CYBER THREAT INTELLIGENCE

DR DEEPAK KUMAR

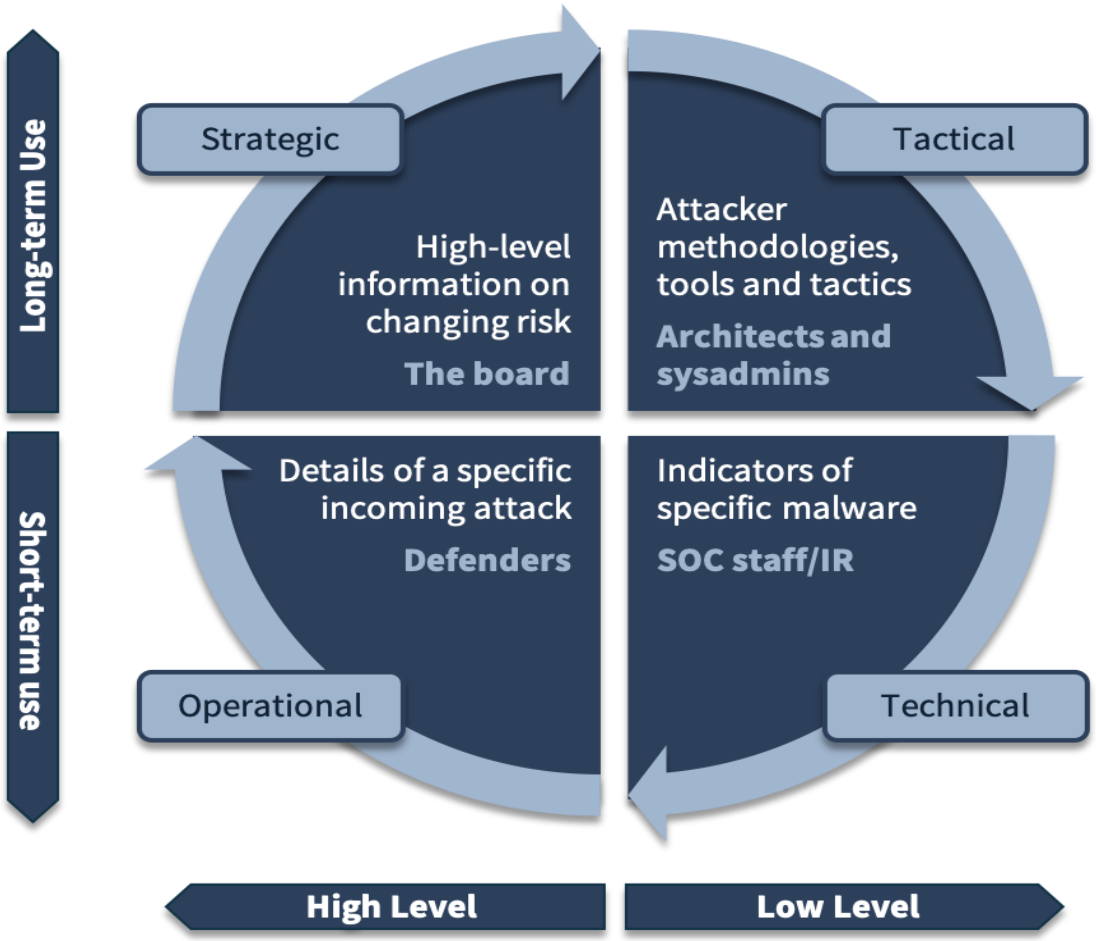
DATA AND CYBER INTELLIGENCE

Threat intelligence is evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets.

– Gartner

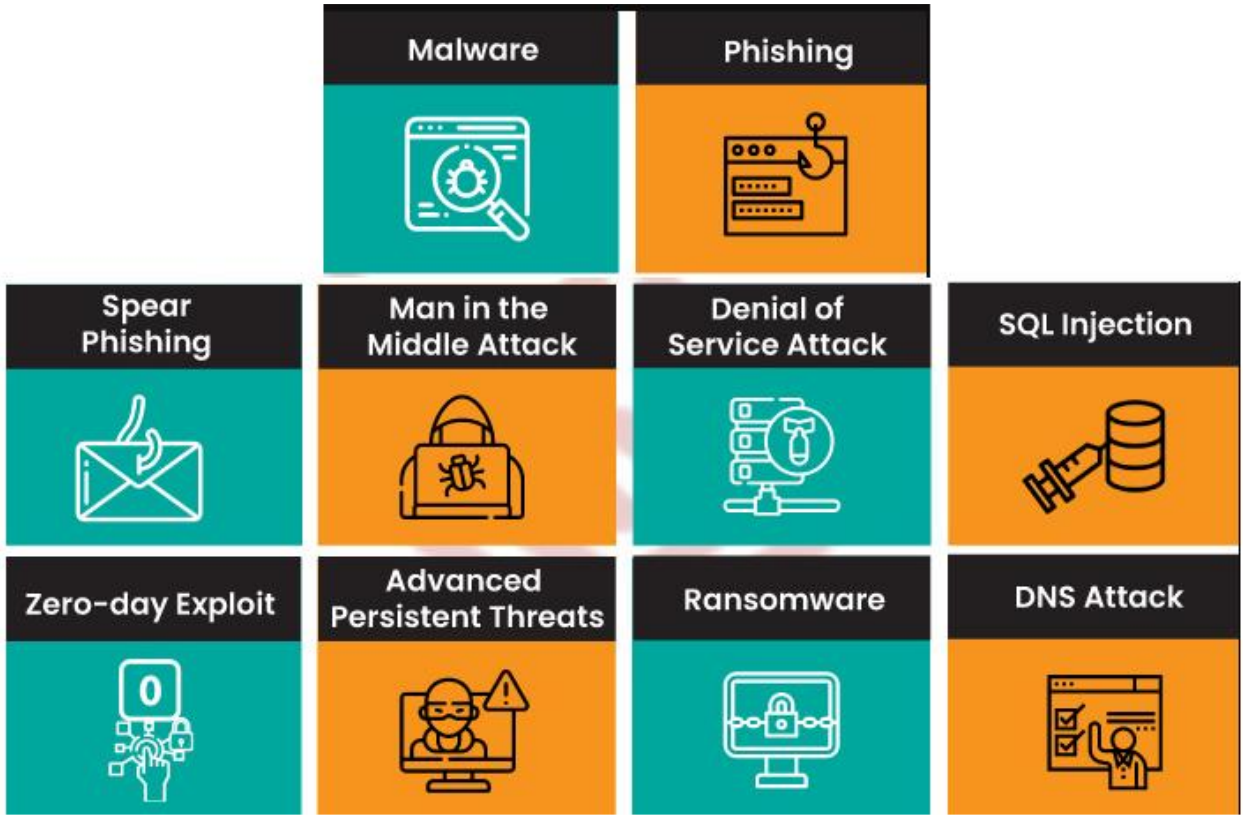
TYPES OF THREAT INTELLIGENCE

Threat intelligence dissent in terms of information assortment, knowledge analysis, intelligence consumption.

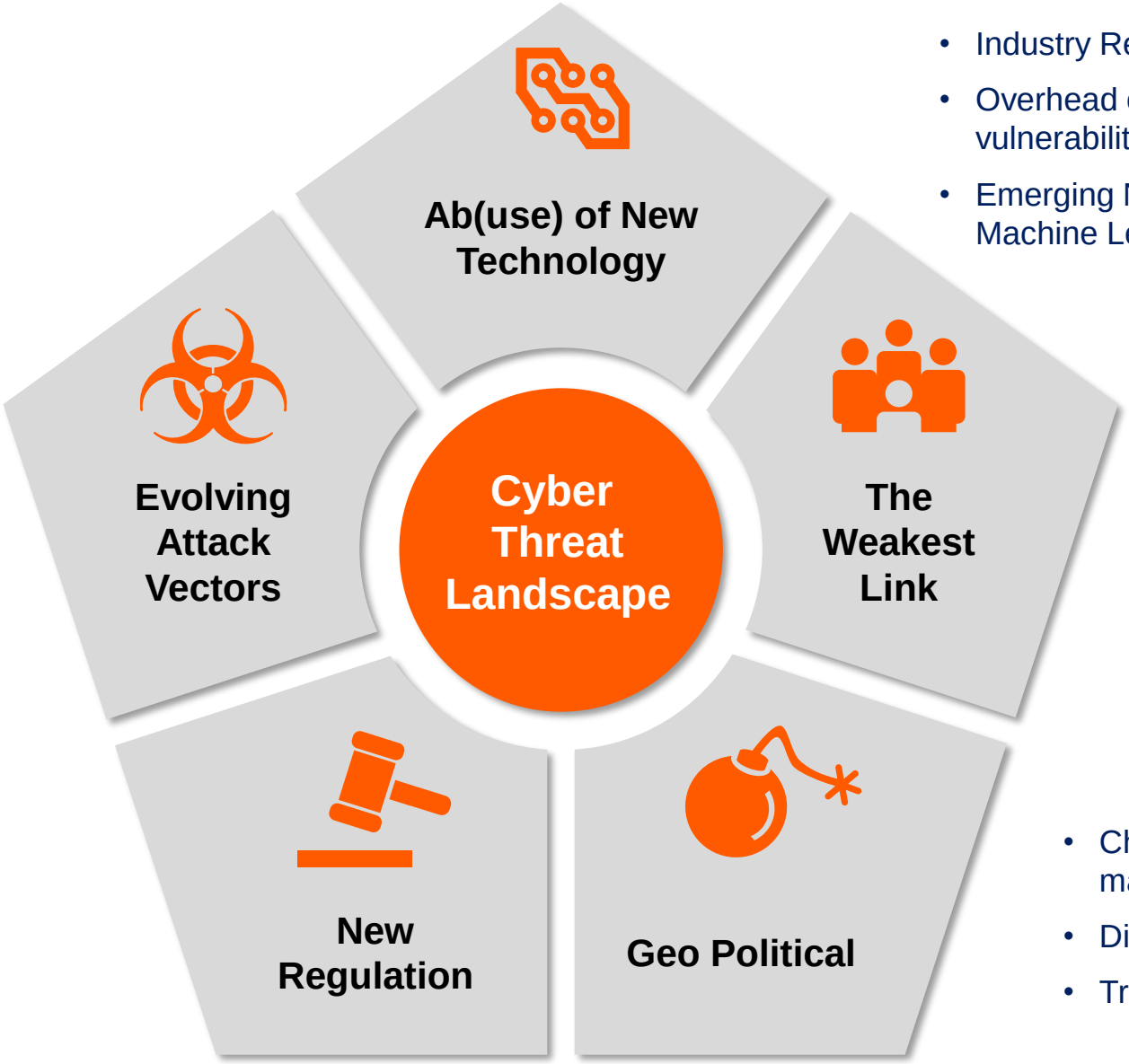


CYBER THREATS

Any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information.



THE CYBER THREAT LANDSCAPE AND ATTACK SURFACE



- Industry Reliance on the Cloud
- Overhead of constantly patching critical software vulnerabilities
- Emerging New Technologies Mature – AI and Machine Learning

- Rise in Ransomware & DDOS
- Evolving Zero-Day APTs
- Advanced ‘Undetectable’ Malware
- Larger Data Breaches
- (Possible) Targeting of Critical Infrastructure

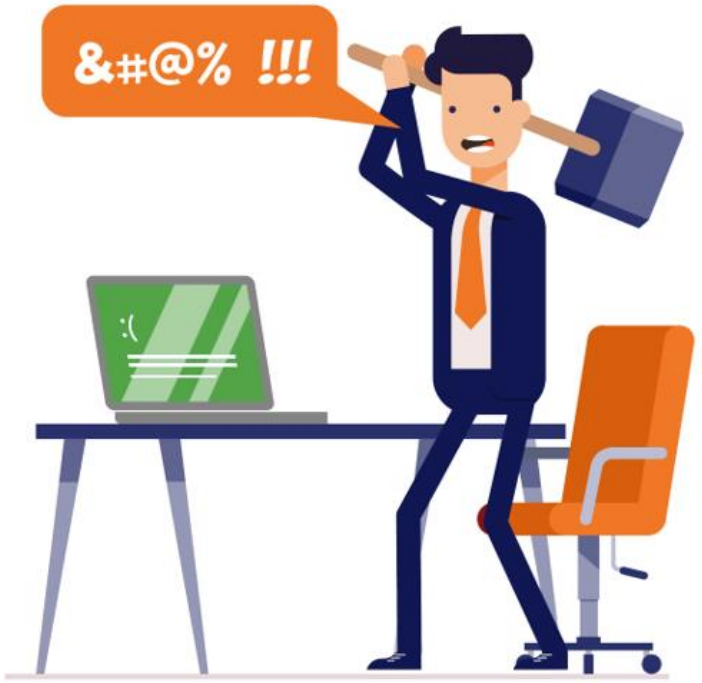
- Endless (Spear) Phishing
- Rise in Insider Threats – The Enemy Within
- Skills Shortage

- Cyber Resilience
- Fines for PII Breaches
- Crypto Currency Regulation

- Cheap and readily available malicious services
- Disguised campaign attack
- Tracking of adversaries

Bad Guys

CYBER THREATS COME FROM



Cyber threats come from numerous threat actors including:

- Hostile Nation-States
- Terrorist Groups
- Organized Crime Organizations
- Corporate Spies
- Hacktivists
- Disgruntled Insiders
- Hackers
- Natural Disasters
- Accidental Actions of Authorized Users

PHASES OF CTI LIFECYCLE

A fundamental framework for all fraud, physical, and cybersecurity programs whether mature and sophisticated in their operations, or merely aspiring.

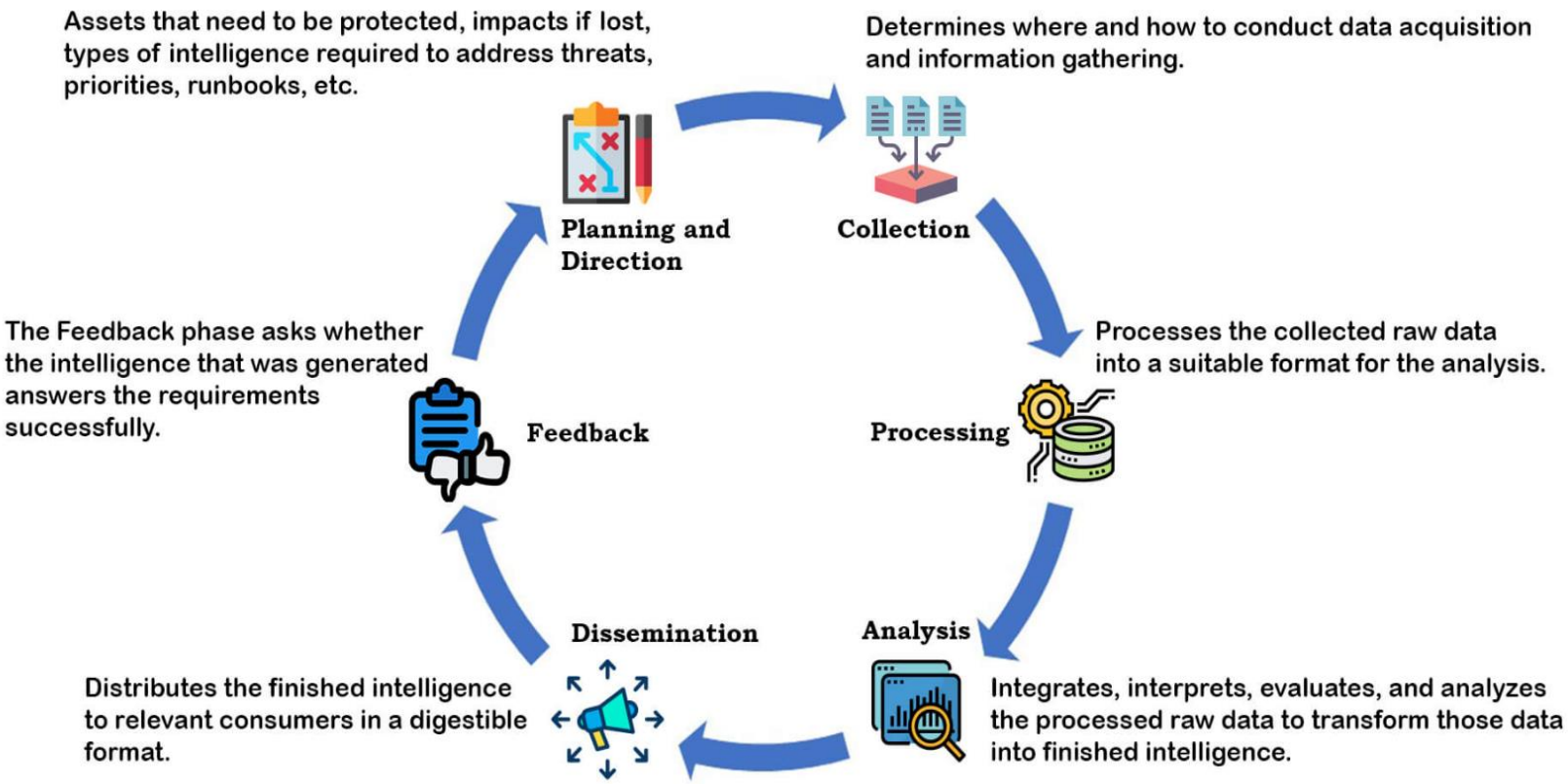


Image Source: https://hackersterminal.com/

IMPORTANCE OF CTI

Threat intelligence is actionable - it's timely, provides context, and is able to be understood by the people in charge of making decisions

Boosts the organization's and Critical National Infrastructure (CNI) cyber defense capabilities

Predictive analysis & enable better incident prioritization

Speeds up incident investigations, analyses and remediation's

Leverages key insights and context to prioritize vulnerabilities

Strengthen internal alerts and Policies

Topline Metrics

Overall more efficient IT security teams

32%

3-year ROI

284%

To payback

4 Months

Security Operational Efficiencies

Less staff time spent compiling security reports

34%

Earlier identification of threats

10x

Faster resolution of security threats

63%

Risk Reduction

22%

More security threats identified before impact

86%

Reduction in unplanned downtime

$1M

Potential penalties/fines per breach avoided

ATTRIBUTION

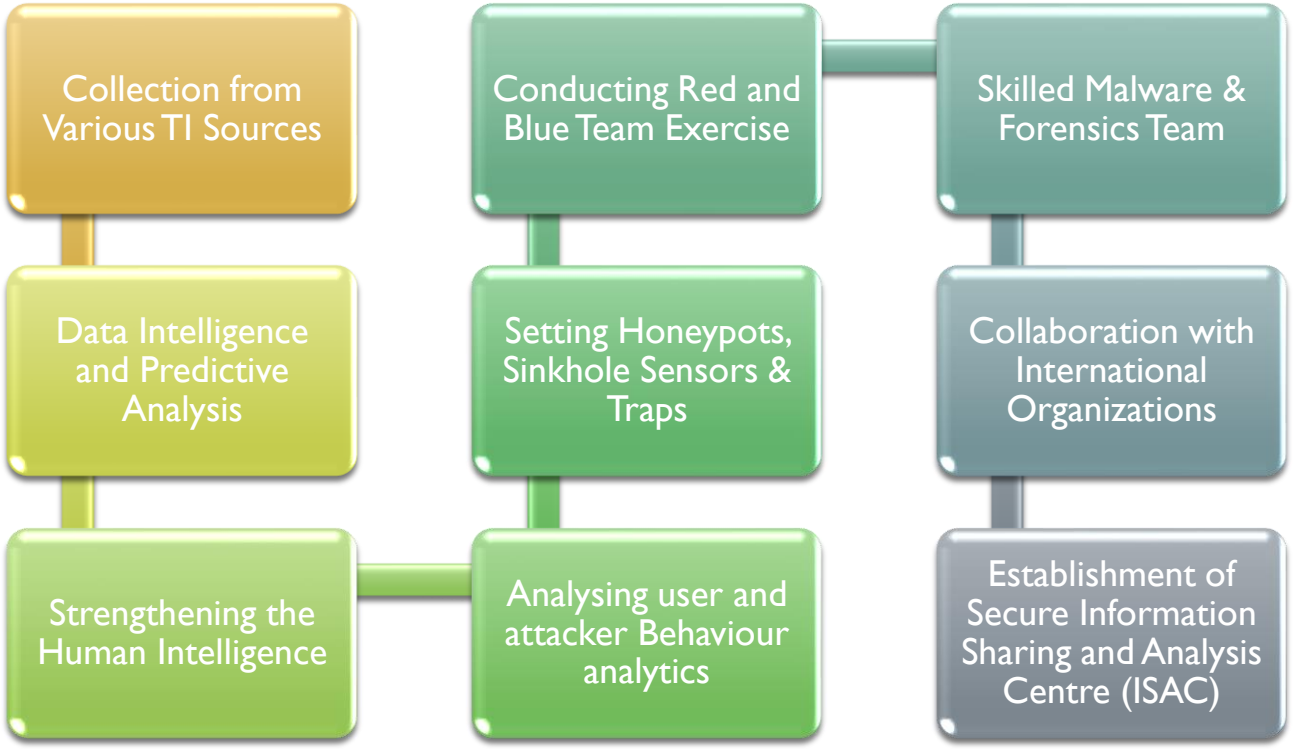
Behind every attack is a "who," "why," and "how."

The "**who**" is called attribution. The "**why**" is called motivation or intent. The "**how**" is made up of the TTPs the threat actor employs.

FUTURISTIC CYBER THREAT IDENTIFICATION

When it comes to detecting and mitigating threats, speed is crucial. Security programs must be able to detect threats quickly and efficiently so attackers don't have enough time to root around in sensitive data.

There are several methods available in the defender's arsenal:



DR. D3PAK KUMAR (D3)
DIGITAL FORENSICS | CYBER INTELLIGENCE

CRITICAL INFORMATION INFRASTRUCTURES (CII)

Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy. Most commonly associated with the term are facilities for:

EDUCATION

WATER

DEFENCE

TELECOMMUNICATION

FINANCIAL

GOVERNMENT

HOSPITAL

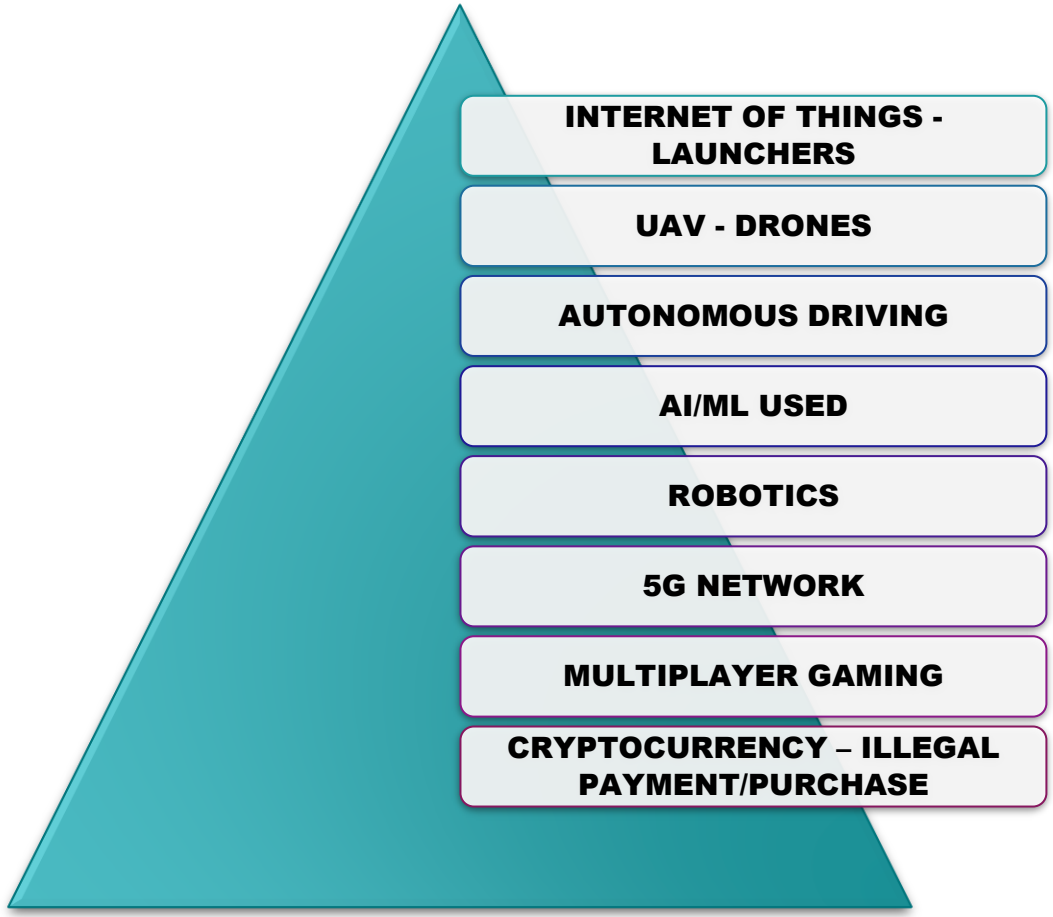
INDUSTRY

ENERGY

TRANSPORTATION

- Don’t assume that you’re not a target. Draw up battle plans. Learn from the mistakes of others
- Amateurs hack systems, professionals hack people. — **Bruce Schneier**

HYBRID ATTACK & TECHNOLOGIES



Debugging port open by default, allowing attackers to gain root access in the system


Critical traffic light system vulnerability could cause 'chaos' on the roads

Adam Bannister 09 June 2020 at 14:47 UTC
Updated: 09 June 2020 at 14:48 UTC

Vulnerabilities | Hardware | IoT

Open port gave green light to hardware hackers

A critical vulnerability in a traffic light controller deployed on roads across Europe could cause "sustained traffic chaos", according to a security expert from the firm that discovered the problem.

The hardware (Swarco CPU LS4000), which controls traffic lights at intersections, had a debugging port open by default, allowing attackers to gain root access without needing to bypass access controls.

The flaw – which has now been patched by Austrian manufacturer Swarco Traffic Systems – was exploitable remotely with modest technical skill, according to a US-CERT advisory issued last week.

- **Control subverting of traffic signals**
  - **breaking VIP security protocol chains**
  - **Create congestion to specific routes**
  - **altering police patrolling, etc.**
- **May utilize compromised traffic control system to attack associated system, for example CCTV**

DR. D3PAK KUMAR (D3)
DIGITAL FORENSICS | CYBER INTELLIGENCE

TRUST, TLP and IOC

- **To Defend your Data, You need Knowledge – Threat Intelligence**
- **Trust** is one of the most challenging attributes of cyber threat intelligence sharing.
- **Traffic Light Protocol (TLP)** is defined into four colors, namely, **WHITE** (no restrictions), GREEN (sharing with peers and partners, not publicly), AMBER (sharing only inside own organization on who-need-to-know basis), and RED (no sharing), and antitrust rules.
- **Indicator of Compromise (IOC)** in Cybercrime: Domain, URL, IP, Mobile Number, SMS Gateway, UPI Handle, Wallet, Bank Details, Profile Handle, Emails, Modus Operandi.....

DR. D3PAK KUMAR (D3)
DIGITAL FORENSICS | CYBER INTELLIGENCE

CLOUD ATTACK VECTOR ADVERSARIES

- Credential theft
- Vulnerability exploitation
- Abuse of cloud service providers
- Exploitation of misconfigured image containers
- Use of cloud services for hosting malware
- Command and control

Tier 1-
Collection of Threat Feeds

INPUT

Cyber Threat Intelligence

ANALYSIS

Malware & VAPT Lab
(Sandbox)

Static analysis

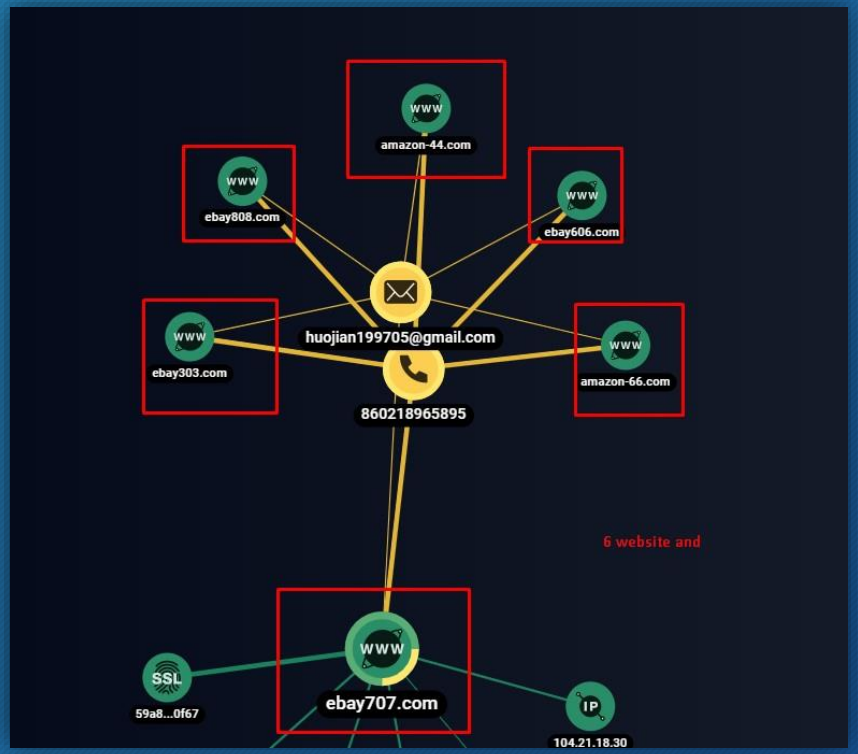
Dynamic analysis

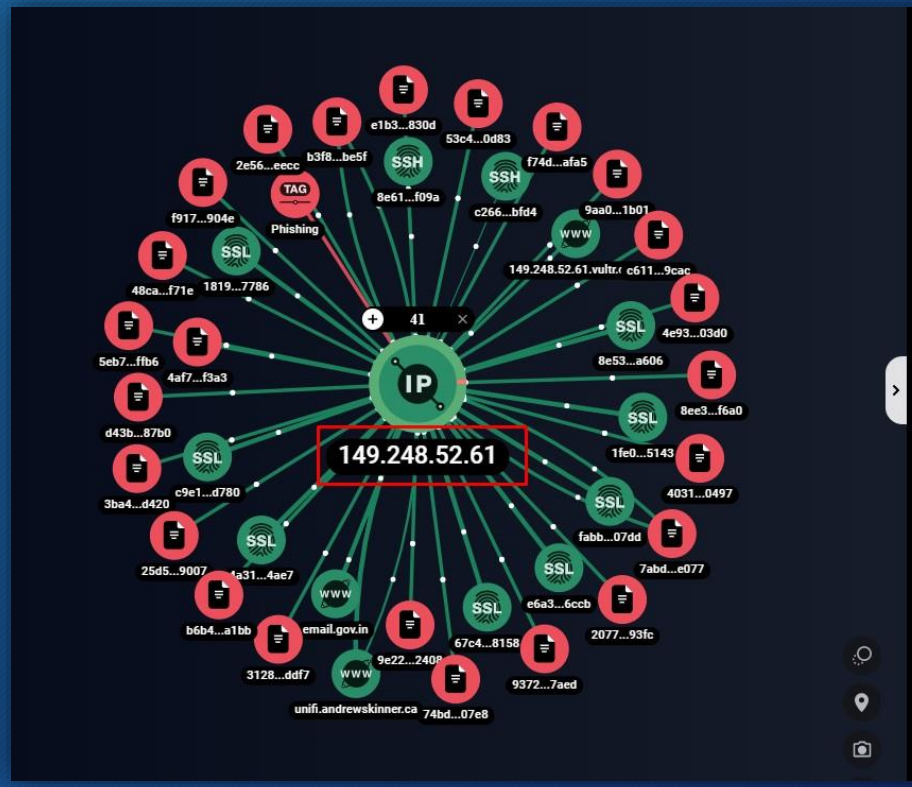
Memory analysis

OUTPUT

- Advisory
- Predictive Alerts
- Trends & Technology
- New Modus Operandi
- Reports

ATTRIBUTION





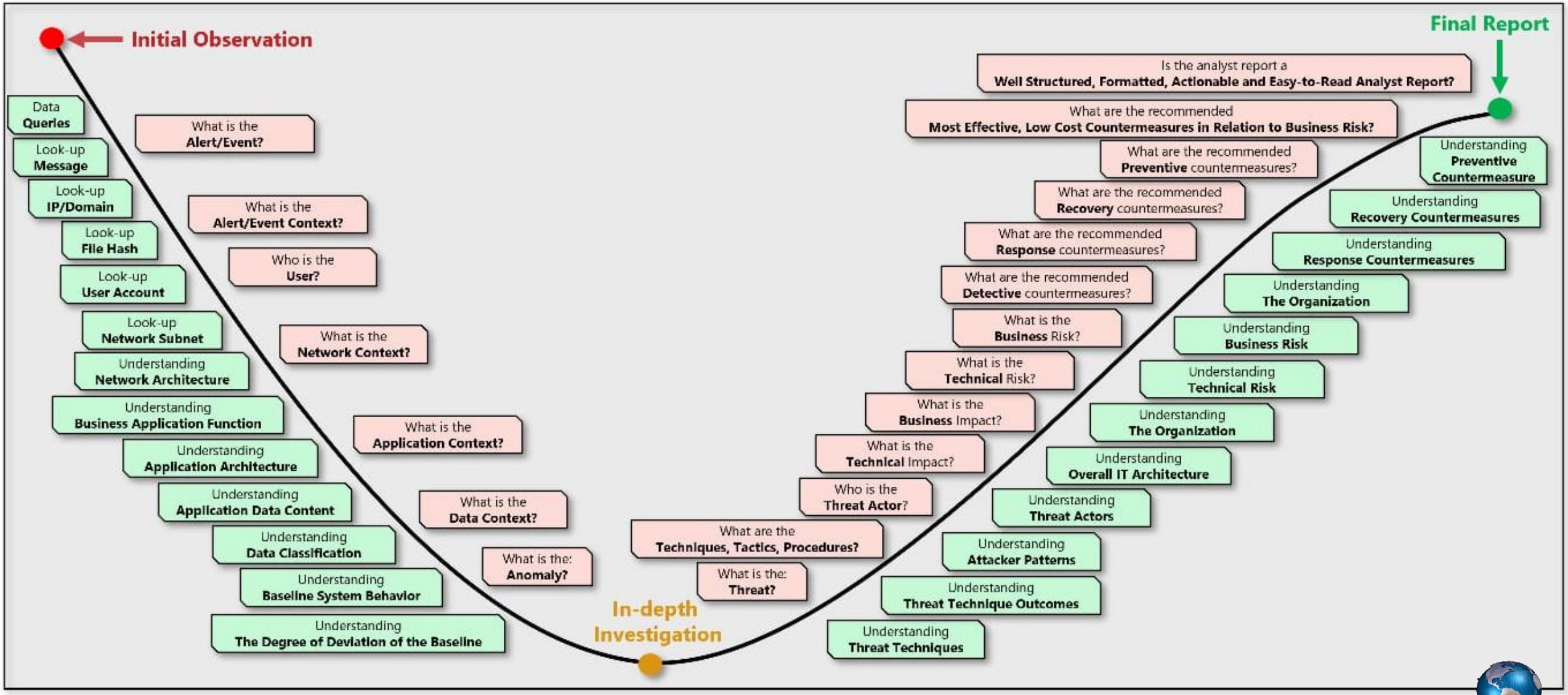
Active since 2021.03.30

inetnum	149.248.4.0 - 149.248.5.255
org-name	Vultr Holdings, LLC (VHL-60)
netname	NET-149-248-4-0-23
descr	https://rdap.arin.net/registry/ip/149.248.4.0
status	Reassigned
parent	CHOOP-1 (NET-149-248-0-0-1)
nethandle	NET-149-248-4-0-1
cidr	149.248.4.0/23
created	2018-08-29T00:00:00Z
last-modified	2018-08-29T00:00:00Z
type	inetnum

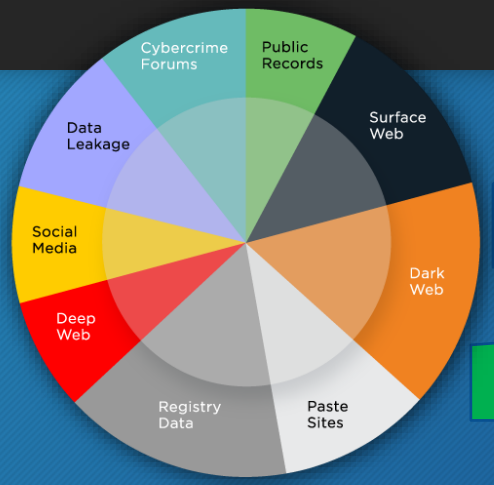
Active since 2021.02.27

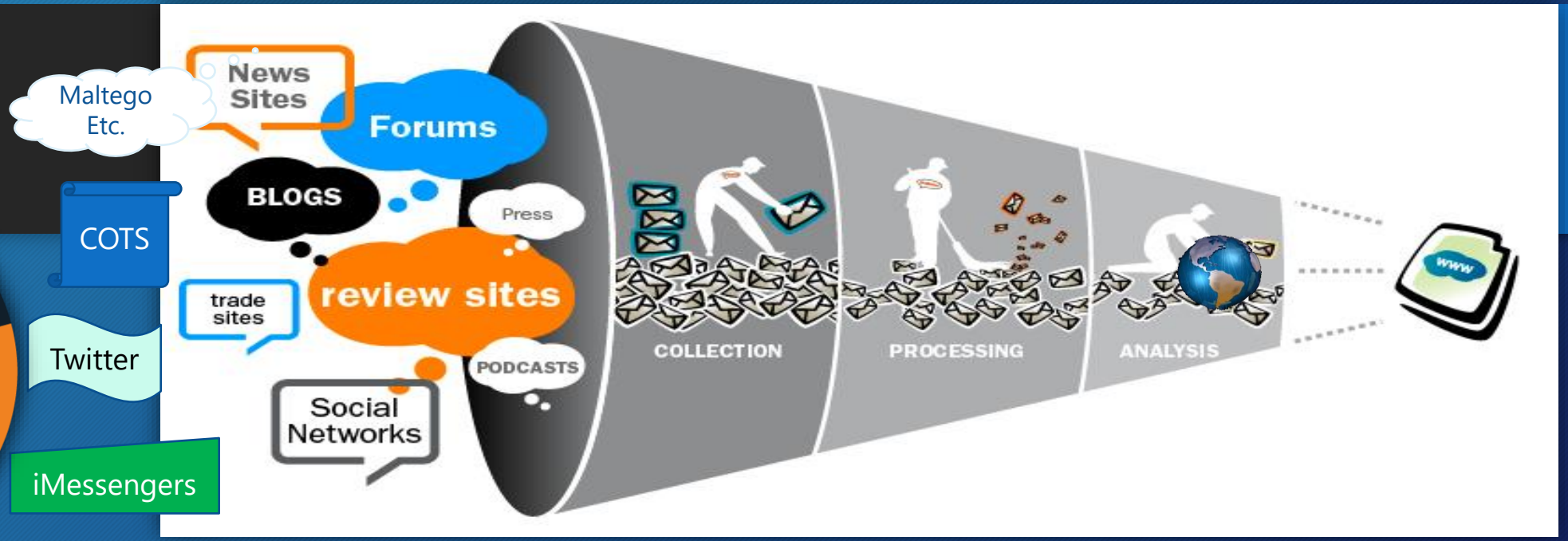
inetnum	149.248.0.0 - 149.248.63.255
org-name	The Constant Company, LLC (CHOOP-1)
netname	CHOOP-1
descr	https://rdap.arin.net/registry/ip/149.248.0.0
origin	AS20473
status	Direct Allocation
parent	NET149 (NET-149-0-0-0-0)
nethandle	NET-149-248-0-0-1
cidr	149.248.0.0/18
created	2018-07-03T00:00:00Z
last-modified	2018-08-28T00:00:00Z
type	inetnum

Source: Group IB Threat Intelligence


Initial Observation
Final Report
Data Queries
Look-up Message
Look-up IP/Domain
Look-up File Hash
Look-up User Account
Look-up Network Subnet
Understanding Network Architecture
Understanding Business Application Function
Understanding Application Architecture
Understanding Application Data Content
Understanding Data Classification
Understanding Baseline System Behavior
Understanding The Degree of Deviation of the Baseline
What is the Alert/Event?
What is the Alert/Event Context?
Who is the User?
What is the Network Context?
What is the Application Context?
What is the Data Context?
What is the: Anomaly?
What are the Techniques, Tactics, Procedures?
What is the: Threat?
In-depth Investigation
Who is the Threat Actor?
What is the Technical Impact?
What is the Business Impact?
What is the Technical Risk?
What is the Business Risk?
What are the recommended Detective countermeasures?
What are the recommended Response countermeasures?
What are the recommended Recovery countermeasures?
What are the recommended Preventive countermeasures?
What are the recommended Most Effective, Low Cost Countermeasures in Relation to Business Risk?
Is the analyst report a Well Structured, Formatted, Actionable and Easy-to-Read Analyst Report?
Understanding Threat Techniques
Understanding Threat Technique Outcomes
Understanding Attacker Patterns
Understanding Threat Actors
Understanding Overall IT Architecture
Understanding The Organization
Understanding Technical Risk
Understanding Business Risk
Understanding The Organization
Understanding Response Countermeasures
Understanding Recovery Countermeasures
Understanding Preventive Countermeasure

WEBINT





COLLECTION

Gather **actionable insights** in raw form concerning to Subject, etc.

PROCESS

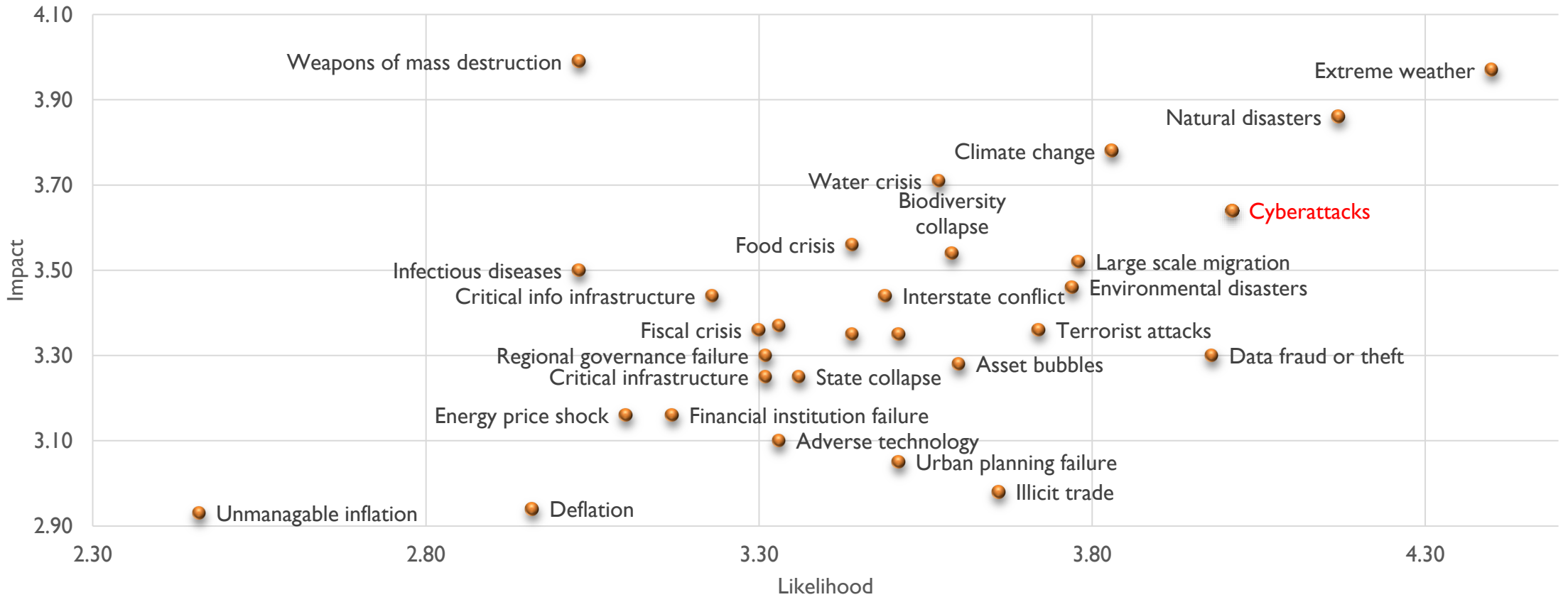
There are three main steps in analysing **web media**:

- **Data** identification,
- **Data** analysis, and
- Information **interpretation**.

OUTPUT

- Disseminate to Concern
- Investigation
- Forensics

THE BIG PICTURE - WORLD ECONOMIC FORUM RANKS 'CYBERATTACKS' AS A TOP GLOBAL RISK



Source: 2018 WEF survey spanning 684 respondents which assessed [likelihood] and [impact] of each risk on a scale of 1 to 5 [very unlikely / minimal impact] to [very likely / catastrophic]

CYBER KILL CHAIN

- **Task**: Identify the Attackers' Step by Step Process
- **Goal**: Disrupting Attackers' operations

Recon

- Motivation
- Preparation
- SE
- OSINT

MITRE ATT&CK:
- Active Scanning
- Passive Scanning
- Determine Domain & IP Address Space
- Analyze Third-Party IT Footprint

Weaponise

- Configuration
- Packaging
- Powershell
- Add

MITRE ATT&CK:
- Malware
- Scripting
- Service Execution

Delivery

- Mechanism of Delivery
- Infection Vector
- Phishing

MITRE ATT&CK:
- Spearphishing Attachment/Link
- Exploit Public-Facing Application
- Supply Chain Compromise

Exploitation

- Technical or human?
- Applications affected
- Method & Characteristics

MITRE ATT&CK:
- Local Job Scheduling
- Scripting
- Rundll32

Installation

- Persistence
- Characteristics of change
- Self0signed Driver

MITRE ATT&CK:
- Application Shimming
- Hooking
- Login Items

C2

- Communication between victim & adversary
- VPN

MITRE ATT&CK:
- Data Obfuscation
- Domain Fronting
- Web Service

Actions & Objectives

- What the adversary does when they have control of the system
- Data Exfil
- APT

MITRE ATT&CK:
- Email Collection
- Data from Local System/Network Share
- Surveillance

CTI SOURCES AND FEEDS

AlienVault Open Threat Exchange

Cisco Talos Intelligence

Group IB

Recorded Future

Department of Homeland Security (DHS) CISA

SANS Internet Storm Center

Google Alerts

Virustotal

MISP

BlueLive

ThreatConnect

Note: Some of the CTI tools and services are mentioned. These are not for endorsement purposes.

Feeds are just the raw data on threats; an analyst extracts the intelligence from them for creating reports

Monitoring and collection of security data on Indicator of compromise (IoCs e.g. IP addresses, Hash Value, Domain name etc. from various sources.

Purpose to identify the **uncommon activity and malicious domains** and **IP addresses**