Threat Intelligence and Dark web Monitoring

Overview of Threat Intel

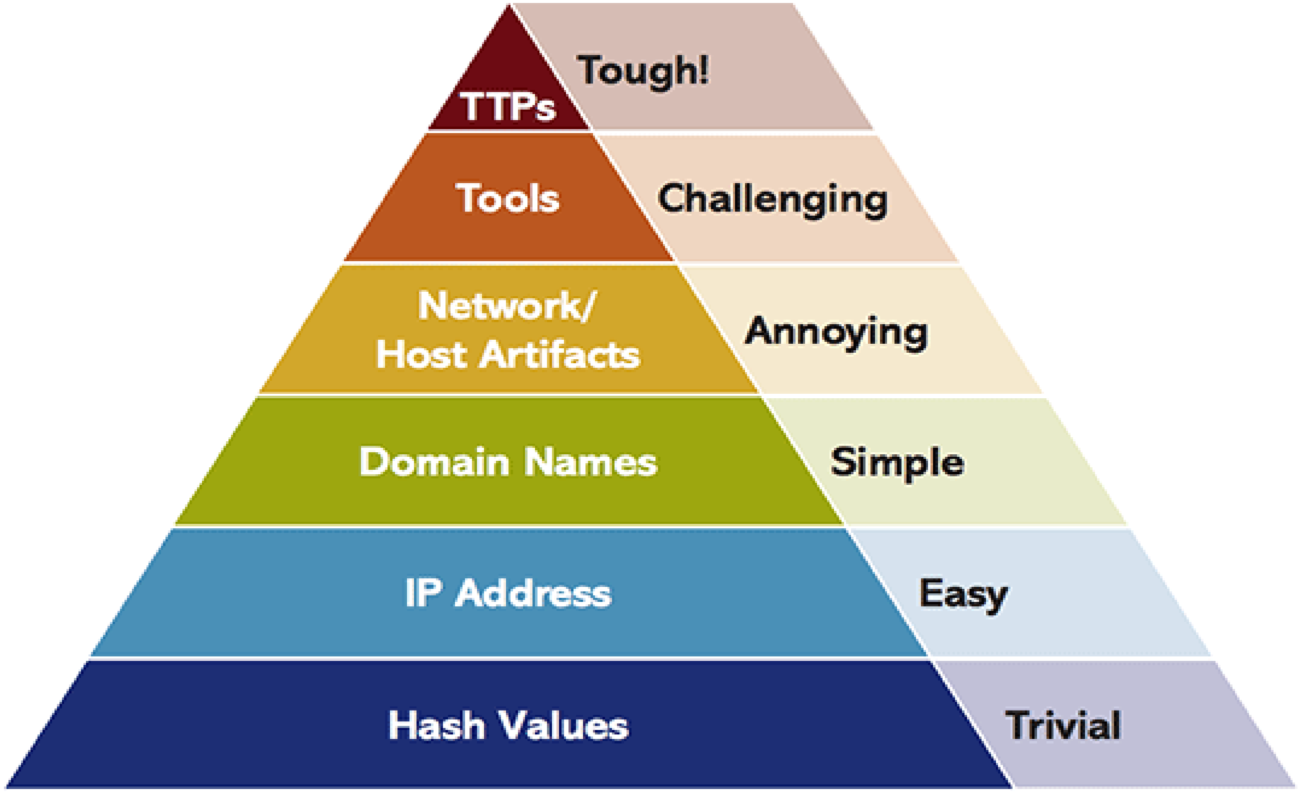
- It is a Growing Field
- High adoption in many organizations
- This information is used to prepare, prevent, and identify the cyber threats looking to take advantage of valuable resources.
- Overall ,threat intelligence is an important investment for many organizations.

Types of Threat Intel

- **Strategic Intel** - Broader trends typically meant for a non-technical audience such as It's intended to inform high-level decisions made by executives and other decision makers at an organization.
- **Operational Intel** - Technical details about specific attacks and campaigns
- **Tactical Intel** - Outlines of the tactics, techniques, and procedures (TTPs) of threat actors for a more technical audience

Pyramid of Pain

It represents the types of indicators that the analyst must look out to detect the activities of an adversary.

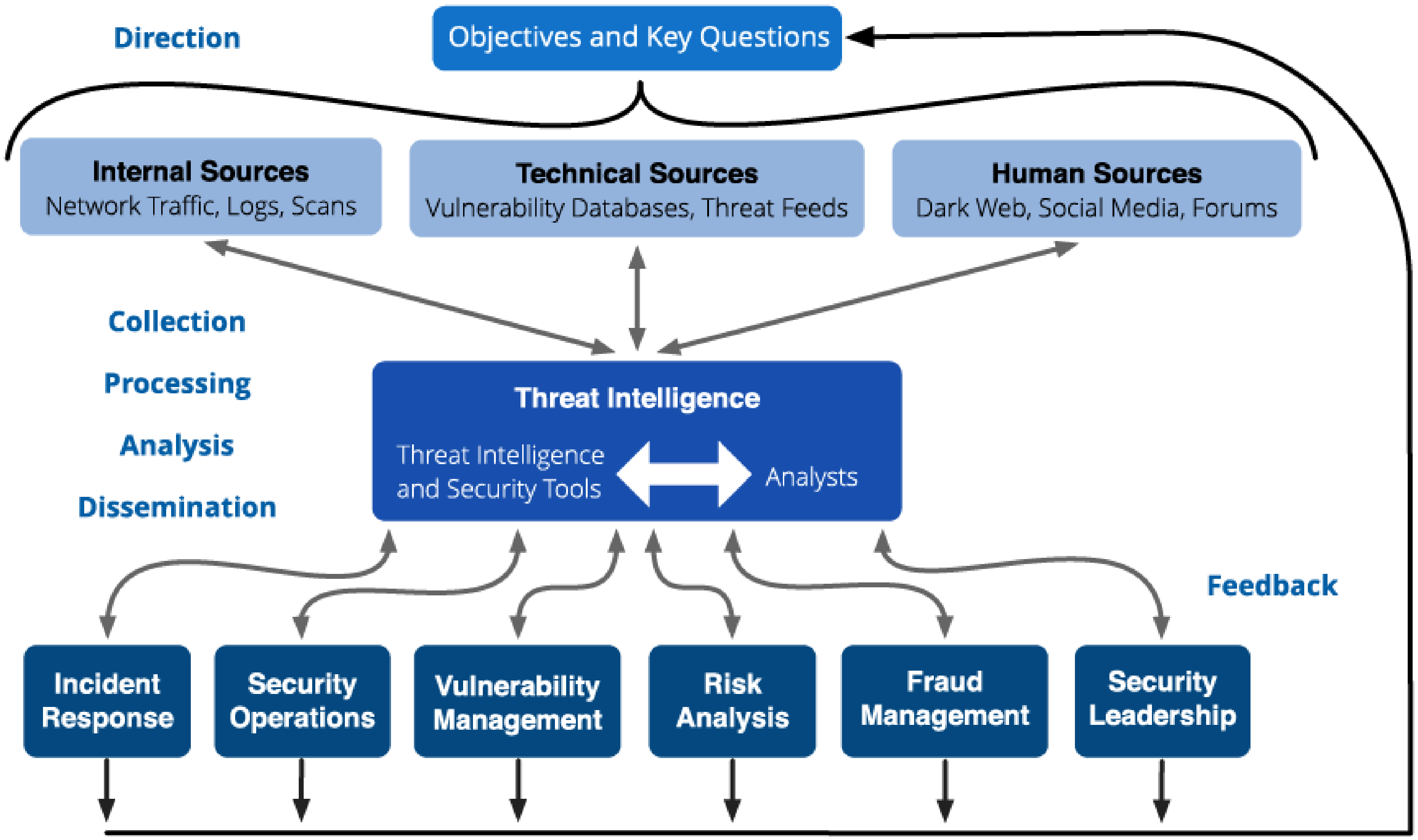


Process of Threat Intel

There are 5 stage process

- **Planning** –> What are you looking for? And what information to be gathered?
- **Collection** –> OSINT/HUMINT – Logs/Data points inside the organization – Honeypots/networks/docs and social networks
- **Processing** –> Once all the raw data has been collected, you need to sort it, organizing it with metadata tags and filtering out redundant information or false positives and negatives
- **Analysis** –> The goal of analysis is to search for potential security issues and notify the relevant teams in a format that fulfills the intelligence requirements outlined in the planning and direction stage - Top of the pyramid of pain
- **Dissemination** –>The finished product is then distributed to its intended consumers. For threat intelligence to be actionable, it has to get to the right people at the right time

Organization Chart



Direction

Objectives and Key Questions

Internal Sources
Network Traffic, Logs, Scans

Technical Sources
Vulnerability Databases, Threat Feeds

Human Sources
Dark Web, Social Media, Forums

Collection

Processing

Analysis

Dissemination

Threat Intelligence

Threat Intelligence and Security Tools

Analysts

Feedback

Incident Response

Security Operations

Vulnerability Management

Risk Analysis

Fraud Management

Security Leadership

STIX

Structured Threat Information eXpression (STIX) provides a common language for describing cyber threat information so it can be shared, stored, and otherwise used in a consistent manner that facilitates automation.

TAXII

Trusted Automated eXchange of Indicator Information (TAXII) is a U.S. Department of Homeland Security (DHS)-led, community- driven effort to standardize the trusted, automated exchange of cyber threat information.

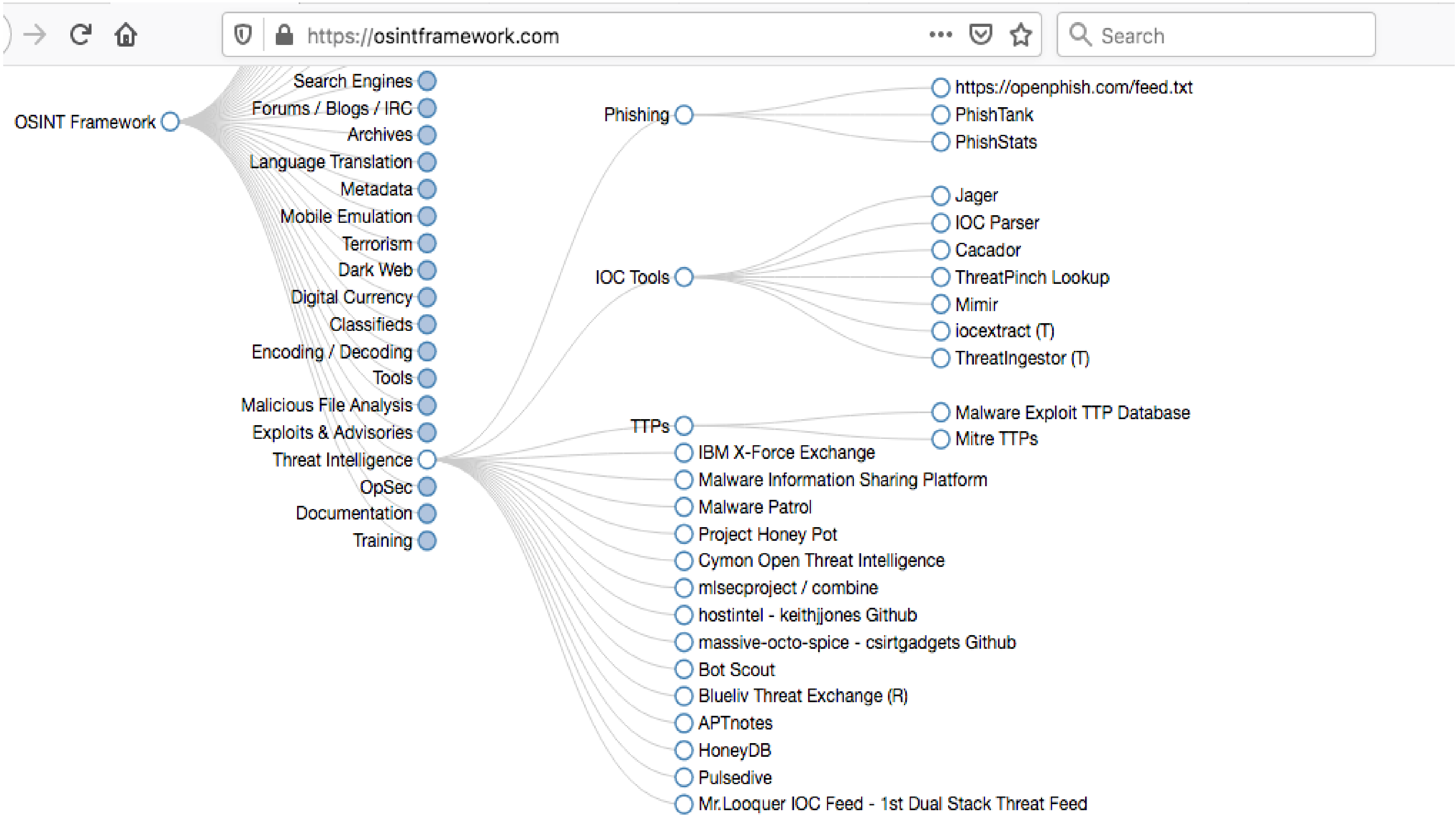
OSINT Using Threat Intel

Open Source Intelligence (OSINT) Framework is a Cybersecurity framework and it is a collection of **OSINT** tools to make your intelligence and data collections tasks easier also known as Digital Footprinting.

OSINT Using Threat Intel

- **Phishing and Spear Phishing** – It is designed to breach the organization's defenses by using email to trick the employees into revealing confidential information, usernames, passwords and other credentials in the process.
- **Indicators Of Compromise (IOCs)** – It can be defined as the pieces of forensic data, such as data found in system log entries or files, that are potentially identified as malicious activity on a system or network.
- **Tactics, Techniques and Procedures (TTPs)** – To examine possible operation methods, a threat hunter should hypothesize specific Tactics, Techniques, and Procedures (TTPs), to understand how these TTPs would appear in specific organizational data sources, and search for them, and that are commonly used by cyber attackers.

OSINT Using Threat Intel



Vendors of Threat Intel

Open Source Intel:

Recorded Future, Digital Shadows, LookingGlassCyber (Cyveillance)

Human Intel:

Booz Allen Hamilton , CrowdStrike, FireEye (iSIGHT Partners), Accenture (VeriSign iDefence), LookingGlassCyber (Cyveillance)

Technical Intel:

Norse Corporation , Anubis Networks, ProofPoint (Emerging Threats)

Adversary Intel:

Booz Allen Hamilton, CrowdStrike, FireEye (iSIGHT Partners), Accenture (Verisign iDefence), Symantec Deepsight

Vulnerability Intel:

FireEye (iSIGHT Partners), Accenture (Verisign iDefence)

Strategic Intel:

Surfwatch labs, Cytegic

References

https://www.fireeye.kr/company/press-releases /2016/fireeye-announces-acquisition-of-isight-partners.html

https://www.symantec.com/services/cyber-security-services/deepsight-intelligence

https://www.checkpoint.com/threat-prevention-resources/

https://www.facebook.com/threatexchange

https://www-03.ibm.com/security/xforce/

https://www.gartner.com/doc/2487216/definition-threat-intelligence

http://security-architect.com/is-threat-intelligence-a-misnomer/

https://www.splunk.com/ko_kr/resources/video.NnczN4MjE6qVYs873PJ4NL2w8Vp8DTj5.html

Dark Web Monitoring

Overview:

- Gaining access to dark web and deep web sources can be extremely powerful.
- The deep web or also called as the dark web is an area of the internet that is only accessible with specific browser software, such as Tor or I2P

Warning:

- The dark web is filled with some awful things and that cannot be unseen.
- Please review the risk or reward before using it.

Uses of Dark Web

<u>For Better Purpose:</u>

- This service uses scrapers and web crawlers to monitor areas of the dark web where stolen information is commonly sold, including websites.
- To provide whistleblowers protection.
- Use of Dark web monitoring can keep tabs on a variety of online sources, including:

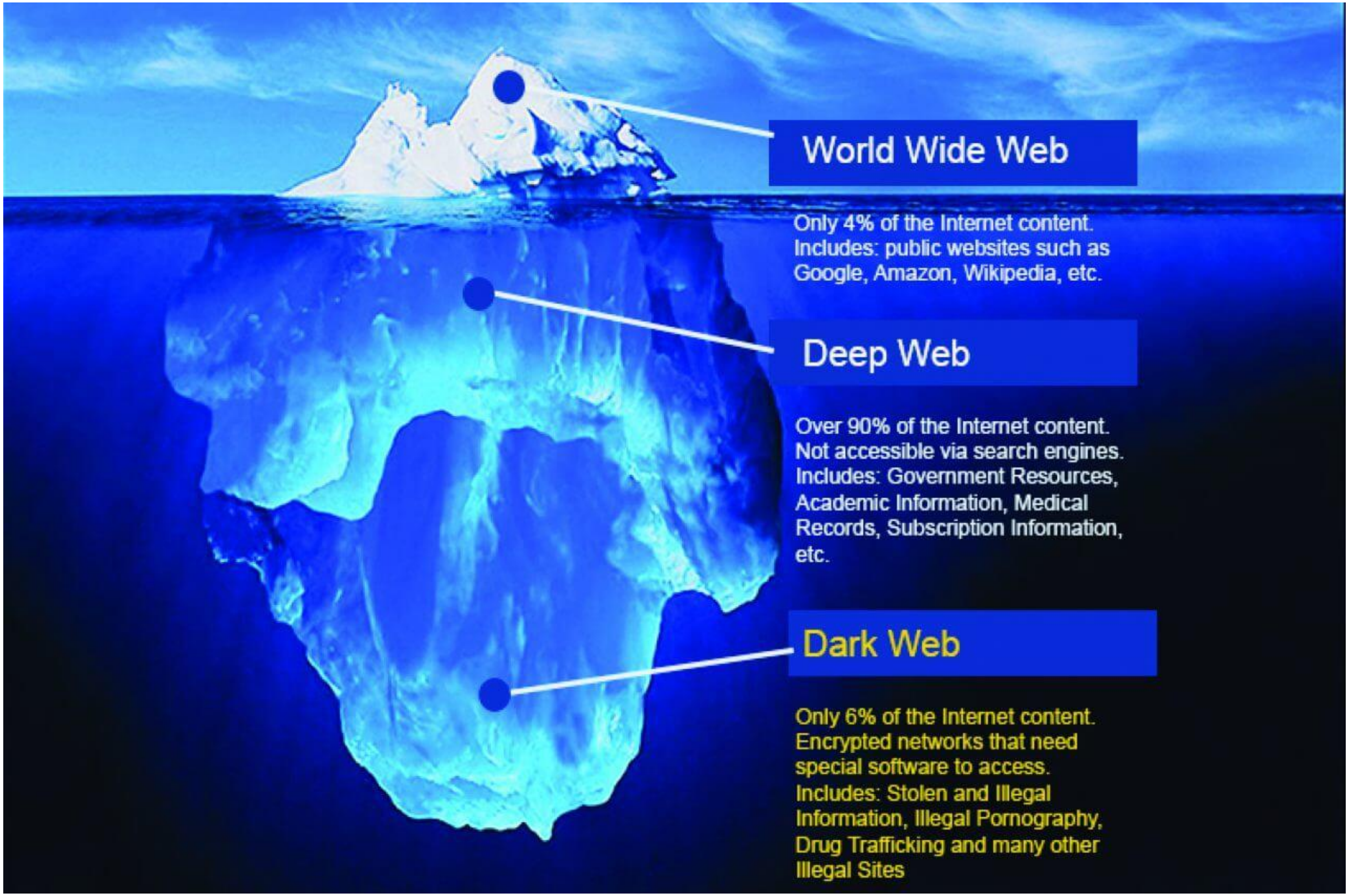
  - Web pages
  - Peer-to-peer sharing networks
  - Forums and chat rooms
  - Blogs
  - Malware samples
  - Social media feeds
  - Web services, servers and file transmissions
  - Tools and Softwares.

Uses of Dark Web

For Worst Purpose:

- Enables sales of illegal firearms, drugs, counterfeits, etc.
- Human Exploitation
- Hiring Hackers, Hitmans, etc.

Understanding the Web



World Wide Web

Only 4% of the Internet content. Includes: public websites such as Google, Amazon, Wikipedia, etc.

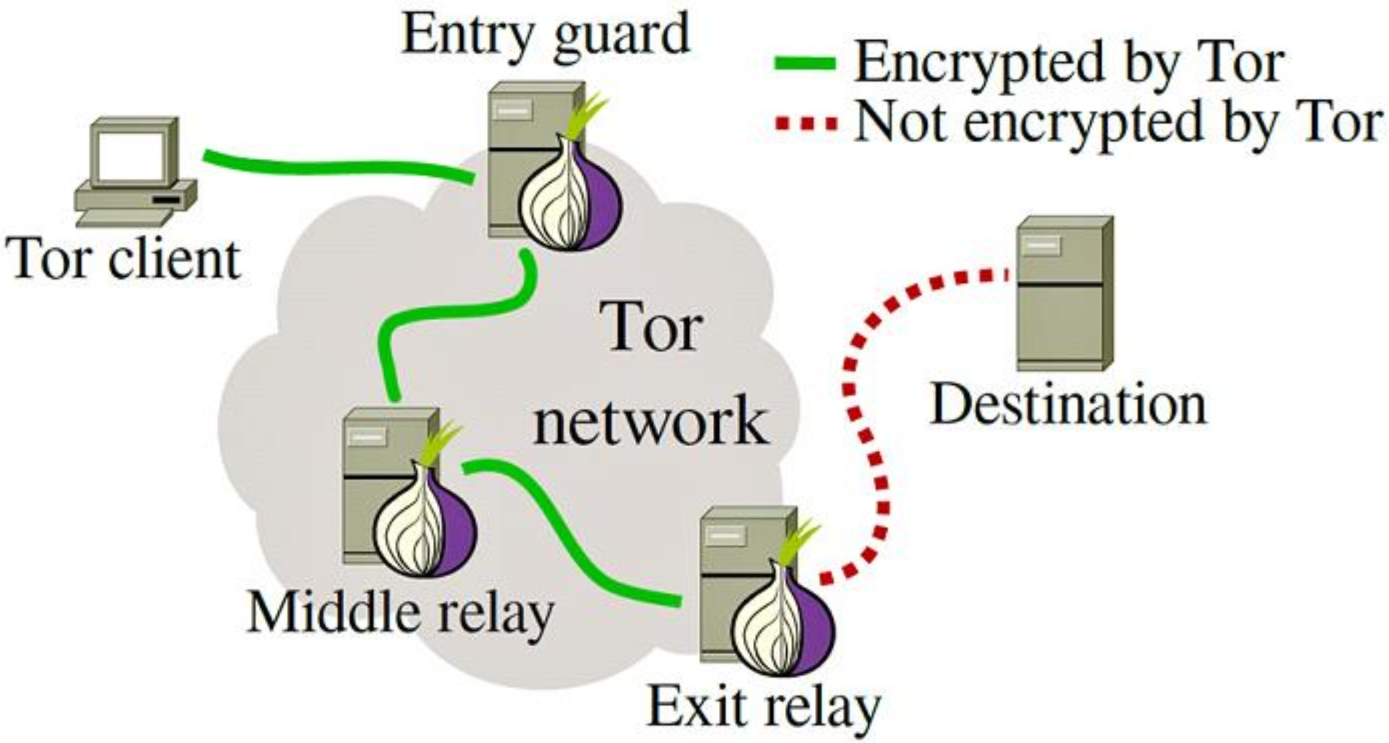
Deep Web

Over 90% of the Internet content. Not accessible via search engines. Includes: Government Resources, Academic Information, Medical Records, Subscription Information, etc.

Dark Web

Only 6% of the Internet content. Encrypted networks that need special software to access. Includes: Stolen and Illegal Information, Illegal Pornography, Drug Trafficking and many other Illegal Sites

How Tor Works



About .onion sites and Challenges

- Can only be accessed when using Tor browser.
- Use of Tor allows for the creation of .onion sites
- Domains are randomly generated, either 16 or 56 characters long
- The Tor browser is modified with Mozilla Firefox browser with numerous integrated scripts and add-ons to protect your privacy while browsing onion sites.
- Payments can be done only with Bitcoin.
- Accounts need to anonymized.
- The network was designed to provide anonymity.
- Use with CAUTION!

Softwares and OS Used

Operating System:

- Tails OS
- Qubes OS
- Kali OS

Softwares:

- Whonix
- Tor Browser
- Tor Firefox

Other Resources

The Hidden Wiki or Onion Wiki:

https://thehiddenwiki.org/

https://zqktlwi4fecvo6ri.onion.ws/wiki/index.php/Main_Page

Hunchly Daily Dark Web Report:

https://www.hunch.ly/darkweb-osint/

Github Onion sites:

https://github.com/topics/onion-sites

Request for Proposal of setting up of Security Operations Centre (SOC)

Aviation Company

Introduction

Globally a number of organizations are now working towards producing standards and guidelines to protect the Cyber security posture of the aviation sector.

The Civil Aviation Authority along with the Cyber Security Division of Ministry of Transport and Communications would like to take a step further in this direction and provide cyber security guidance to this critical sector. These guidelines will assist operators and stakeholders within the aviation sector to improve their cyber security posture and build a resilient organization

Disclaimer:

This document is intended security risks. to provide guidelines to the aviation sector on addressing cyber security risks

Objective

- The Company has decided to build a Security Operation Centre (SOC) to monitor, assess and defend Company‘s information systems in order to protect confidentiality, integrity and availability of the aviation’s data.
- The proposed SOC facility is to be equipped with set of tools such as Security Information and Event Management Tool (SIEM), Incident Management tool, Anti – Advanced Persistent Threat (APT), Privilege Identity Management (PIM), Network Access Control (NAC) and Firewall Analyser given in detail under this RFP and Security Intelligence services for better security monitoring and response capabilities

Scope Of Work

The cyber security guidelines prescribed in this document cover critical information systems within the aviation eco-system. These include but are not limited to:

1. Air Traffic Control Systems
2. Airport Operators (airline reservation system)
3. Airport Information Systems
4. Aircraft operators (Local / National / Foreign carriers operating)
5. Aircraft Systems
6. Airport Tenants (e.g. Cargo, airport operators, etc.)

In General: The bidder shall install, supply, customize, integrate, migrate, test, monitor, manage, backup and troubleshoot the SIEM and other in-scope solutions.

Scope Of Work to be assessed

The intended audience for this documents includes stakeholders that manage the critical information systems within the aviation eco-system. These includes:

1. Air Traffic Control operators that manage communication with airplanes during flight takeoff / landing.
2. Airport Authorities / Operators who manage critical information systems at the airports. This includes Passenger Information Systems, Airport Information System, Baggage Handling systems, Ticket payment/booking systems etc.
3. Information Systems within an airplane including its communication systems, flight entertainment systems, internal controls etc…

Evolving Threats faced by aviation sector

- Phishing attacks
- WiFi-based attacks
- BYOD (Bring Your Own Device)
- DDoS and Botnet attacks
- Jamming attacks
- Remote hijacking

Solutions to be Implemented

1. SIEM tool
2. Vulnerability Management
3. Network Behaviour Anomaly Detection (NBAD)
4. Anti-Advanced Persistent Threat (Anti-APT)
5. Product, Software and Cloud Security
6. Anti-Phishing
7. Malware Monitoring and Penetration Testing
8. Security Intelligent Services
9. ICS/IoT Security

Solutions to be Implemented

Alert Generation:

Solution should be capable to generate alerts, register and send/receive the same through message formats as per user configurable parameters.

Log Collection:

In case the systems/applications are writing logs to the local hard disks, solution should be capable to pull the logs from these devices through secure transfer. Only in case where remote log collection is not feasible, bidder / vendor should install agent on the servers and applications for collection of logs. Raw logs should be made available in case of legal requirement.

Services we require

SOC Team:

The SOC is usually led by a SOC manager, and may include incident responders, SOC analysts (levels 1, 2 and 3), and threat hunters as per the requirements needed. The SOC reports to the CISO, who in turn reports to either the CIO or directly to the CEO.

VAPT Information and Remediation services:

a) Bidder should provide vulnerability assessment services for mentioned devices/servers.

b) Bidder should perform penetr ation testing for servers hosted over Internet

c) Bidder should provide detailed reports of the assessment

d) Bidder should execute this service on quarterly basis

Security/Threat Intelligence Services

The Company intends to have a system for tracking of new and emerging threats & vulnerabilities affecting organization across the world so that company can proactively protect against them.

Bidder should track and provide information on global security threats and help the company to mitigate the relevant risks on continuous and proactive basis.

This service should include:

a) 24*7*365 Continuous tracking of global threats and vulnerabilities to tackle evolving threats and vulnerabilities.

b) Provide trusted detailed reports on newly discovered malicious threats and malware.

Other General Requirements

a) The bidder needs to provide all the hardware and software required as part of this RFP.

b) The sizing of the infrastructure as proposed by the bidder, should be certified by the Original Equipment Manufacturer (OEM).

c) The bidder shall ensure that the hardware proposed does not reach end of life (EOL) and end of support (EOS) during the contract period of three years plus addition of two year post completion of the contract.

d) None of the tools/software/utilities/solutions proposed should be Open Source.

e) The bidder needs to propose any backup solution for backups