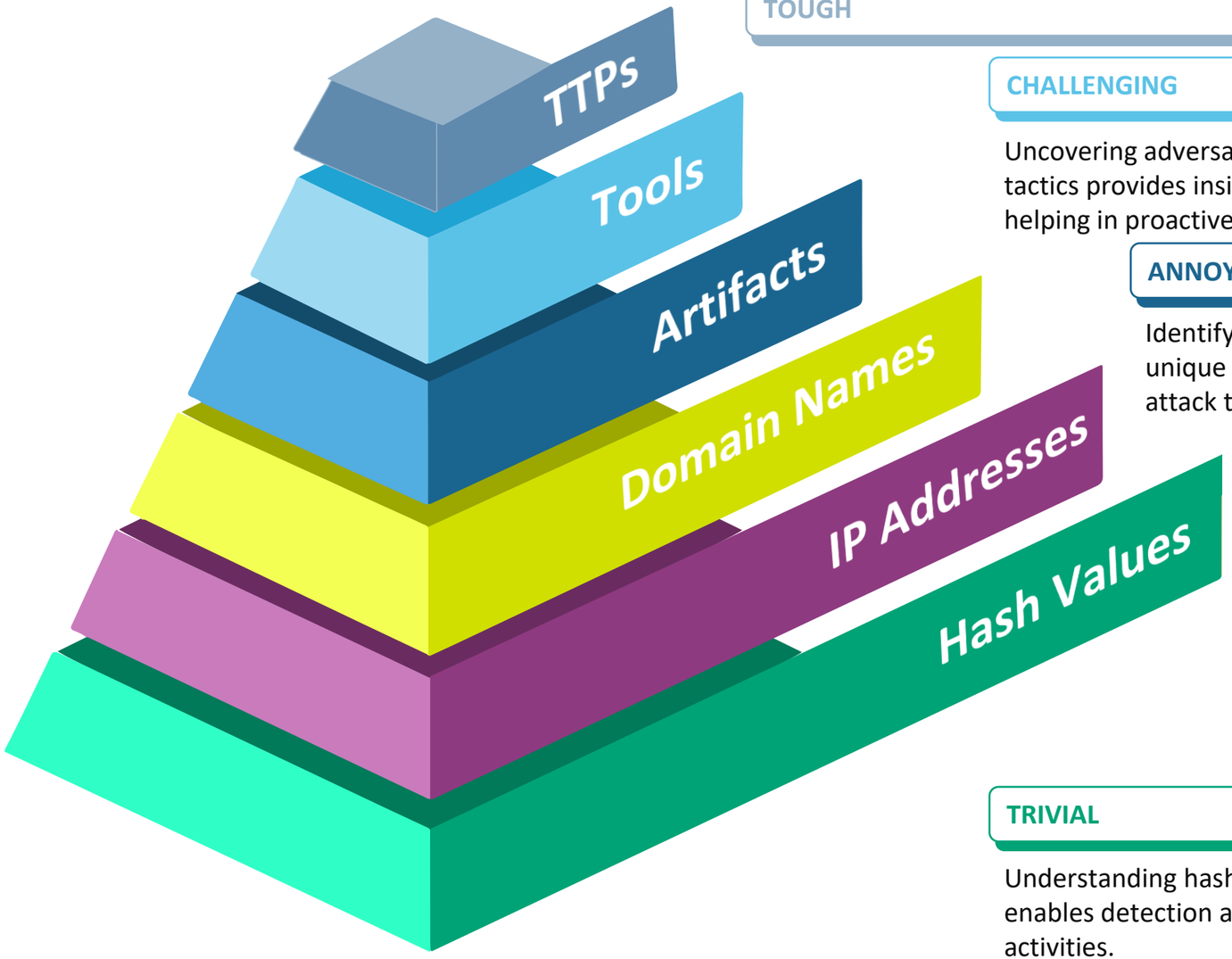
Receiver Side

Read Timestamp, Read trackers, Reader IP, Hostname, Location, OS, Browser Details, Gateway IP, Clicked Status, Redirects, Scan Details

Payload

File Hash, Known malware, C2 Domains, IP address, File Type, File Size, Metadata, Signatures

Information Classification: General



TOUGH

CHALLENGING

Uncovering adversary tools, techniques and tactics provides insights into their techniques, helping in proactive defense.

ANNOYING

Identifying and analysing specific artifacts, such as unique malware samples, aids in understanding attack techniques.

SIMPLE

Tracking and blocking adversary infrastructure, such as command-and-control servers, disrupts their operations.

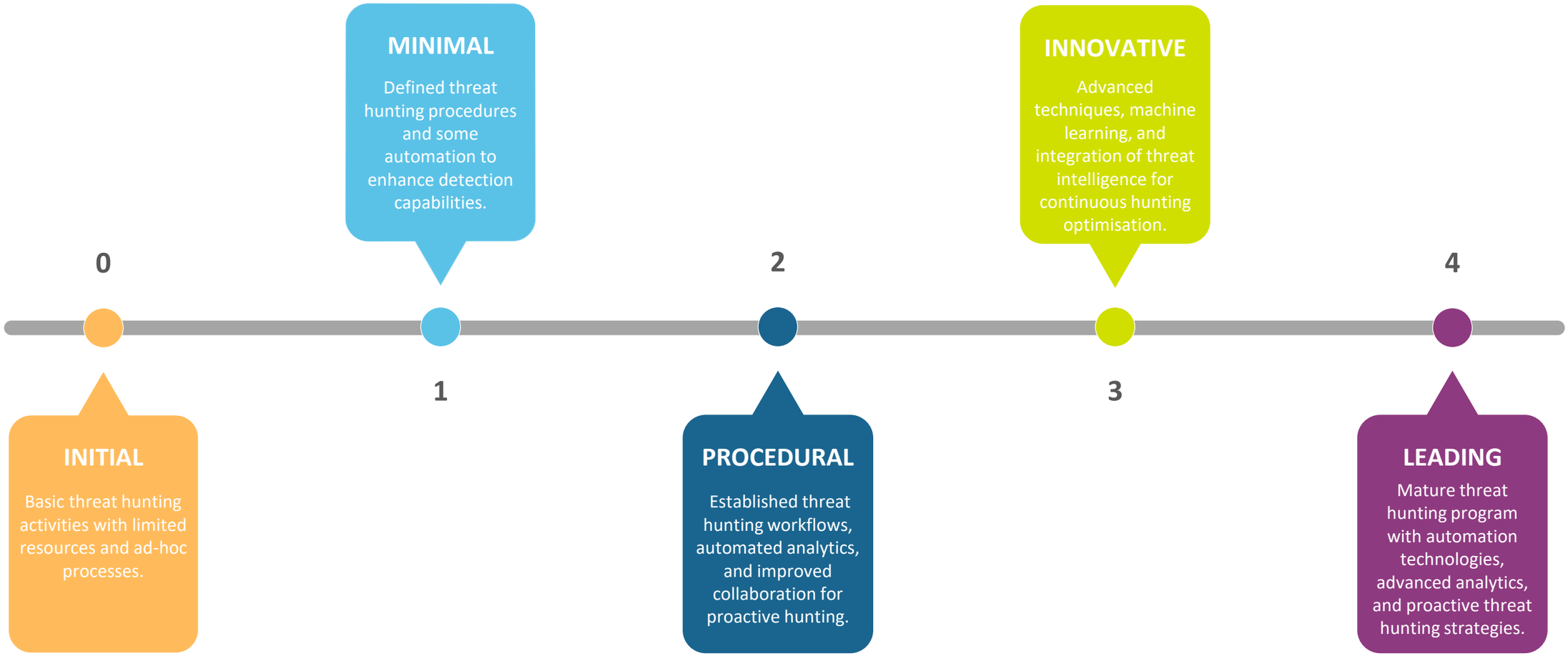
EASY

Low-level indicators like file hashes and IP addresses serve as initial data points for analysis.

TRIVIAL

Understanding hash values and IP addresses enables detection and mitigation of their future activities.

Information Classification: General



Information Classification: General

CTI Frameworks & Data Sharing Models

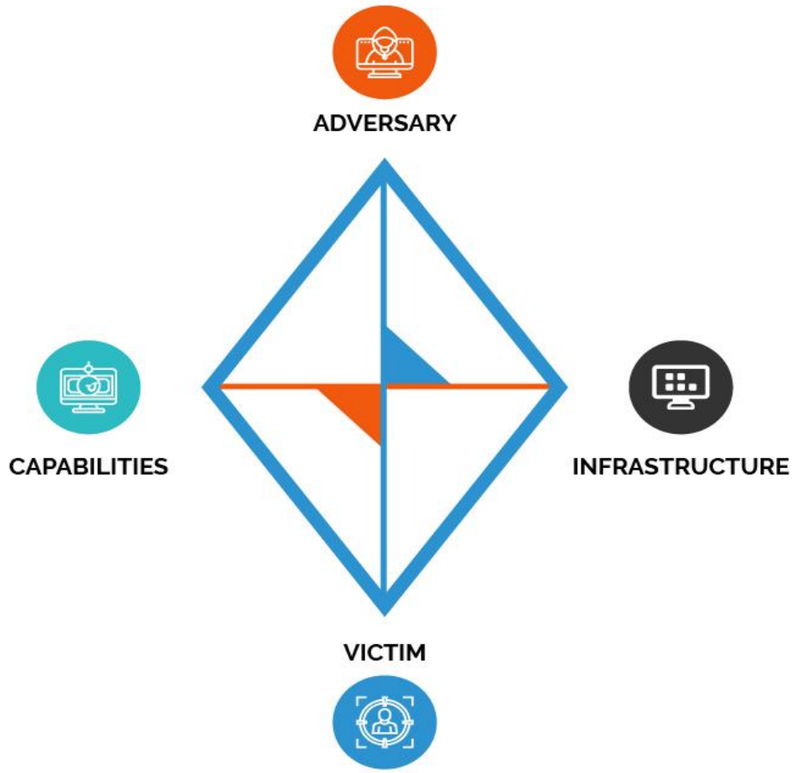
Information Classification: General

STAGES FOR CYBER KILL CHAIN:

- RECONNAISSANCE
- WEAPONIZATION
- DELIVERY
- EXPLOITATION
- INSTALLATION
- COMMAND AND CONTROL
- ACTIONS ON OBJECTIVES

TACTICS FOR MITRE ATT&CK:

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



The diamond model provides a model for threat intelligence central to threat hunting. Each vertex of the diamond model provides a classification point for adversary tactic, techniques and procedures

Information Classification: General

Blue Team

The Blue Team, responsible for defending systems, can leverage threat intelligence and CTI frameworks to enhance their defensive capabilities. By analysing threat intelligence feeds and incorporating CTI frameworks into their security operations, they can proactively identify and respond to emerging threats, strengthen their incident response capabilities, and improve overall resilience against cyberattacks.

Red Team / Adversary

The Red Team, focused on simulating attacks, can benefit from threat intelligence and CTI frameworks by incorporating real-world threat intelligence into their testing methodologies. By using up-to-date threat intelligence feeds and CTI frameworks, they can emulate advanced adversary tactics, techniques, and procedures (TTPs) and provide valuable insights on vulnerabilities and weaknesses within an organisation's defenses.

Purple Team

The Purple Team, combining the Blue and Red Teams, can utilise threat intelligence and CTI frameworks to foster collaboration and improve overall security posture. By sharing relevant threat intelligence with the Blue Team, the Purple Team can help identify gaps, improve detection and response capabilities, and validate the effectiveness of defensive measures against real-world threats discovered through red teaming exercises. This collaboration fosters a continuous feedback loop to enhance overall security resilience.

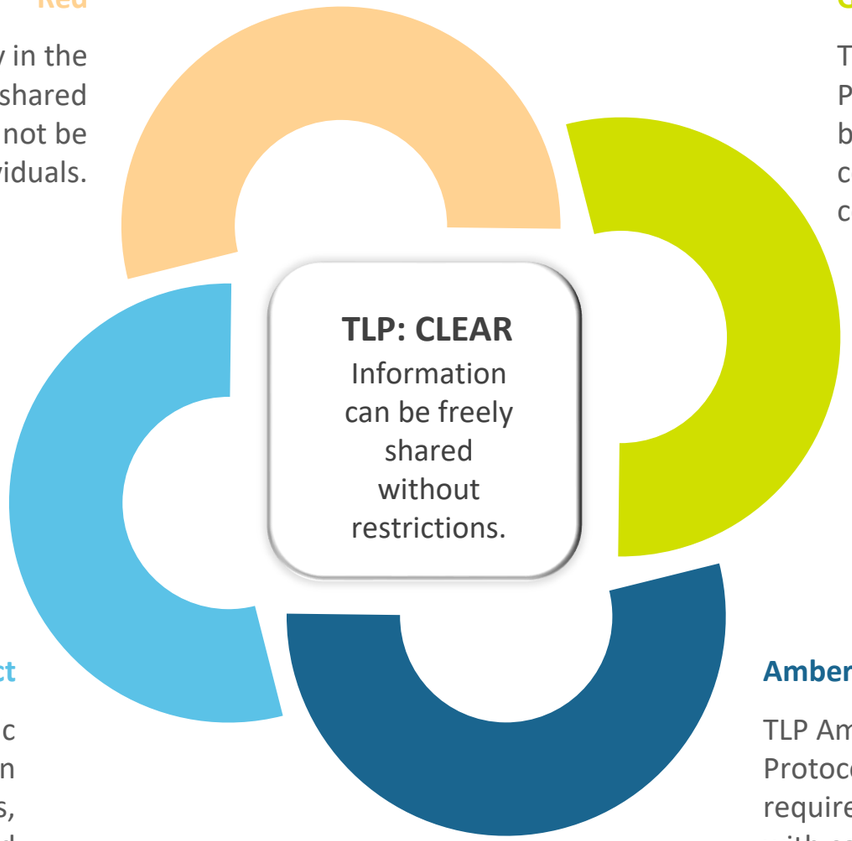
Information Classification: General

Red

TLP Red is the highest level of confidentiality in the Traffic Light Protocol, indicating that the shared information is strictly confidential and should not be disclosed to any unauthorised individuals.

Green

TLP Green is a designation within the Traffic Light Protocol indicating that the shared information can be widely disseminated within an organisation or community without restrictions or concerns for confidentiality.



Amber + Strict

TLP Amber + Strict is a designation within the Traffic Light Protocol indicating that the shared information requires heightened confidentiality measures, limiting its distribution to a specific and restricted audience.

Amber

TLP Amber is a designation within the Traffic Light Protocol indicating that the shared information requires limited disclosure and should be handled with care, shared only with authorised individuals.

Information Classification: General

TAXII

TAXII (Trusted Automated Exchange of Indicator Information) enables secure sharing of cyber threat intelligence data.

It follows a structured format and protocol for exchanging indicators of compromise (IOCs) between organisations.

TAXII facilitates real-time information sharing, enhancing cyber defenses and enabling swift response to threats.

It promotes interoperability, standardisation, and automation in the cybersecurity community, fostering collaboration against evolving threats.

STIX

STIX (Structured Threat Information eXpression) is a standardised language for describing and sharing cyber threat information.

It enables organisations to exchange structured data about threats, vulnerabilities, and incidents in a consistent manner.

STIX provides a common framework for threat intelligence analysts to collaborate, analyse, and respond to cyber threats.

It supports automation and integration with other security tools, facilitating faster and more effective threat detection and response.

Information Classification: General

Identifying and Profiling Threat Actors

Information Classification: General

Hacktivists & Scriptkiddies

Threat intelligence must encompass monitoring both hacktivist activities, driven by social or political motivations, and scriptkiddie actions, executed by inexperienced attackers utilising pre-written tools, to effectively understand the diverse range of threats organisations face in the cybersecurity landscape.

APT Groups & Ransomware Gangs

APT (Advanced Persistent Threat) groups are sophisticated, organised, and often state-sponsored adversaries that carry out targeted cyber espionage or sabotage campaigns, requiring in-depth threat intelligence analysis to detect, attribute, and mitigate their activities effectively.

Ransomware gangs are cybercriminal organisations that employ ransomware as a means to extort money from individuals and organisations. Understanding their tactics, techniques, and infrastructure through threat intelligence enables proactive defense and incident response against ransomware attacks.

Insider Threats

Insider threats refer to individuals within an organisation who misuse their authorised access to cause harm, leak sensitive information, or disrupt operations. Threat intelligence plays a crucial role in detecting and mitigating insider threats through behavior monitoring and anomaly detection.

Cyber Criminals & Cyber-mercenaries

Cyber criminals are individuals or groups who engage in illicit activities for financial gain, such as stealing data, conducting fraud, or launching ransomware attacks. Threat intelligence helps in understanding their tactics, identifying their infrastructure, and mitigating their impact.

Cyber mercenaries are skilled individuals or groups who are hired to conduct cyber attacks on behalf of others, often for political or financial motives. Threat intelligence aids in tracking and monitoring their activities, attributing attacks, and countering their operations.

Information Classification: General

Compiling the List of Priority Threat Actors

Actors targeting Company A

Actors targeting Company A's industry peers

Actors targeting Company A's industry

Opportunistic actors

Threat Landscape Analysis

Intent Scoring

Intent notes the level of intent the attacker has on your company

Attack Intent

Capability

Capability is how advanced the group is

1 — Limited skills and resources
2 — Basic
3 — Moderate
4 — Advanced
5 — Superior

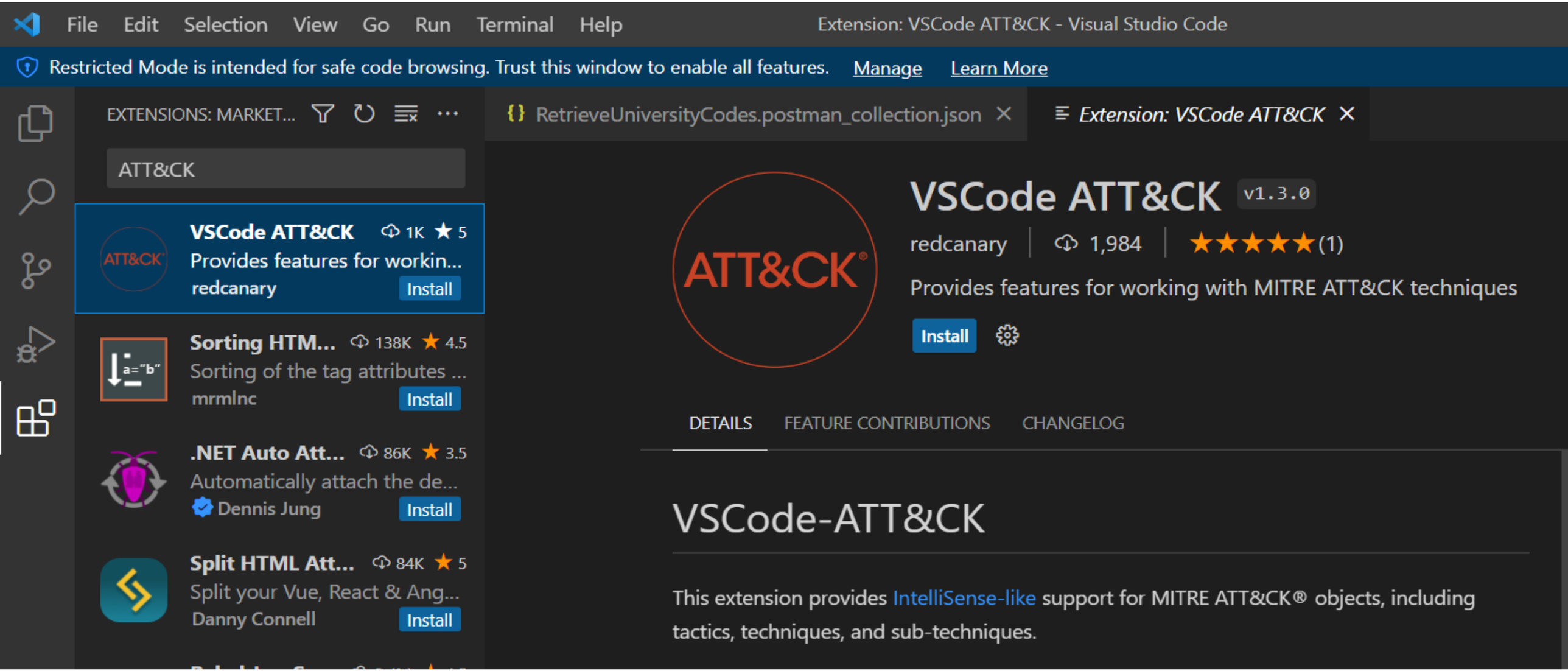
Skillset

A Priority Threat Actors Heatmap

With the capability and intent rankings, the final step is to visulise the data. This helps illustrate which actors may be more important to focus on.

Visualise

Information Classification: General



Information Classification: General

File Edit Selection View Go Run Terminal Help — Extension: Markdown PDF - Visual Studio Code

Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More

EXTENSIONS: MARKET...

yzane markdown pdf

Markdown PDF
Convert Markdown to PDF
yzane ✓ Disabled

Markdown 205K ★ 2
Markdown Paste Image To ...
starkwang Install

Markdown All ... 6.6M ★ 5
All you need to write Markd...
Yu Zhang Install

Markdown P... 4.3M ★ 4.5
Markdown Preview Enhance...
Yiyi Wang Install

{} RetrieveUniversityCodes.postman_collection.json

Extension: Markdown PDF

Markdown PDF v1.4.4

yzane | 1,640,072 | ★★★★½ (103)

Convert Markdown to PDF

✓ Disabled Uninstall

This extension has been disabled because the current

DETAILS FEATURE CONTRIBUTIONS CHANGELOG

Markdown PDF

This extension converts Markdown files to pdf, html, png or jpeg files.

Information Classification: General

```
# OceanLotus
## Threat Actor Profile
#### **ID: TA-G0050-OL**

The Ocean Lotus APT group is a hacker group operating against both private and government organisations and their opponents since **2014**. The primary motivation behind the attacks carried out by the Ocean Lotus group is information theft and espionage given the private information sought to be obtained in the attacks and the **high-profile individuals targeted**.

The targets of the Ocean Lotus group are generally foreign companies with sure success and interests in *Vietnams* hospitality, manufacturing, and consumer goods sectors. As well as the private sector, the Ocean Lotus group targets politicians and journalists opposed to the Vietnamese government.

## Associated Group Descriptions

|Name           | Description                                |
|---------------|--------------------------------------------|
|SeaLotus       | In 2016, Ocean Lotus was observed targeting a number of Vietnamese organizations with a watering hole attack.|
```

OceanLotus

Threat Actor Profile

ID: TA-G0050-OL

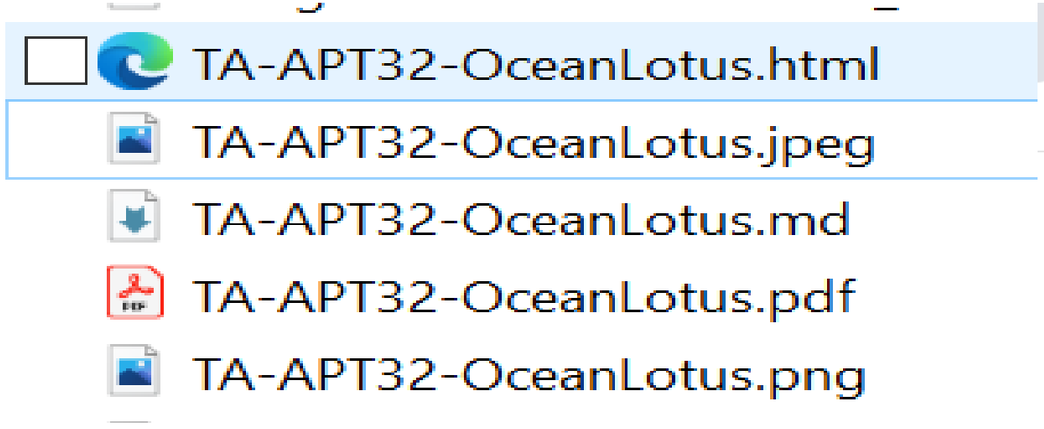
The Ocean Lotus APT group is a hacker group operating against both private and government organisations and their opponents since **2014**. The primary motivation behind the attacks carried out by the Ocean Lotus group is information theft and espionage given the private information sought to be obtained in the attacks and the **high-profile individuals targeted**.

The targets of the Ocean Lotus group are generally foreign companies with sure success and interests in *Vietnams* hospitality, manufacturing, and consumer goods sectors. As well as the private sector, the Ocean Lotus group targets politicians and journalists opposed to the Vietnamese government.

Associated Group Descriptions

Name	Description
SeaLotus	In 2016, Ocean Lotus was observed targeting a number of Vietnamese organizations with a watering hole attack.

Information Classification: General



TA-APT32-OceanLotus.pdf - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools TA-APT32-OceanL... ×

1 / 1 75%

OceanLotus

Threat Actor Profile

ID: TA-G0050-OL

The Ocean Lotus APT group is a hacker group operating against both private and government organisations and their opponents since **2014**. The primary motivation behind the attacks carried out by the Ocean Lotus group is information theft and espionage given the private information sought to be obtained in the attacks and the **high-profile individuals targeted**.

The targets of the Ocean Lotus group are generally foreign companies with sure success and interests in *Vietnams* hospitality, manufacturing, and consumer goods sectors. As well as the private sector, the Ocean Lotus group targets politicians and journalists opposed to the Vietnamese government.

Associated Group Descriptions

Name	Description
SeaLotus	In 2016, Ocean Lotus was observed targeting a number of Vietnamese organizations with a watering hole attack.

TA-APT32-OceanLotus.md

File | C:/Users BlackHat%202023/TA-APT...

OceanLotus

Threat Actor Profile

ID: TA-G0050-OL

The Ocean Lotus APT group is a hacker group operating against both private and government organisations and their opponents since **2014**. The primary motivation behind the attacks carried out by the Ocean Lotus group is information theft and espionage given the private information sought to be obtained in the attacks and the **high-profile individuals targeted**.

The targets of the Ocean Lotus group are generally foreign companies with sure success and interests in *Vietnams* hospitality, manufacturing, and consumer goods sectors. As well as the private sector, the Ocean Lotus group targets politicians and journalists opposed to the Vietnamese government.

Associated Group Descriptions

Name	Description
SeaLotus	In 2016, Ocean Lotus was observed targeting a number of Vietnamese organizations with a watering hole attack.

Information Classification: General

Threat Intelligence Reporting & Dissemination

Information Classification: General

Threat Landscape Report
A comprehensive analysis outlining the current cybersecurity threat landscape trends.

Threat Analysis Report
In-depth assessment revealing vulnerabilities, risks, and mitigation strategies for threats.

Centralised TI Sharing, P2P TI Sharing, Hybrid TI Sharing
Collaborative sharing of threat intelligence through a centralised & P2P platforms.

YARA & SIGMA Rules
Patterns and logic for detecting malware and security events.

Information Classification: General

01 IOC API
Data sent to SIEM & LOGGING

02 IOC API
Next-Gen Firewalls

03 SNORT
Intrusion Detection

04 IOC API
Web Proxy

05 SANDBOX
Malware Analysis

06 TAILORED INTEL
Situational Analysis

07 EXPLOITS API
Data Analytics

08 REPORT API
Intel Platform

Information Classification: General

Anti Virus

Anti-virus software leverages threat intelligence to proactively detect and block known malware and emerging threats.

Endpoint Detection & Response

EDR applications leverage threat intelligence to detect, investigate, and respond to advanced and targeted cyber threats.

Cloud Access Security Broker

CASB applications leverage threat intelligence to provide visibility, control, and protection against cloud-based security risks and threats.

SIEM Agent

SIEM leverages threat intelligence to enhance log analysis, correlation, and detection of security incidents for effective response.

Identity Detection and Response

Identity Detection and Response leverages threat intelligence to identify and respond to identity-based threats and unauthorised activities.

Vulnerability Management Agent

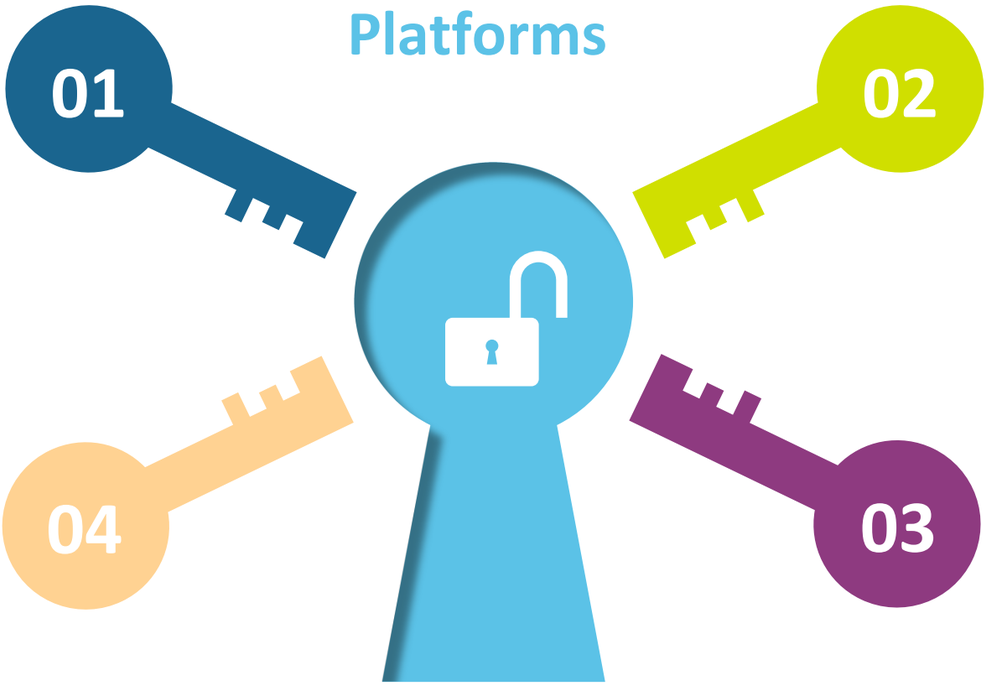
Vulnerability management agents leverage threat intelligence to prioritise and remediate vulnerabilities and exploit based on real-time threat data.

Information Classification: General

Open-Source Threat Intelligence Platform

Information Classification: General

Open-source Threat Intelligence Platforms



OPENCTI

OpenCTI

OpenCTI is an open source platform allowing organisations to manage their cyber threat intelligence knowledge and observables.

YETI

Yeti is a platform meant to organise observables, indicators of compromise, TTPs, and knowledge on threats in a single, unified repository.

MISP Threat Sharing

MISP

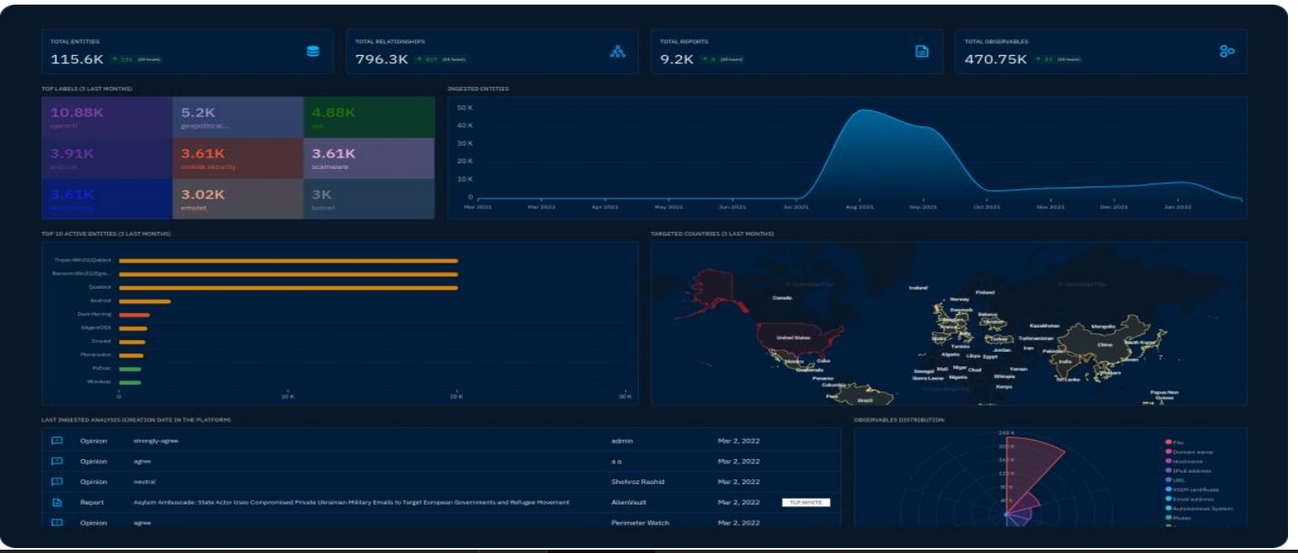
The MISP is an open source software solution for collecting, storing, distributing and sharing cyber security indicators and threats about cyber security incidents analysis and malware analysis. MISP is designed by and for incident analysts, security and ICT professionals or malware reversers to support their day-to-day operations to share structured information efficiently.

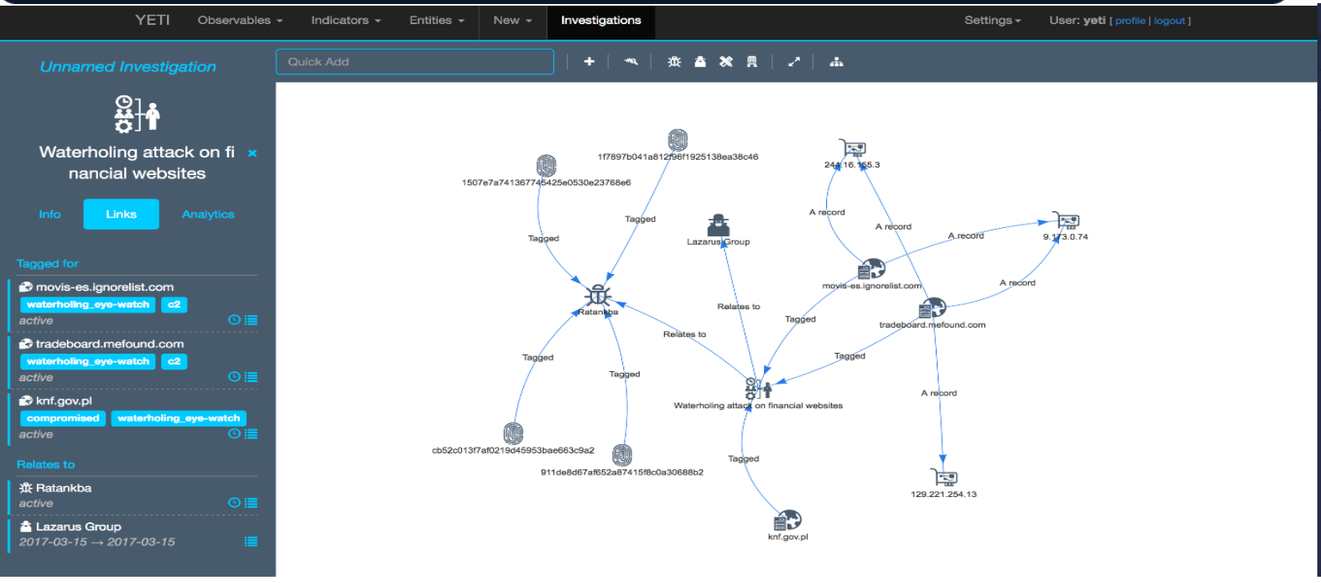
Intel owl

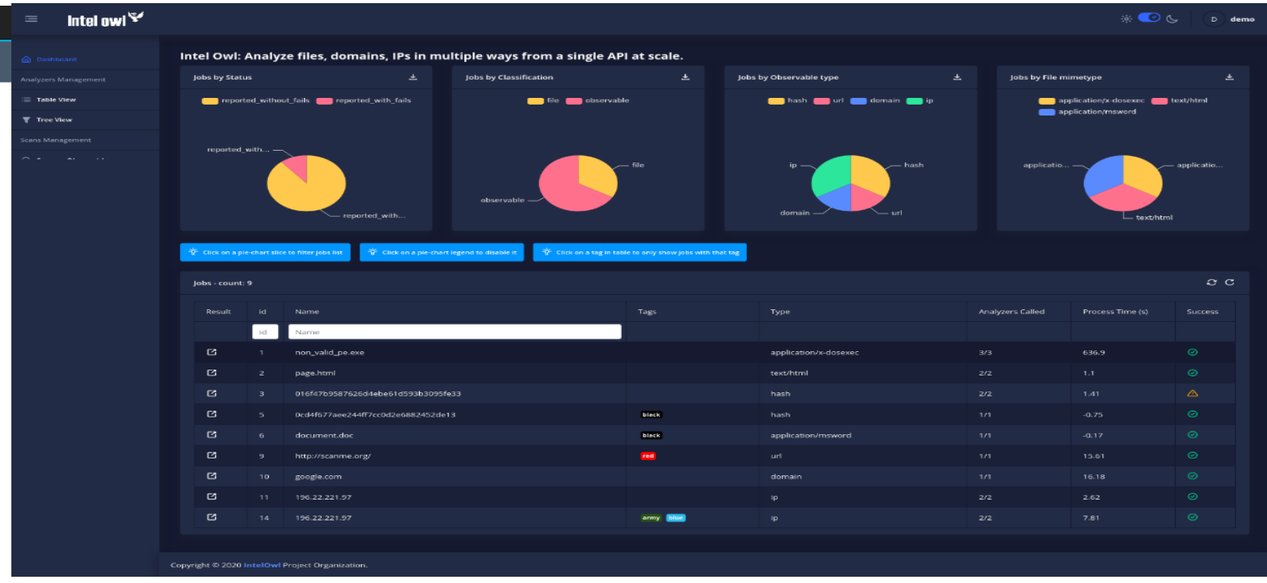
IntelOwl

Intel Owl is an Open Source Intelligence, or OSINT solution to get threat intelligence data about a specific file, an IP or a domain from a single API at scale.

Information Classification: General







Information Classification: General

Community Projects on TTPs

Information Classification: General

Cobalt Strike & Empire

The goal of this site is to point one to the best C2 framework for the needs based on your adversary emulation plan and the target environment.

DLL unhooking & SGN

The goal of this free database is to centralise the information about malware evasion techniques.

.7Z, .eml, .dcom & .exe

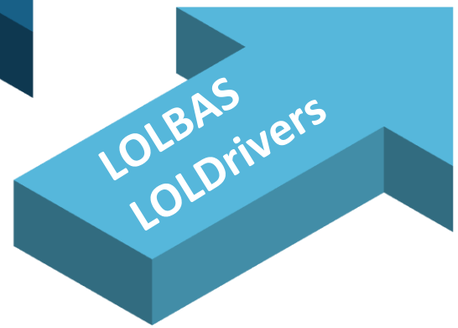
With Filesec BlueTeam can Stay up-to-date with the latest file extensions being used by attackers.

Curl, mount, python & pwsh

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

Procdump.exe & cmd.exe

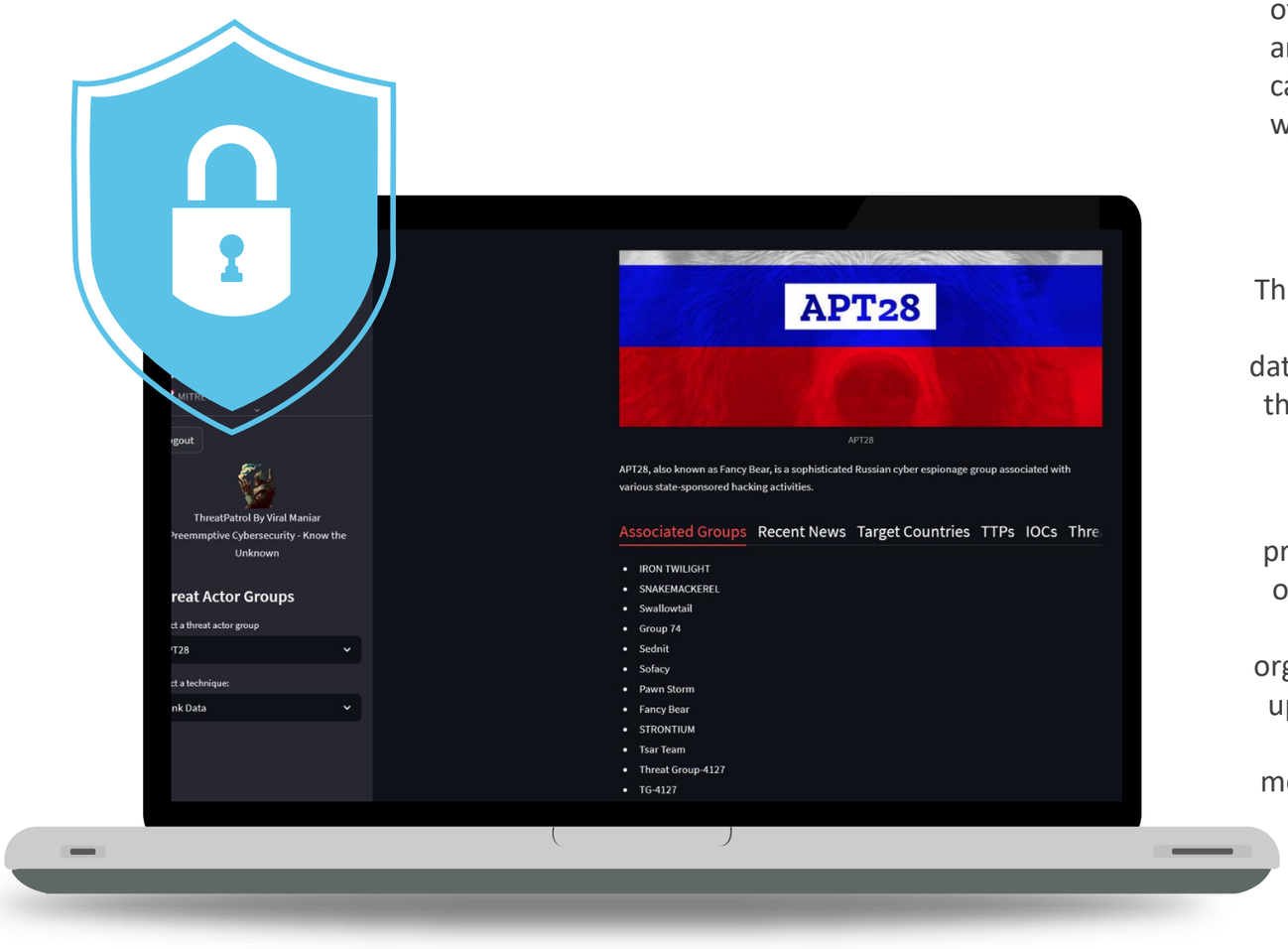
Living Off The Land Binaries & Drivers is a curated list of Windows drivers used by adversaries to bypass security controls and carry out attacks.



Information Classification: General

ThreatPatrol

Information Classification: General



ThreatPatrol - Protecting your Environment with Intelligence

ThreatPatrol is a powerful open-source SaaS tool that offers Blue Teams a wealth of information on potential threats, allowing them to gain situational awareness and perform threat hunting. The tool's flexibility is a significant advantage, as it can be hosted on the cloud or on an internal standalone machine, providing users with the convenience and customisation options they need.

Threat Actors

ThreatPatrol offers a comprehensive database of over 160 threat actor groups.

Feed Sources

ThreatPatrol also provides feeds from over 100+ different sources, allowing organisations to stay up-to-date with the latest attack methods and trends

Functionalities

Cyber Defenders can add, update, or degrade TTPs and IOCs for their network and map them to the MITRE Framework, which can be visualised on the dashboard in graph form, and generate reports for sharing with executive members.

TTPs

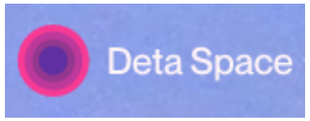
This information is regularly updated to ensure that users have access to the latest information on potential threats, providing insights into emerging threats and enabling proactive measures to prevent cyber-attacks.

Information Classification: General

Streamlit

Streamlit

Streamlit is an open-source Python library that enables developers to build intuitive, interactive, and visually appealing web applications for data exploration, visualisation, and machine learning, without the need for extensive web development expertise.



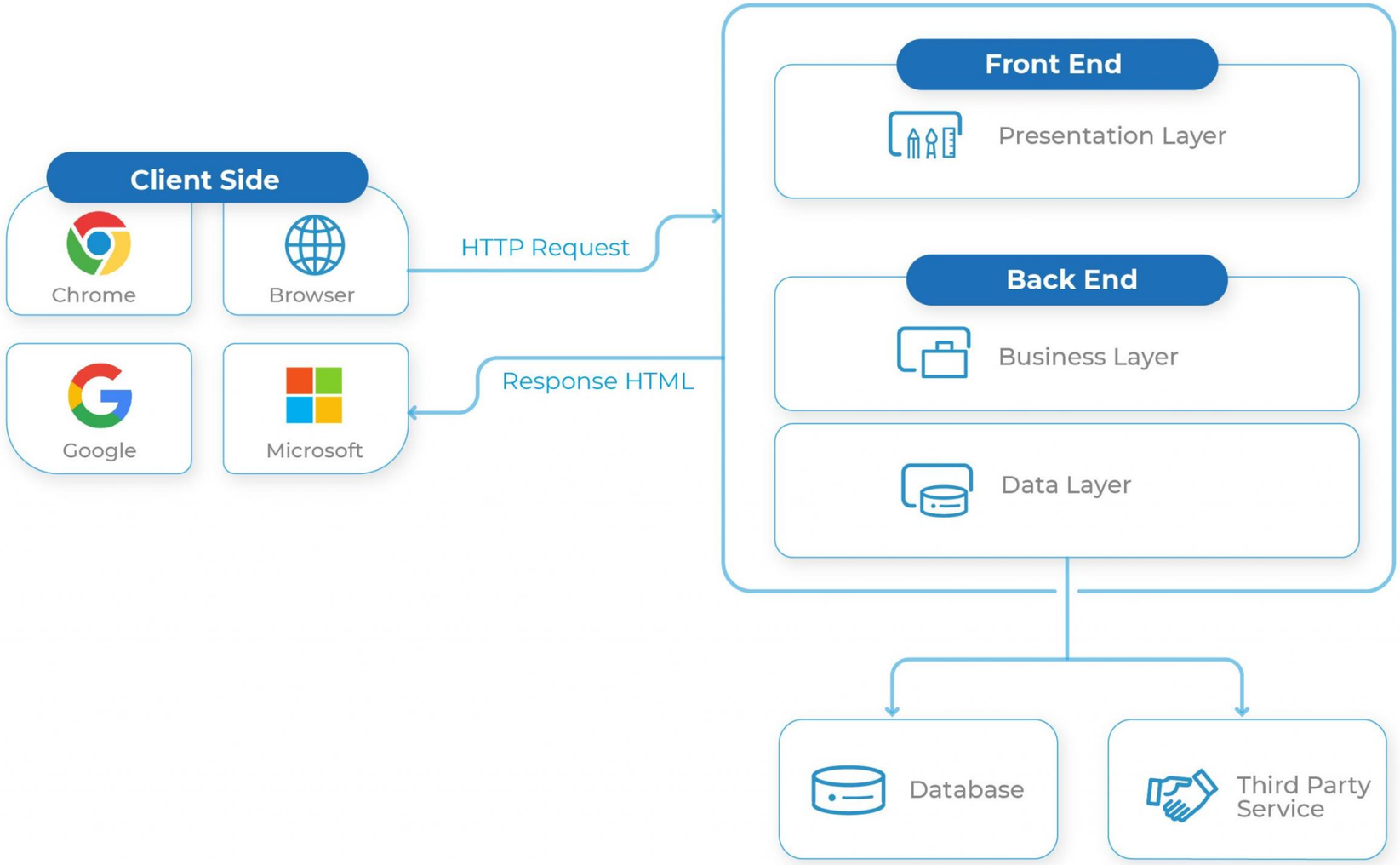
Deta

Deta is a cloud-based platform that simplifies data management tasks, providing developers with tools and infrastructure to easily store, process, and deploy data-intensive applications, accelerating development and deployment cycles.

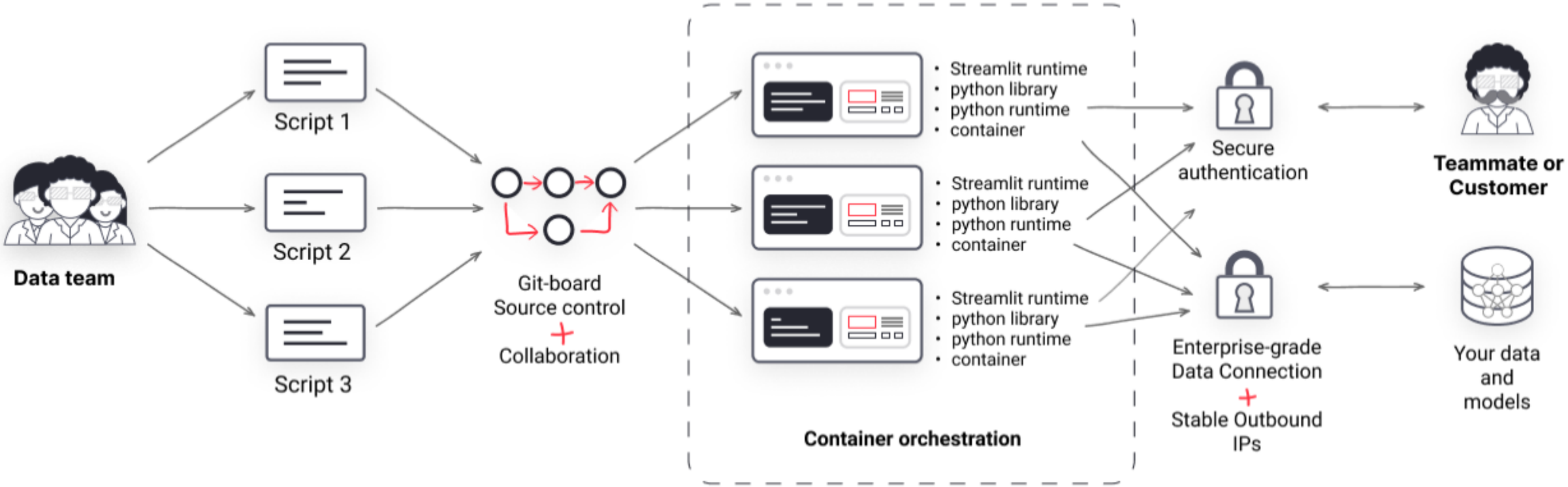
Docker

Docker is an open-source platform that allows developers to automate the deployment and management of applications using containerisation technology. It enables efficient and scalable software deployment, making it easier to package, distribute, and run applications across different environments. Docker simplifies the development process, enhances portability, and promotes resource optimisation, leading to faster and more reliable application delivery.

Information Classification: General



Information Classification: General



Information Classification: General

Information Classification: General

- Homepage
- Threat Feeds
- IOC Normalization
- Analysts Tasks
- MITRE ATTACK

Logout

ThreatPatrol By Viral Maniar

Threat Actor Groups

Select a threat actor group

APT28

Select a technique:

Junk Data

APT28

APT28, also known as Fancy Bear, is a sophisticated Russian cyber espionage group associated with various state-sponsored hacking activities.

Associated Groups | Recent News | Target Countries | TTPs | IOCs | Thre

- IRON TWILIGHT
- SNAKEMACKEREL
- Swallowtail
- Group 74
- Sednit
- Sofacy
- Pawn Storm
- Fancy Bear
- STRONTIUM
- Tsar Team
- Threat Group-4127
- TG-4127

Information Classification: General

APT28, also known as Fancy Bear, is a sophisticated Russian cyber espionage group associated with various state-sponsored hacking activities.

Associated Groups | Recent News | Target Countries | TTPs | IOCs | Thre

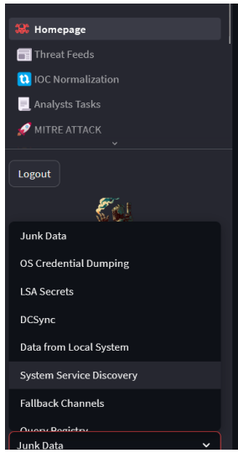
United States

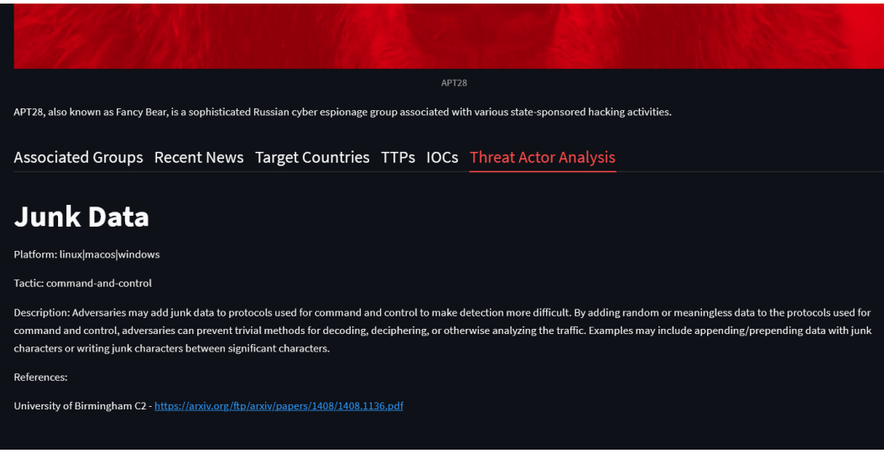
Canada

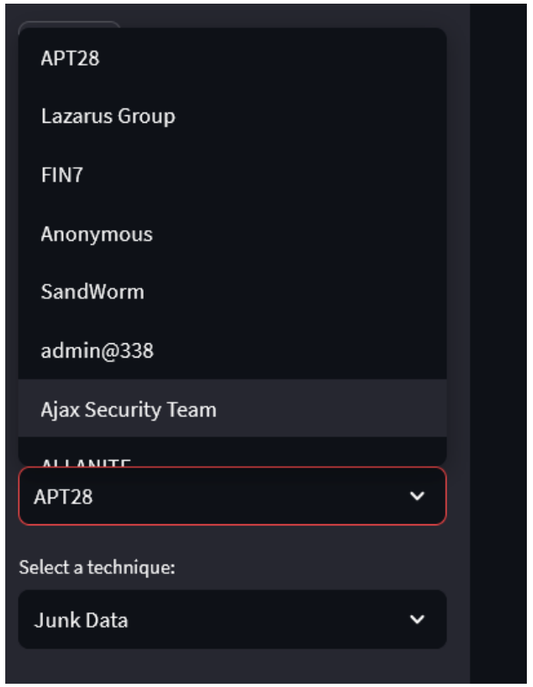
Australia

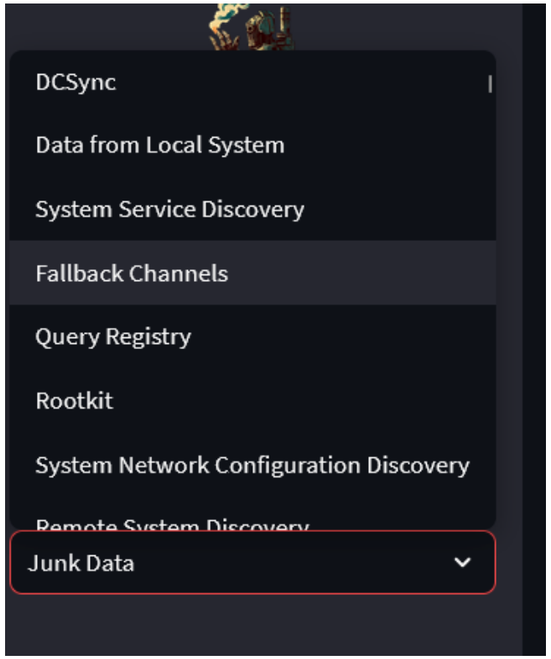
Germany

Japan









Information Classification: General

VARUTRA SM
An Infoshare Systems, Inc. Company

THN

KrebsonSecurity
In-depth security news and investigation

naked security

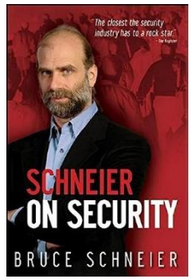
AKEYLESS

McAfee™

TechRepublic.

hackerone

BLEEPINGCOMPUTER



Graham Cluley

da vinci CYBERSECURITY
DaVinciCybersecurity.co.za

SOCRadar®
Your Eyes Beyond

COMPUTERWORLD

NIST

THE CYBER EXPRESS
By CYBLE

welivesecurity™

TREND MICRO

AT&T Cybersecurity

proofpoint®

Acunetix
by Invicti

UpGuard

Heimdal®

imperva

IDENTITYIQ

Quick Heal
Security Simplified

SEQRITE
Enterprise Cybersecurity Solutions by Quick Heal

PCI Security Standards Council

INFOSEC INSIGHTS
by SECTIGO Store

TrustArc

ZONEALARM
By Check Point

gt government technology

it governance

wallarm

secpod

CHEAP SSL
BEST PRICE SSL SHOP

SecureBlitz

CYBER DEFENSE magazine

SOC PRIME

CyberHoot

CyberTalk.org

BINARY DEFENSE

Information Classification: General

Homepage
Threat Feeds
IOC Normalization
Analysts Tasks
MITRE ATTACK
Logout

ThreatPatrol By Viral Maniar

Choose the RSS feed URL:

https://www.welivesecurity.com/f...

WeLiveSecurity

Last updated on: Thu, 13 Jul 2023 15:48:44 +0000

The danger within: 5 steps you can take to combat insider threats

Published on: Thu, 13 Jul 2023 09:30:45 +0000

Some threats may be closer than you think. Are security risks that originate from your own trusted employees on your radar? The post <a href="https://www.w
/2023/07/13/danger-within-5-steps-combat-insider-threats/" rel="nofollow">The danger within: 5 steps you can take to combat insider threats appeared first on <a
href="https://www.welivesecurity.com/" rel="nofollow">WeLiveSecurity

ESET Research Podcast: Finding the mythical BlackLotus bootkit

Published on: Wed, 12 Jul 2023 09:30:13 +0000

A story of how an analysis of a supposed game cheat turned into the discovery of a powerful UEFI threat The post <a href="https://www.welivesecurity.com/20
research-podcast-finding-mythical-blacklotus-bootkit/" rel="nofollow">ESET Research Podcast: Finding the mythical BlackLotus bootkit appeared first on <a
href="https://www.welivesecurity.com/" rel="nofollow">WeLiveSecurity

Information Classification: General

- Homepage
- Threat Feeds
- IOC Normalization
- Analysts Tasks
- MITRE ATTACK

Logout

ThreatPatrol By Viral Maniar

STIX Object Viewer

Select a page

IOC

IOC Normalization

Add IOC

IOC Type

IP Address

IOC Value

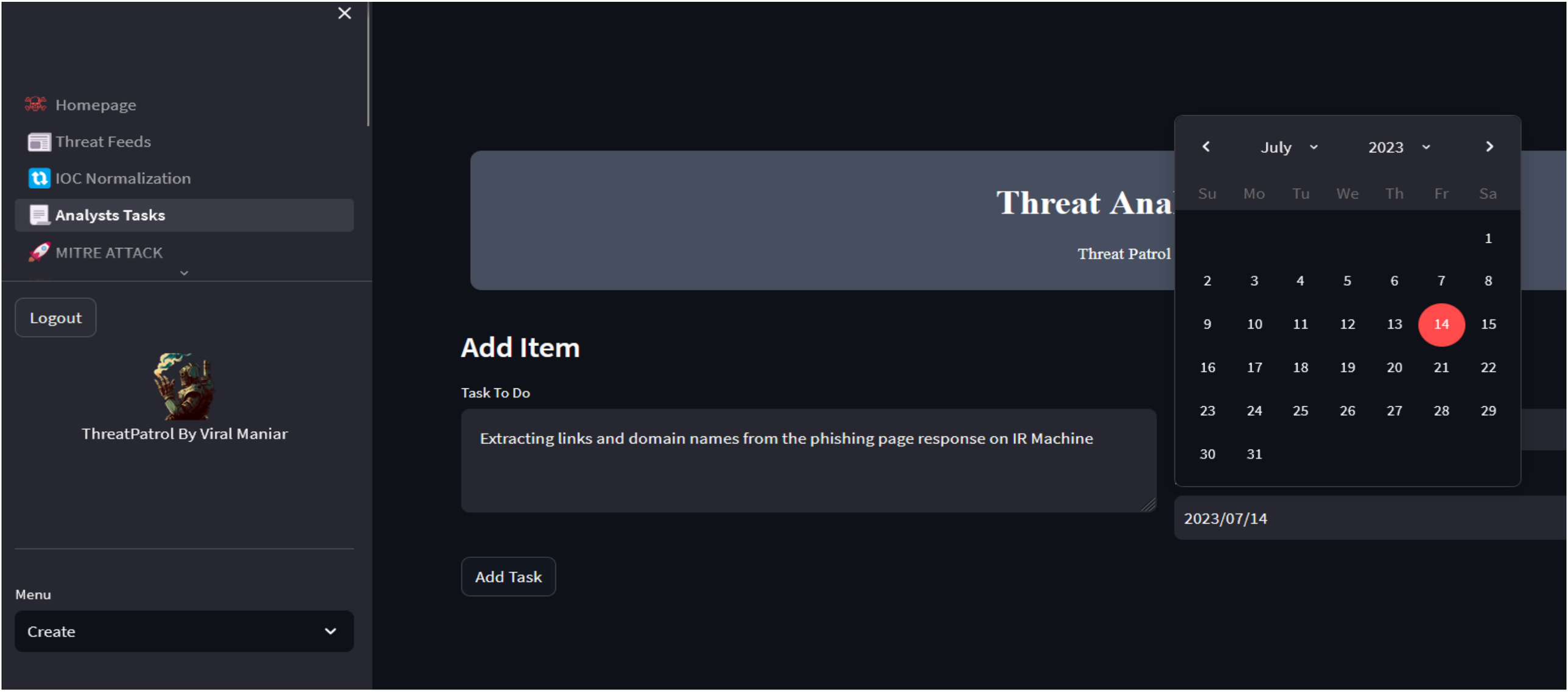
Add

Existing IOCs

Fetch IOCs from NIST

CVE ID

Fetch



Information Classification: General

- Homepage
- Threat Feeds
- IOC Normalization
- Analysts Tasks
- MITRE ATTACK

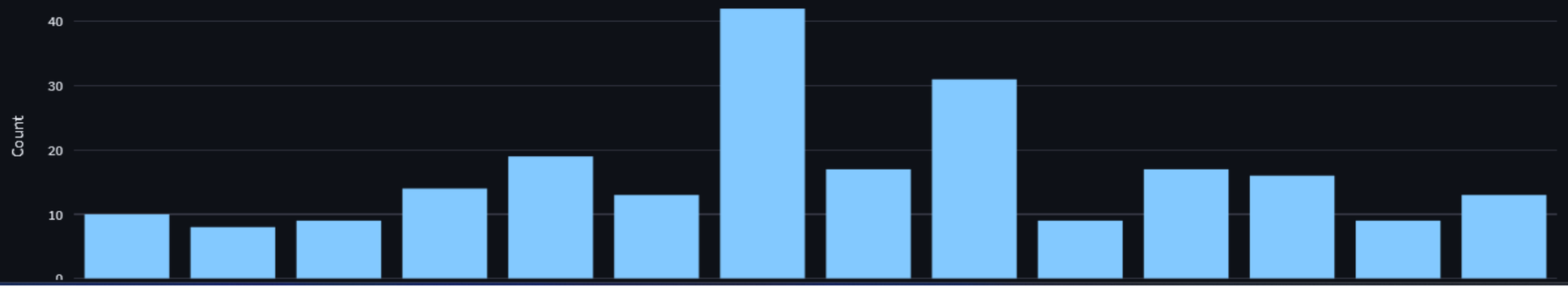
Select Column

Reconnaissance

Filter Value

	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation
0	Active Scanning	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation	Abuse Elevation Cor
1	Gather Victim Host Information	Acquire Infrastructure	Exploit Public-Facing Application	Command and Scripting Interpreter	BITS Jobs	Access Token Manip
2	Gather Victim Identity Information	Compromise Accounts	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution	Boot or Logon Autos
3	Gather Victim Network Information	Compromise Infrastructure	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts	Boot or Logon Initia
4	Gather Victim Org Information	Develop Capabilities	Phishing	Exploitation for Client Execution	Browser Extensions	Create or Modify Sys
5	Phishing for Information	Establish Accounts	Replication Through Removable Media	Inter-Process Communication	Compromise Client Software Binary	Domain Policy Modi
6	Search Closed Sources	Obtain Capabilities	Supply Chain Compromise	Native API	Create Account	Escape to Host
7	Search Open Technical Databases	Stage Capabilities	Trusted Relationship	Scheduled Task/Job	Create or Modify System Process	Event Triggered Exe
8	Search Open Websites/Domains	None	Valid Accounts	Serverless Execution	Event Triggered Execution	Exploitation for Priv
9	Search Victim-Owned Websites	None	None	Shared Modules	External Remote Services	Hijack Execution Flo

Total Count of Items in Each Column



Information Classification: General

- Homepage
- Threat Feeds
- IOC Normalization
- Analysts Tasks
- MITRE ATTACK
- **Dashboard**
- fanger
- Scraper
- Living off the Land Drivers
- File Extension
- Living Off The Land Binaries
- Threat Canvas

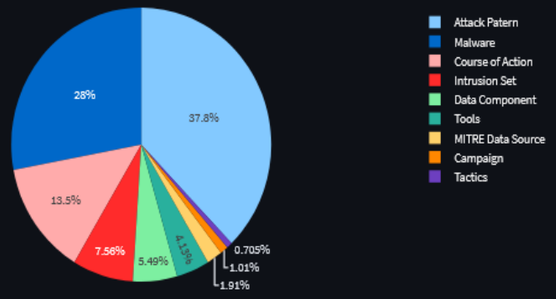
2	Platforms	The Computing Environment where offensive behaviors occur
3	Procedures	The Unique Implementation detail of an offensive behavior
4	Tactics	The Goals an adversary is seeking throughout the attack lifecycle
5	Techniques	The Offensive Behaviors conducted by an adversary
6	Malware	The Known Hostile Programs designed to cause harm
7	Tools	The Legit Programs used to cause harm

	Summary	Count
0	MITRE Data Source	38
1	Tools	82
2	Tactics	14
3	Data Component	109
4	Malware	555
5	Intrusion Set	150
6	Course of Action	267
7	Campaign	20
8	Attack Patern	750

Select chart type:

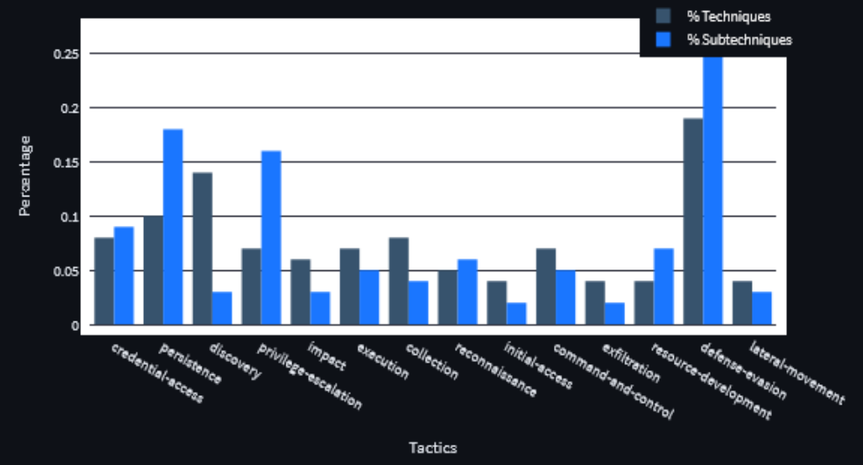
Pie Chart

Data Distribution



- Homepage
- Threat Feeds
- IOC Normalization
- Analysts Tasks
- MITRE ATTACK
- **Dashboard**
- fanger
- Scraper
- Living off the Land Drivers
- File Extension
- Living Off The Land Binaries
- Threat Canvas

Tactics Split Bar Chart



	INDEX	PLATFORMS	TECHNIQUES	SUBTECHNIQUES	% TECHNIQUES	% SUBTECHNIQUES	TOTAL
0	1	containers	32	21	0.14	0.04	53
1	2	azure-ad	26	38	0.12	0.07	64
2	3	pre	18	70	0.08	0.13	88
3	4	saas	35	42	0.16	0.08	77
4	5	linux	160	210	0.7	0.38	370
5	6	office-365	40	51	0.18	0.1	91
6	7	network	50	33	0.22	0.06	83
7	8	macos	164	220	0.71	0.4	384
8	9	google-workspace	31	43	0.14	0.08	74
9	10	iaas	54	50	0.24	0.09	104

Information Classification: General

- Homepage
- Threat Feeds
- IOC Normalization
- Analysts Tasks
- MITRE ATTACK
- Dashboard
- fanger
- Scraper

Logout

ThreatPatrol By Viral Maniar

IOC Fanging

Fang/Defang IOCs

Threat Patrol - BlackHat

Enter IOCs (URLs or IP addresses)

Paste your IOCs here

```
191.70.69.31
60.182.137.135
111.159.171.57
238.4.45.97
10.76.24.193
139.96.225.16
34.162.75.75
14.171.55.70
135.205.85.130
37.26.161.145
208.175.191.239
102.203.246.250
11.67.1.85
27.135.193.228
84.12.11.86
77.22.253.216
207.199.67.73
148.91.46.132
231.231.111.8
21.147.160.73
159.120.212.248
164.51.222.116
135.136.151.241
158.117.3.37
33.147.157.194
```

Fanged IOCs

Fang-Defang

Fanged IOCs

```
191[.]70[.]69[.]31
60[.]182[.]137[.]135
111[.]159[.]171[.]57
238[.]4[.]45[.]97
10[.]76[.]24[.]193
139[.]96[.]225[.]16
34[.]162[.]75[.]75
14[.]171[.]55[.]70
135[.]205[.]85[.]130
37[.]26[.]161[.]145
208[.]175[.]191[.]239
102[.]203[.]246[.]250
11[.]67[.]1[.]85
27[.]135[.]193[.]228
84[.]12[.]11[.]86
77[.]22[.]253[.]216
207[.]199[.]67[.]73
148[.]91[.]46[.]132
231[.]231[.]111[.]8
21[.]147[.]160[.]73
159[.]120[.]212[.]248
164[.]51[.]222[.]116
135[.]136[.]151[.]241
158[.]117[.]3[.]37
33[.]147[.]157[.]194
```

Information Classification: General

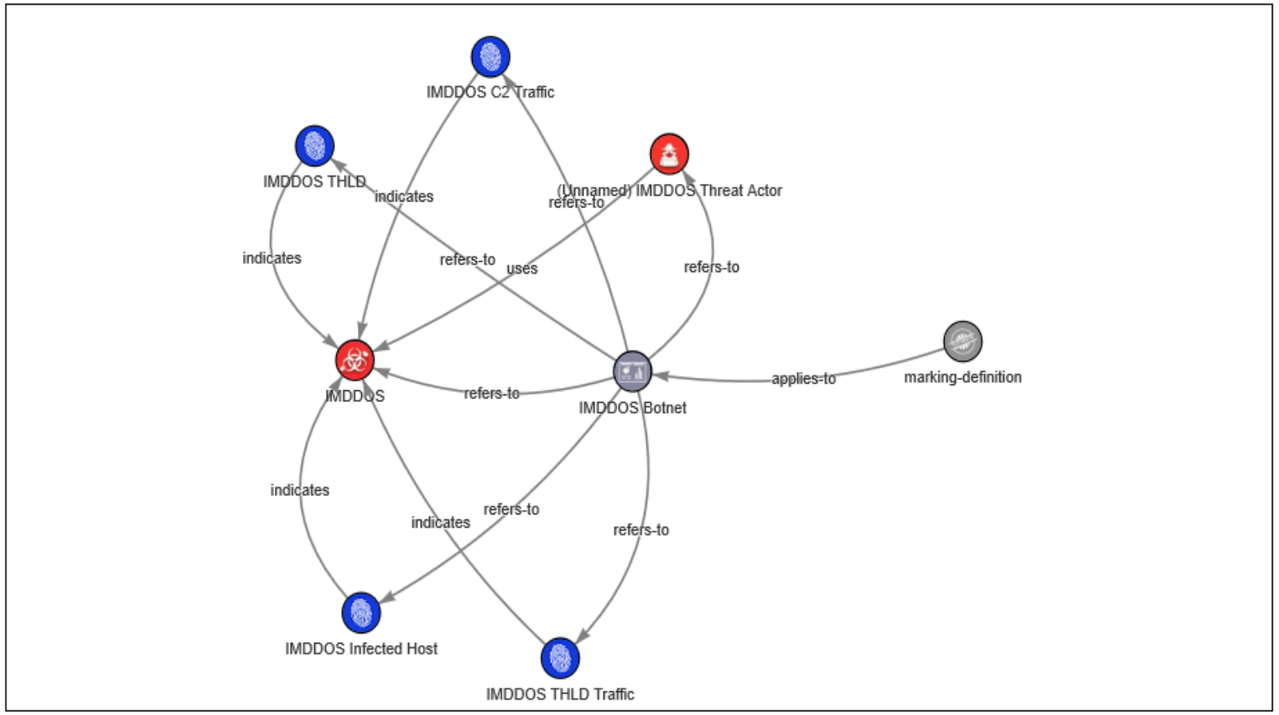
- Homepage
- Threat Feeds
- IOC Normalization
- Analysts Tasks
- MITRE ATTACK
- Dashboard
- fanger
- Scraper
- Living off the Land Drivers
- File Extension
- Living Off The Land Binaries
- Threat Canvas

Logout

ThreatPatrol By Viral Maniar

STIX Visualisation

STIX Visualizer stixvis.json



Selected Node

Linked Nodes

Incoming Edges:

Outgoing Edges:

Legend

- Marking-definition
- Report
- Malware
- Threat-actor
- Indicator

Integration with enrichment sources, enhancing data quality and providing comprehensive insights to optimise decision-making processes.

Enrichment Sources

Q4 2023

This will be streamlining processes and enabling efficient response to threats through intelligent automation.

Workflow Design for Actions

Q3 2024

A sophisticated scoring mechanism for IOCs to effectively prioritise and mitigate threats based on their severity and relevance.

Scoring Mechanism

Q2 2024

I will focus on the uplift of the Threat Canvas, empowering users with a comprehensive framework for threat modeling and risk assessment to enhance their security posture through visualisation.

Uplift of Threat Canvas

Q4 2024

Information Classification: General

THREAT PATROL
BLUE TEAM

THANK YOU

@ManiarViral

UniSuper

Information Classification: General