Cyber-Security

Ishan Bhatt

Agenda

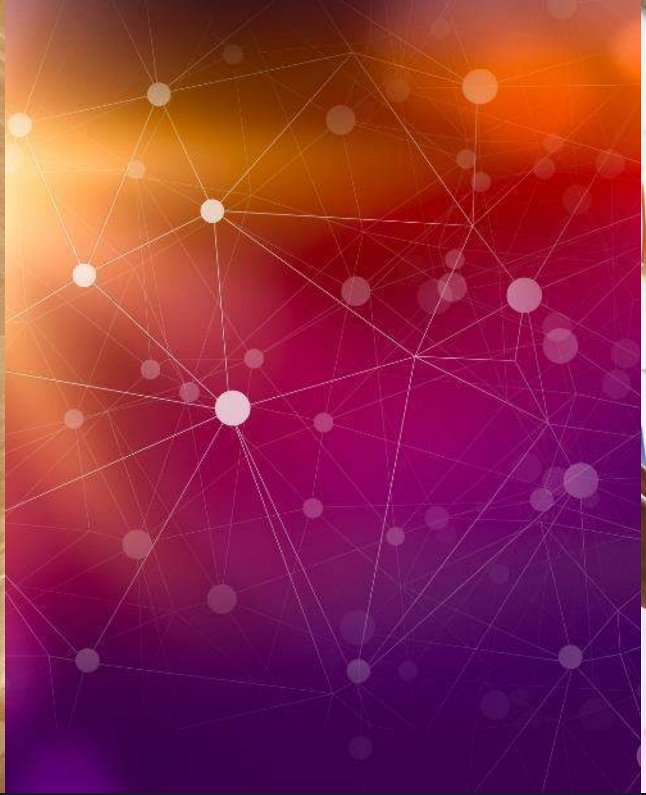
Career Options

Cyber Security Overview

The Basics

Key Concepts

Core Topics



Introduction

- Look at Career Options.
- Introduction to Cyber Security and Basics
- View some key cyber areas

Topic one

Career Options

Common Career Paths

- Data Science
- Data Analytics
- Game Development
- Cloud Operations
- AI & Machine Learning
- Cyber Security
- Research
- Software Development

> Find a job you enjoy doing, and you will never have to work a day in your life.
>
> **- Mark Twain**

Cyber Security as a Career

CYBER PAYS BETTER

The U.S. Bureau of Labor Statistics (BLS) reports that the median annual salary for information security analysts is $102,600. This **salary is more than double the national median earnings** of workers across all industries ($45,760).

GROWING DEMAND & SUPPLY SHORTAGE

The number of unfilled cybersecurity jobs worldwide grew 350% between 2013 and 2021, from 1 million to 3.5 million, according to Cybersecurity Ventures. The industry researcher also predicts that in five years, the same number of jobs will still be open.

REGULATORY COMPLIANCE

- **Amazon**: $877 million – GDPR violation
- **Equifax**: (At least) $575 Million - "failure to take reasonable steps to secure its network.“
- **Instagram**: $403 million - violating children’s privacy under the terms of the GDPR
- **T-Mobile**: $350 million - “unauthorized access” to T-Mobile’s systems after a portion of customer data was listed for sale on a known cybercriminal forum.

306

Global Cyber Incidents in August 2022

9.87

Average/Day

Topic two

Cyber Security Overview

Overview

WHAT IS CYBER SECURITY ?

- The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide **confidentiality**, **integrity**, and **availability**.

WHO NEEDS CYBER SECURITY PROFESSIONALS ?

- Financial Institution.
- Government.
- Military.
- Health.
- Manufacturing
- Any industry working with someone else’s data.

Cyber Security

CIA

RISK MANAGEMENT

- Security Strategies
- Risk Assessments
- Security Architecture
- Compliance Reviews
- Risk & Governance
- Awareness

OFFENSIVE

- Vulnerability Assessment.
- Penetration Testing.
- Bug Bounty
- Network Intrusion.
- Hacking

DEFENSIVE

- Data Protection.
- Log Monitoring.
- Incident Response.
- Threat Intelligence and detection.
- Cyber Forensics.

Topic three

The Basics

Basics..

VULNERABILITY

Weakness in an information system that could be exploited or triggered by a threat.

- Bugs
- Misconfiguration
- Poor process or control

+

THREAT

Any circumstance or event with the potential to adversely impact an information system.

- Cyber Criminals
- Nation State Actors
- Internal Threats

↓ exploit

RISK

Materialization of financial loss, disruption or damage to the reputation of an organization.

- This is considered as **inherent risk**

Inherent Risk + Cyber Controls = Residual Risk

Basics..

Cyber Controls

ADMINISTRATIVE

- Regulations
- Standards
- Policies
- Procedures
- Legal Contracts
- Service level agreements

PREVENTATIVE

- Firewalls
- Web Proxy
- Email Gateways
- Anti Virus
- Patch Management

DETECTIVE

- Vulnerability Scanning
- Log Monitoring
- Security Reviews

CORRECTIVE

- Incident Response
- Cyber Forensics
- Business Continuity & Disaster Recovery

Topic four

Key Concepts

Concepts..

OPEN SYSTEMS INTERCONNECTION (OSI)

The original objective of the OSI model was to provide a set of design standards for equipment manufacturers so they could communicate with each other.
The OSI model defines a hierarchical architecture that logically partitions the functions required to support system-to-system communication

7. **Application**: Provides different services to the application

6. **Presentation**: Converts the information

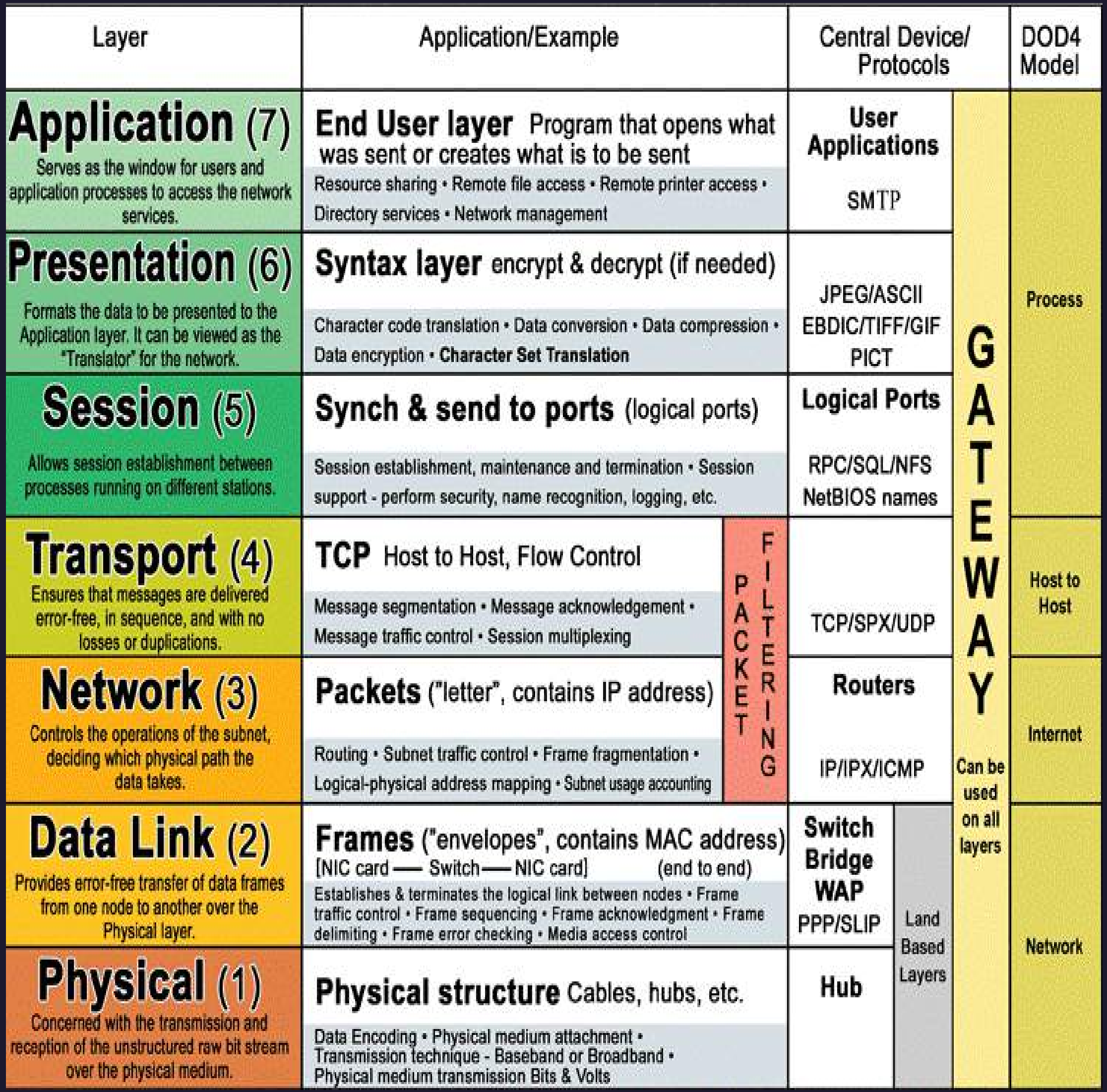
5. **Session**: Handles problems which are not communication issues

4. **Transport**: Provides end to end communication control

3. **Network**: Routes the information in the network

2. **Data Link**: Provides error control

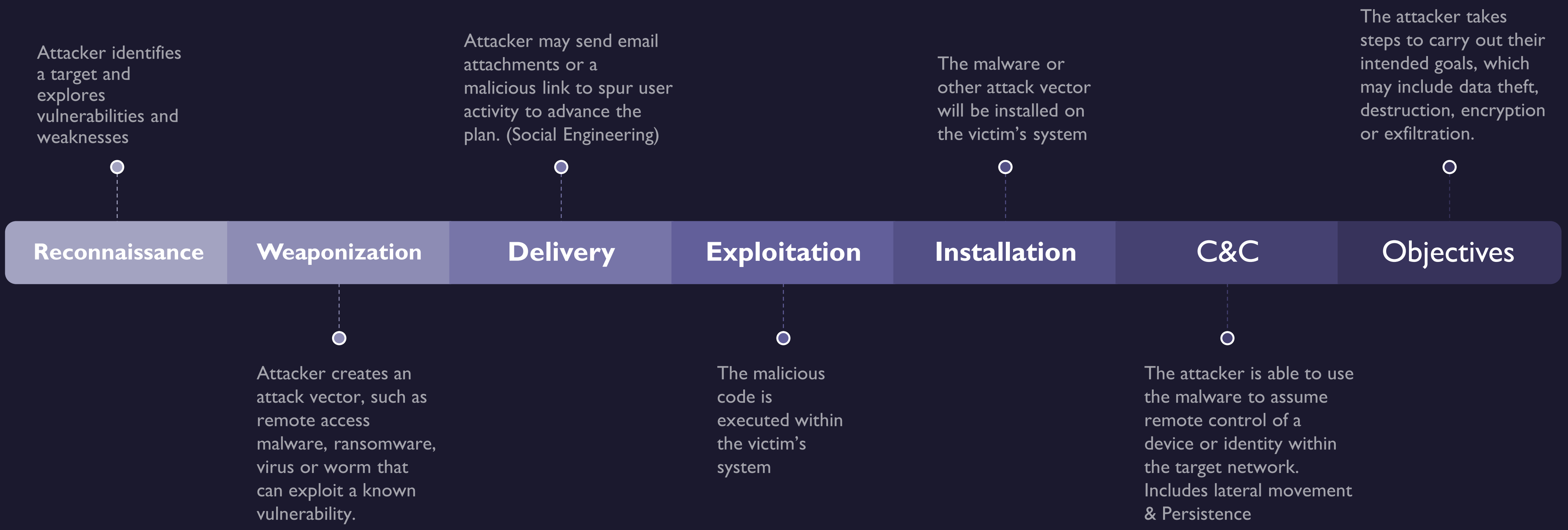
1. **Physical**: Connects the entity to the transmission media



Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		**GATEWAY** Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

Concepts..

Cyber Kill Chain



Reconnaissance

Attacker identifies a target and explores vulnerabilities and weaknesses

Weaponization

Attacker creates an attack vector, such as remote access malware, ransomware, virus or worm that can exploit a known vulnerability.

Delivery

Attacker may send email attachments or a malicious link to spur user activity to advance the plan. (Social Engineering)

Exploitation

The malicious code is executed within the victim's system

Installation

The malware or other attack vector will be installed on the victim's system

C&C

The attacker is able to use the malware to assume remote control of a device or identity within the target network. Includes lateral movement & Persistence

Objectives

The attacker takes steps to carry out their intended goals, which may include data theft, destruction, encryption or exfiltration.

Upgrade of cyber kill chain

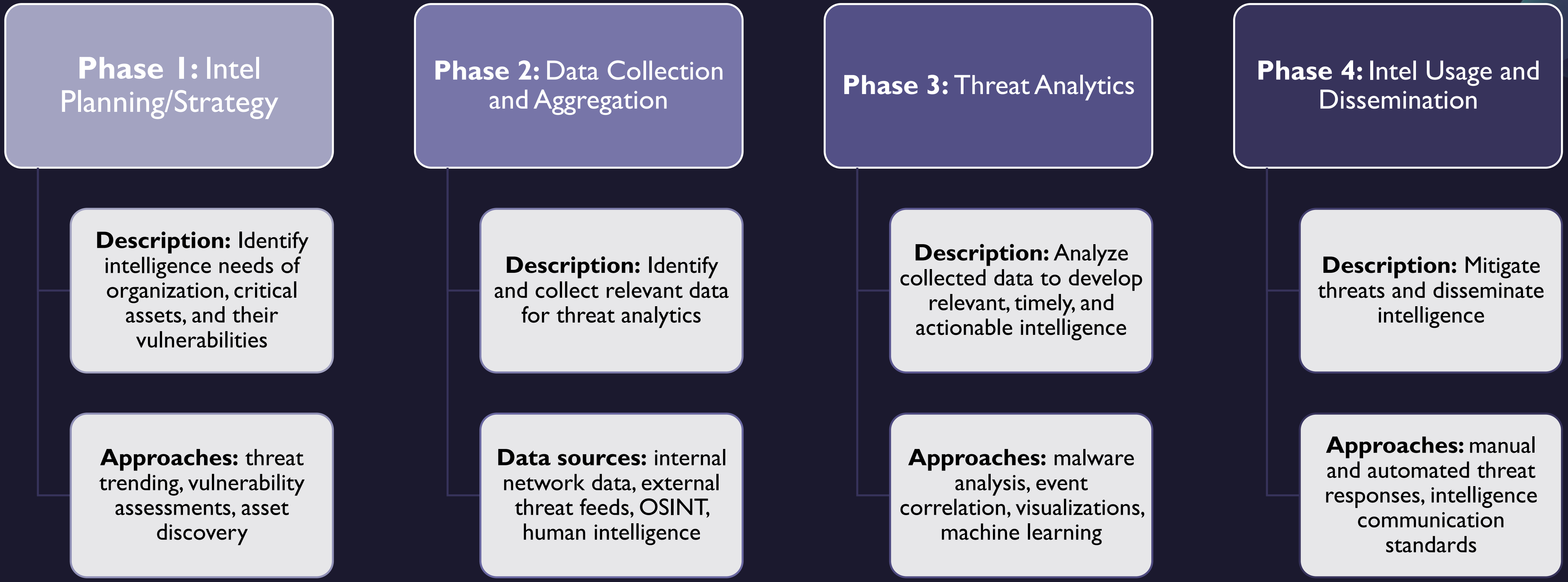
https://attack.mitre.org/

Topic five

Core Topics

Cyber Threat Intelligence

FUNDAMENTALS OF CTI OPERATIONS



Phase 1: Intel Planning/Strategy

Description: Identify intelligence needs of organization, critical assets, and their vulnerabilities

Approaches: threat trending, vulnerability assessments, asset discovery

Phase 2: Data Collection and Aggregation

Description: Identify and collect relevant data for threat analytics

Data sources: internal network data, external threat feeds, OSINT, human intelligence

Phase 3: Threat Analytics

Description: Analyze collected data to develop relevant, timely, and actionable intelligence

Approaches: malware analysis, event correlation, visualizations, machine learning

Phase 4: Intel Usage and Dissemination

Description: Mitigate threats and disseminate intelligence

Approaches: manual and automated threat responses, intelligence communication standards

Cyber Threat Intelligence

THREAT INTELLIGENCE MUST PROVIDE THE CONTEXT TO MAKE INFORMED DECISIONS AND TAKE ACTION.

Threat intelligence needs to be timely, clear, and actionable. It has to come at the right time, in a form that is understandable. It should enrich your knowledge, not complicate the decision-making process. It should help put everybody on the same page.

PEOPLE AND MACHINES WORK BETTER TOGETHER.

Machines can process and categorize raw data orders exponentially faster than humans. On the other hand, humans can perform intuitive, big-picture analysis much better than any artificial intelligence . When people and machines are paired, each works smarter, saving time and money, reducing human burnout, and improving security overall.

THREAT INTELLIGENCE IS FOR EVERYONE.

No matter what security role you play, threat intelligence makes a difference. It’s not a separate domain of security — it’s context that helps you work smarter. Threat intelligence should integrate with the solutions and workflows you already rely on.

Incident Response

WHAT IS INCIDENT RESPONSE.

Incident response is a process that allows organizations to identify, prioritize, contain and eradicate cyberattacks. The goal of incident response is to ensure that organizations are aware of significant security incidents, and act quickly to stop the attacker, minimize damage caused, and prevent follow on attacks or similar incidents in the future.

Preparation Review and codify an organizational security policy, perform a risk assessment, identify sensitive assets, define which are critical security incidents the team should focus on, and build a Computer Security Incident Response Team (CSIRT).

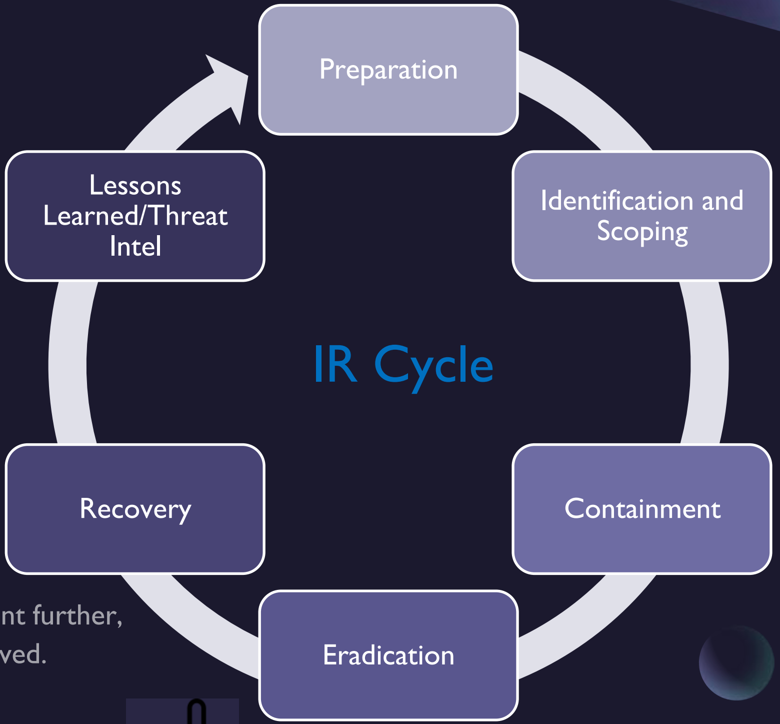
Identification Monitor IT systems and detect deviations from normal operations, and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.

Containment Perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding clean systems.

Eradication Remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.

Recovery Bring affected production systems back online carefully, to prevent additional attacks. Test, verify and monitor affected systems to ensure they are back to normal activity.

Lessons Learned Perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved.



IR Cycle

Preparation

Identification and Scoping

Containment

Eradication

Recovery

Lessons Learned/Threat Intel

SLA's, Compliance Management

COMPLIANCE MONITORING.

Compliance monitoring is an exercise to measure the compliance effectiveness across the entire cyber security program including business continuity and Privacy.

You need to know what to comply to.

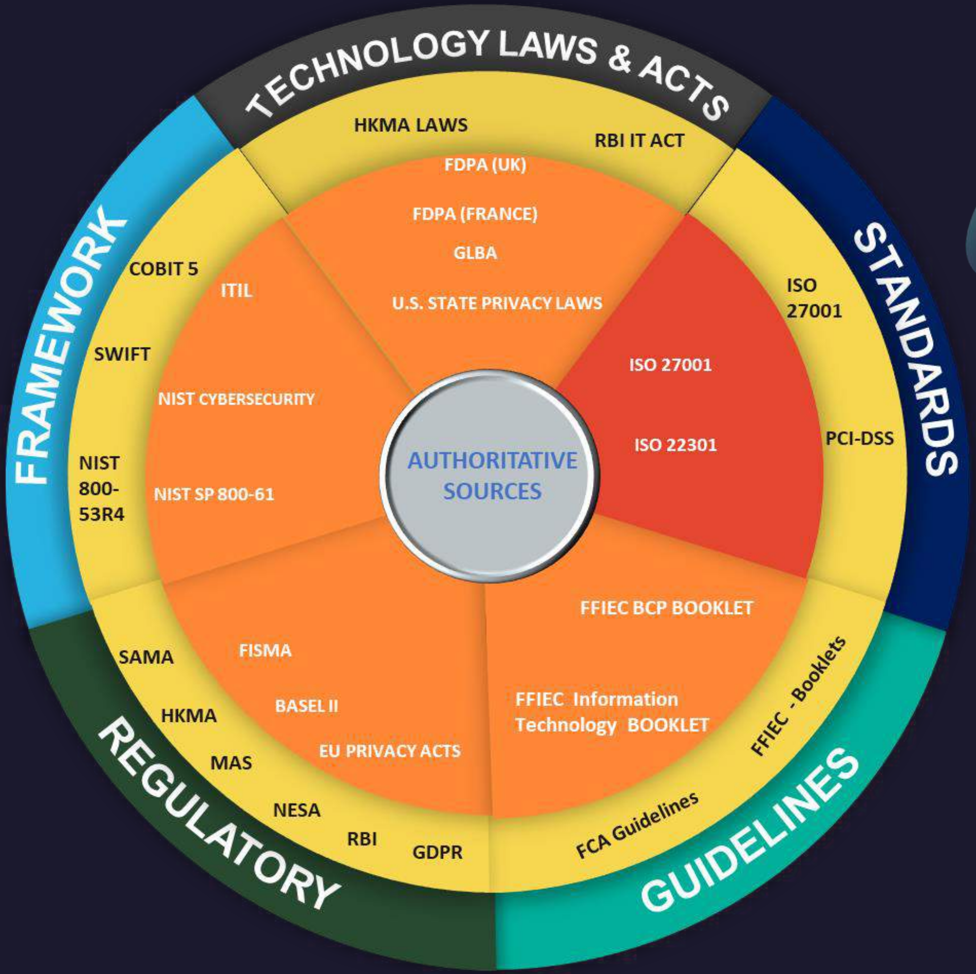
UNIFIED COMPLIANCE FRAMEWORK

- Identify all regulations and standards.
- Document and track through a governance platform.
- Helps avoid duplication of efforts.
- Better visibility and transparency with compliance team.
- Efficient policy and procedure definition.

Are we meeting our obligations ?

SERVICE LEVEL AGREEMENTS

When cyber services are provided to multiple remote locations from a head office, service level agreements are documented to ensure continuous delivery of services and evidences to cover regulatory audits and requirements.



Summary

Identify your area of interest.

Work on the basics and concepts

Develop your skill along with knowledge

Work towards excellence.

Thank You

Ishan Bhatt