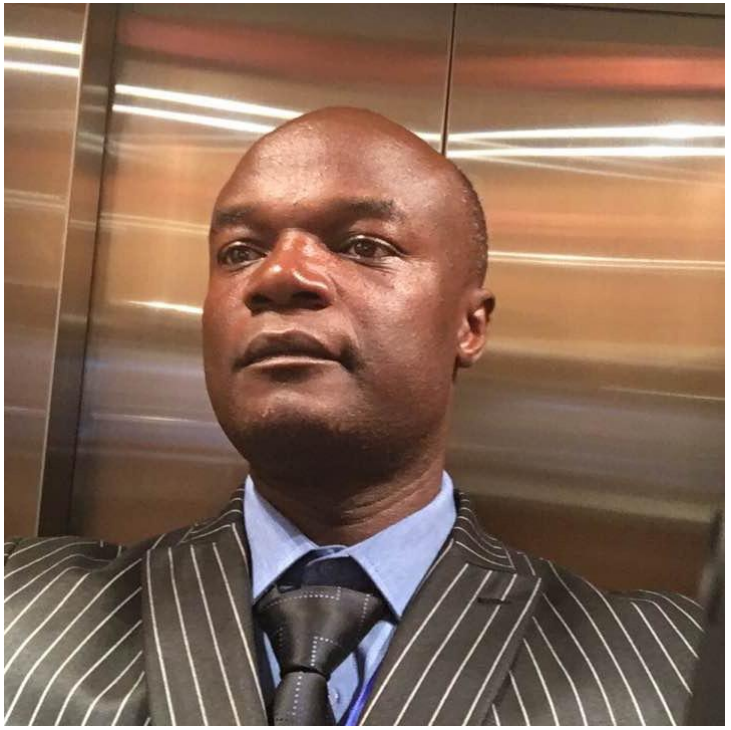
Martin Luther

Consultant and Specialist in Digital Forensics and Cyber Crimes Investigations

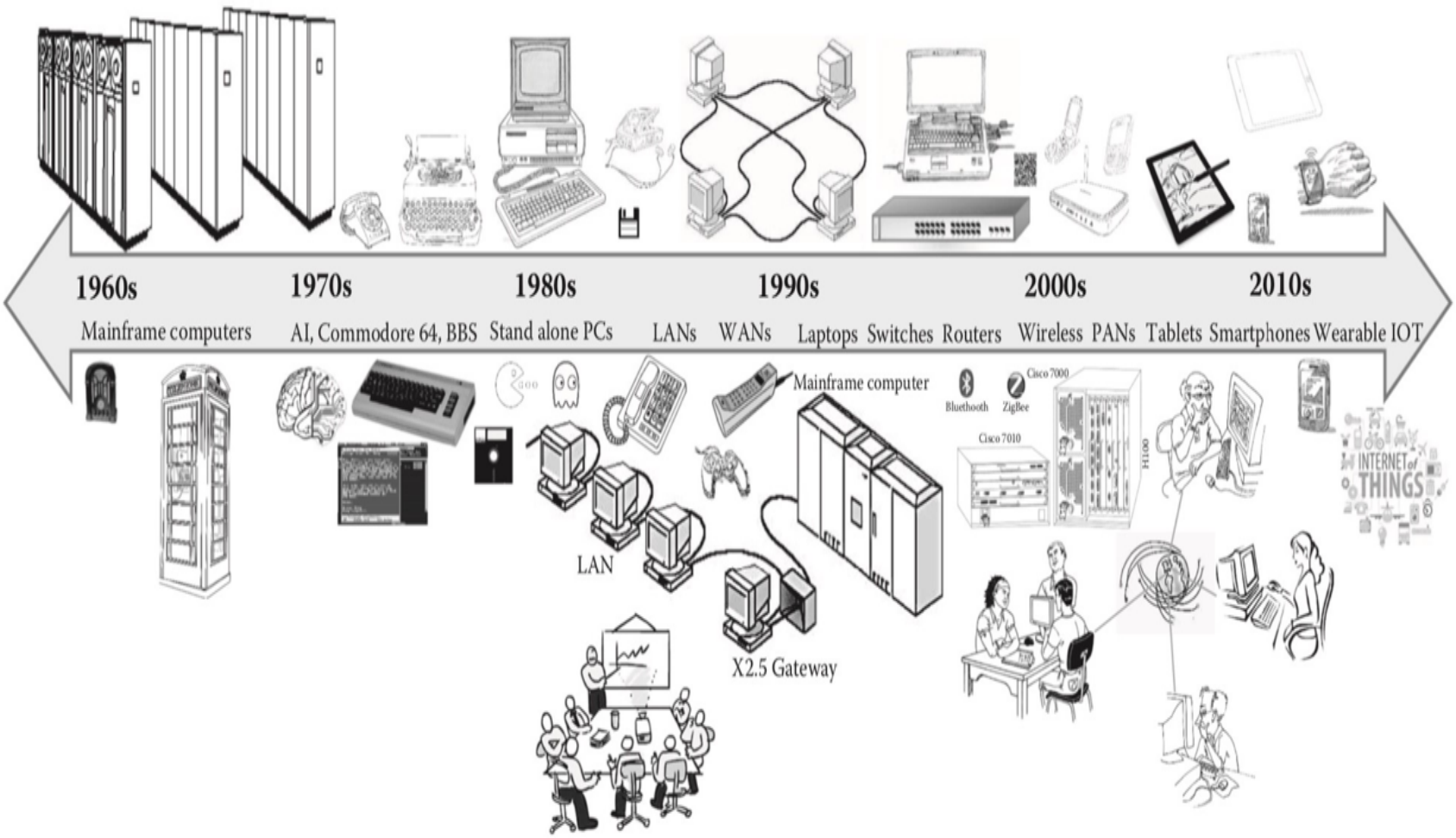
TOPIC: Cyber Security



Agenda Items

- Introduction
- Cyberspace
- Cybersecurity Framework
- Cybersecurity Threats
- Cyber Attacks
- Competence Required in Cybersecurity

Computing and Culture Shock



Cyberspace

- Cyber comes from “cybernetics,” a term coined in 1948 to apply to the comparative study of automatic control systems, such as the brain/nervous system and mechanical-electrical communication systems.

- The term cyberspace was coined by William Gibson in his novel Neuromancer (1984) to describe a futuristic computer network into which users plug their brains.

- Cyberspace encompasses not only the online world and the internet but also the whole wired and wireless world of communications in general

Cybersecurity Definitions

- The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this (Oxford English Dictionary)

- Measures taken to protect a computer or a computer system (as on the Internet) against unauthorized access or attack (Merriam-Webster)

- The body of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access (WhatIs.com)

- Refers to preventative methods used to protect information from being stolen, compromised, or attacked (Technopedia)

Cyber security

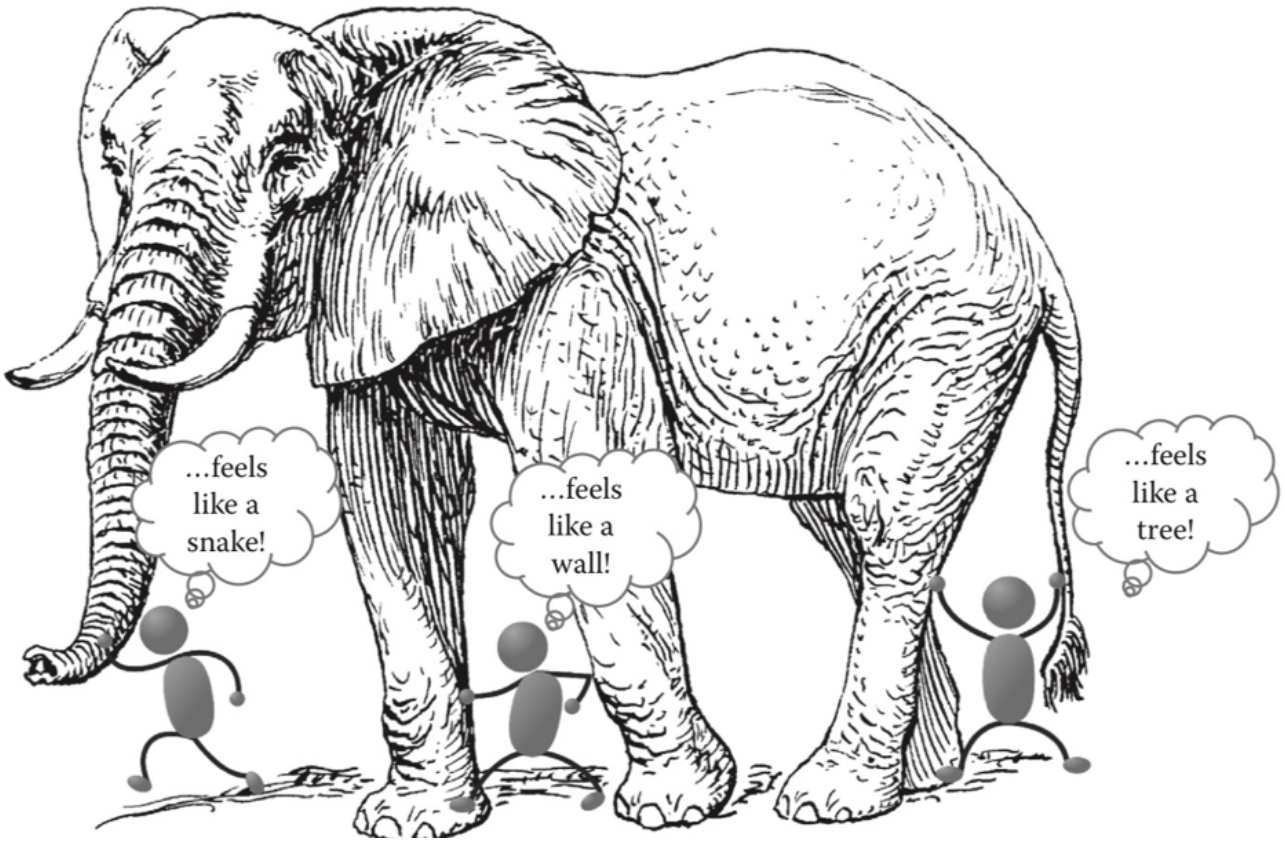
The protection of information systems; software and hardware that use, store, and transmit that information

Through systematic risk assessment and vulnerability management.

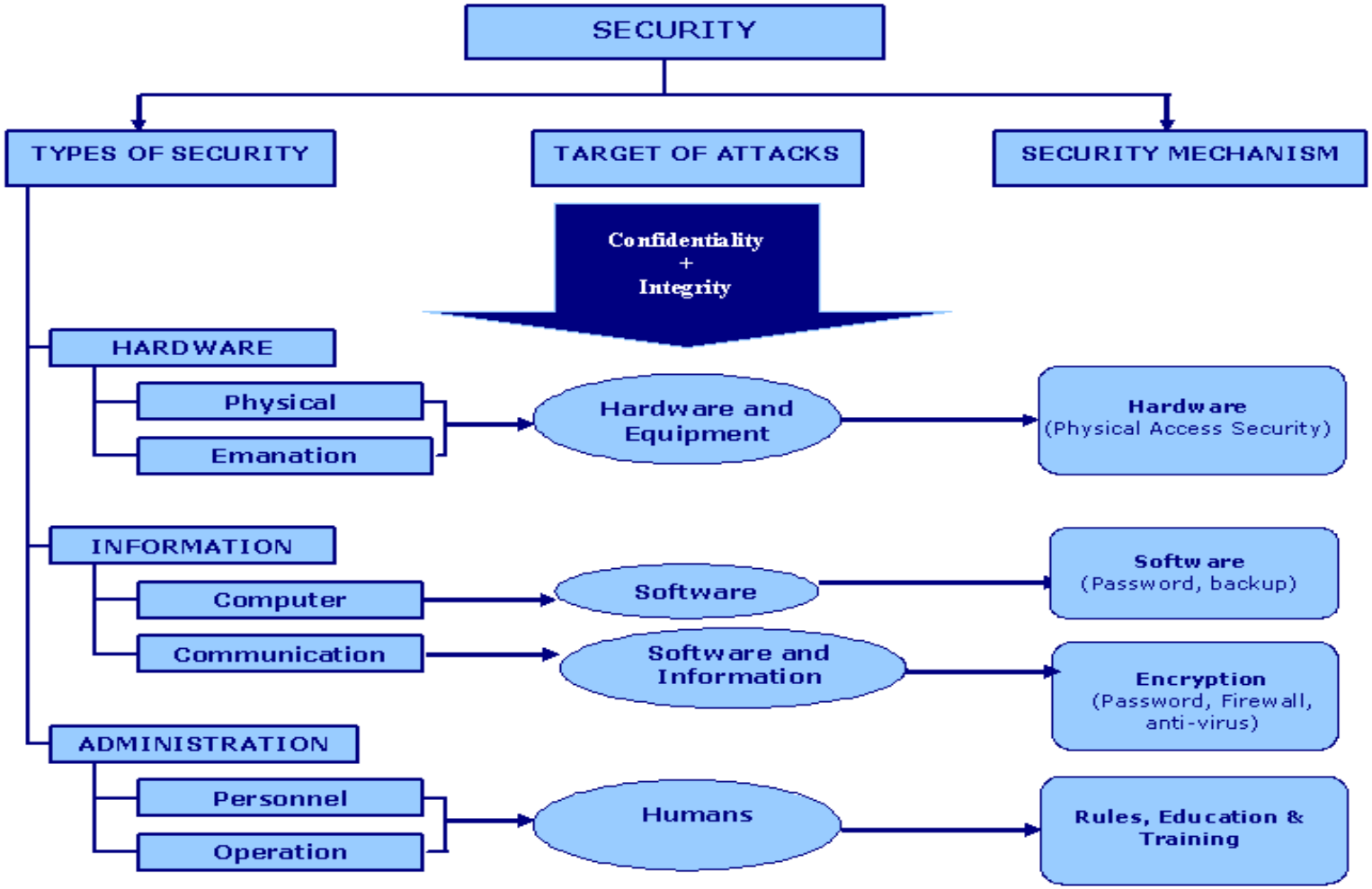
- *Is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.*

The adoption of appropriate legislation against the misuse of ICT for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures

Six Blind Men and An Elephant



Cyberattacks



DIFFERENT KINDS OF CYBER SECURITY THREATS

BRING YOUR OWN DEVICE (BYOD) POLICIES

Using personal devices infected with a virus at work can easily compromise the organization's network as well.

SHADOW IT SYSTEMS

Usually, these IT systems aren't compatible with an organization's central IT system. As a result, data loss and security threat keep rising.

DDOS

The distributed denial-of-service attack floods theorganization's network with traffic and ultimately shuts it down.

MALWARE ATTACK

Malicious software programs can get ahold of your sensitive information without you even noticing.

FLAWS IN INTERNET OF THINGS (IOT)

Devices connected through a flawed Internet of Things is more to security issues.

INSIDE MAN

Bad players within an organization can easily breach security because of easy access.

CRYPTO-MALWARE

This malware get access to your computer's processing power and use it to mine cryptocurrencies.

PHISHING EMAIL

Phishing emails contain the trojan horse or ransomware viruses. 97% of the people can't tell the difference and open it, releasing the virus.

DATA BREACH

Many use obsolete data storage networks that are prone to data breaches.

INSECURE APPLICATION USER INTERFACE (API)

The lack of proper security measures in the Application User Inter-face can cause security breaches.

FILELESS MALWARE

This malware don't exist as a file in the hard drive and work in the background.

STEGWARE

Stegware are malicious files hidden within another file, such as video, image, messages, etc.

CLOUD ABUSE

Most of the cloud storage can be accessed by hacking the Virtual Machine.

SINGLE FACTOR PASSWORDS

Using only a single factor password isn't enough to offer full security in 2019 because they are easy to crack.

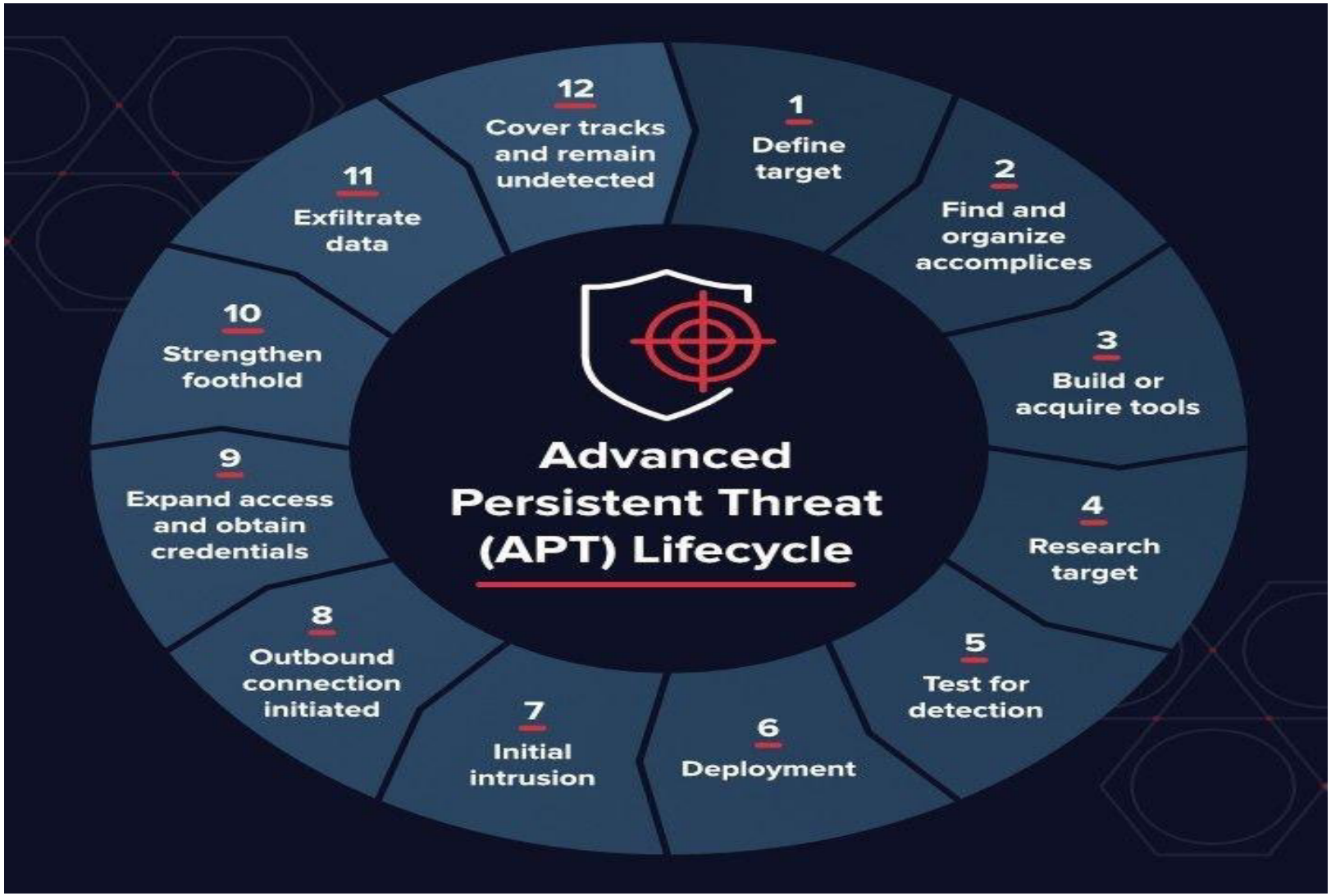
ZERO-DAY THREATS

Most of the programs come with security holes, and cybercriminals find this security lopes and use it.

WHALING

It's a form of phishing attack where the attacker convinces to be reliable but later abuses the data.

Advanced Persistent Threat (APT)



10 Steps To Cyber Security

Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

Network Security

Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

Malware Prevention

Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

Monitoring

Establish a monitoring strategy and develop supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

Incident Management

Establish an incident response and disaster recovery capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

User Education and Awareness

Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Home and Mobile Working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

Secure Configuration

Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

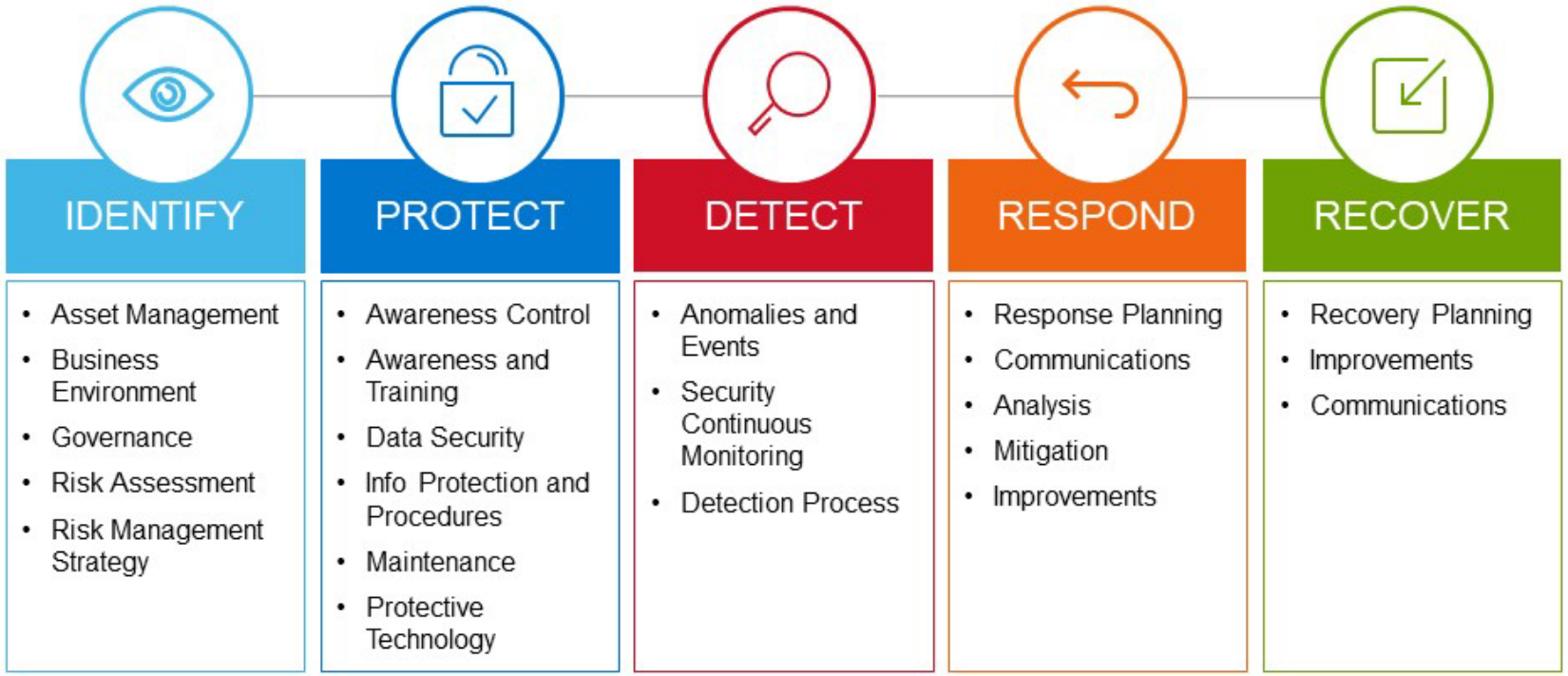
Removable Media Controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing into the corporate system

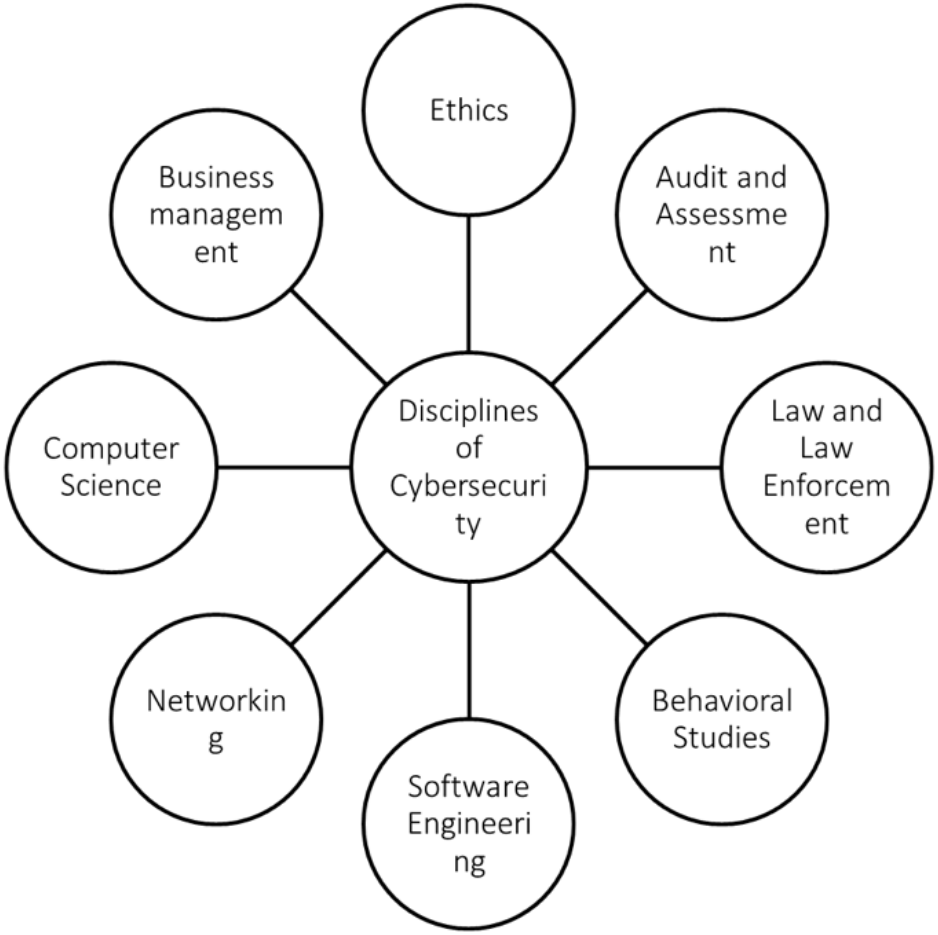
Managing User Privileges

Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

NIST Cybersecurity Framework Overview



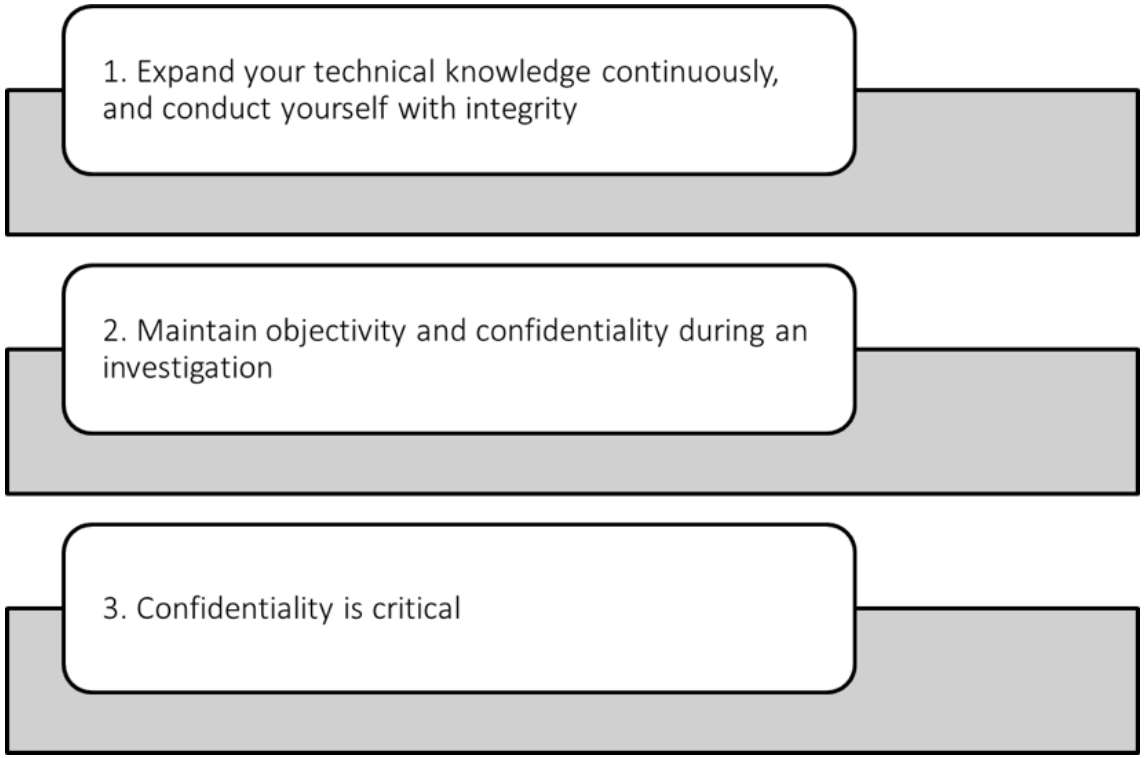
Competencies Required in Cybersecurity



- Attention to Detail
- Technical Knowledge
- Problem solving skills
- Knowledge of mobile technology

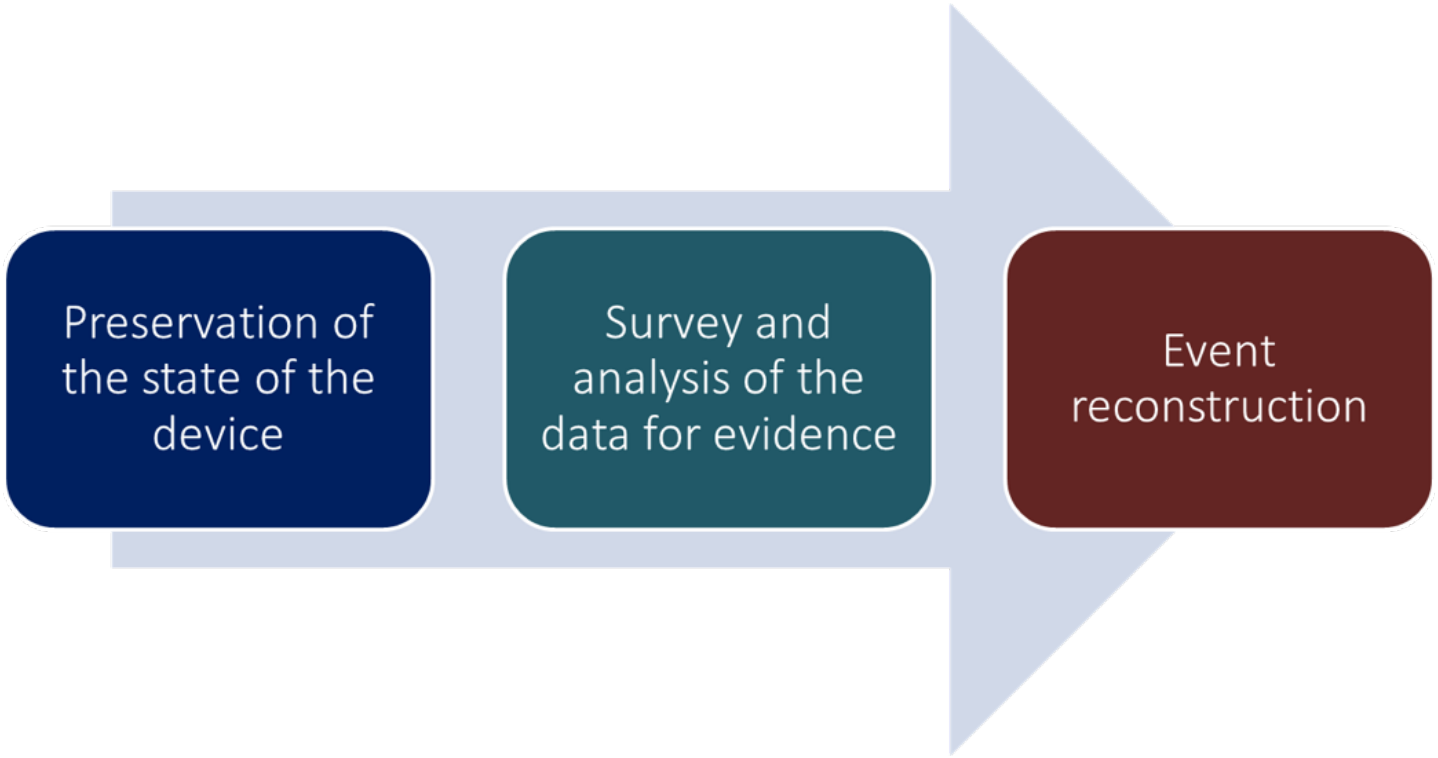
Maintaining Professional Conduct

- Professional conduct, includes ethics, morals, and standards of behavior

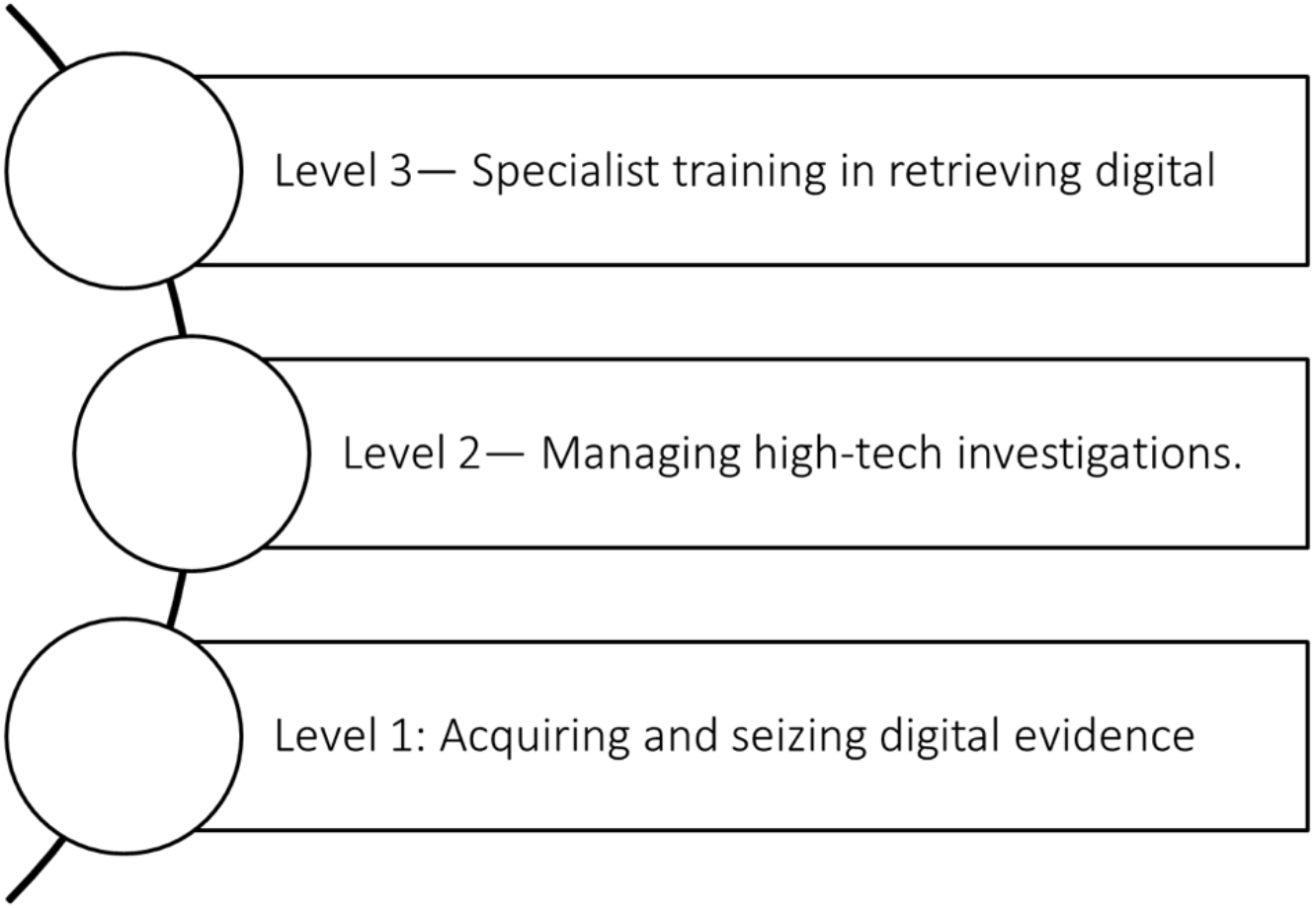


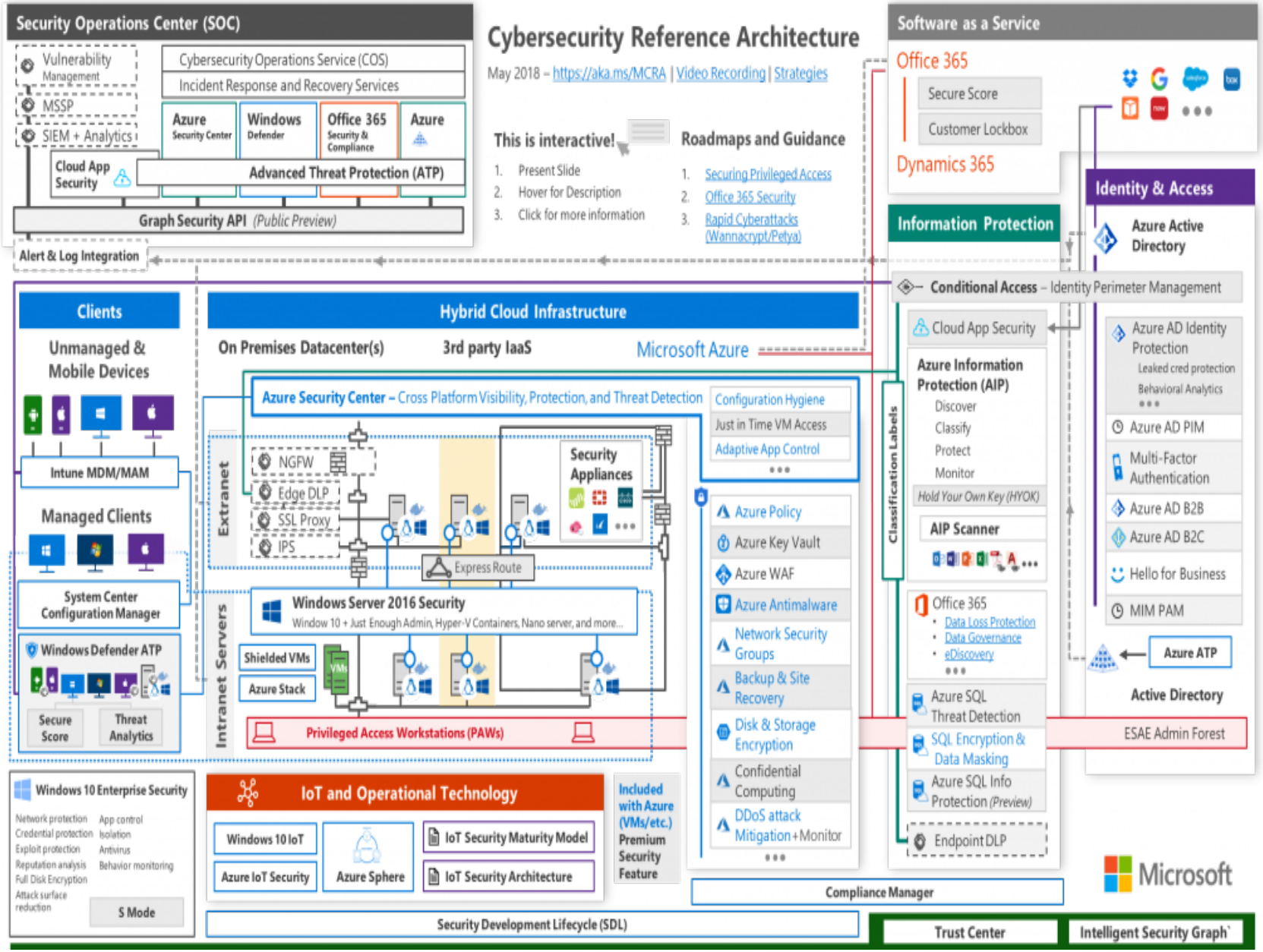
Digital Forensics Steps

The process of digital forensics is typically as follows:



Levels of law Enforcement Expertise




Security Operations Center (SOC)
Vulnerability Management
MSSP
SIEM + Analytics
Cybersecurity Operations Service (COS)
Incident Response and Recovery Services
Azure Security Center
Windows Defender
Office 365 Security & Compliance
Azure
Cloud App Security
Advanced Threat Protection (ATP)
Graph Security API (Public Preview)
Alert & Log Integration
Cybersecurity Reference Architecture
May 2018 – https://aka.ms/MCRA | Video Recording | Strategies
This is interactive!
1. Present Slide
2. Hover for Description
3. Click for more information
Roadmaps and Guidance
1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)
Software as a Service
Office 365
Secure Score
Customer Lockbox
Dynamics 365
Identity & Access
Azure Active Directory
Information Protection
Conditional Access – Identity Perimeter Management
Clients
Unmanaged & Mobile Devices
Intune MDM/MAM
Managed Clients
System Center Configuration Manager
Windows Defender ATP
Secure Score
Threat Analytics
Hybrid Cloud Infrastructure
On Premises Datacenter(s)
3rd party IaaS
Microsoft Azure
Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection
Configuration Hygiene
Just in Time VM Access
Adaptive App Control
Extranet
NGFW
Edge DLP
SSL Proxy
IPS
Security Appliances
Express Route
Intranet Servers
Windows Server 2016 Security
Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...
Shielded VMs
Azure Stack
Privileged Access Workstations (PAWs)
Azure Policy
Azure Key Vault
Azure WAF
Azure Antimalware
Network Security Groups
Backup & Site Recovery
Disk & Storage Encryption
Confidential Computing
DDoS attack Mitigation+Monitor
Classification Labels
Cloud App Security
Azure Information Protection (AIP)
Discover
Classify
Protect
Monitor
Hold Your Own Key (HYOK)
AIP Scanner
Office 365
Data Loss Protection
Data Governance
eDiscovery
Azure SQL Threat Detection
SQL Encryption & Data Masking
Azure SQL Info Protection (Preview)
Endpoint DLP
Azure AD Identity Protection
Leaked cred protection
Behavioral Analytics
Azure AD PIM
Multi-Factor Authentication
Azure AD B2B
Azure AD B2C
Hello for Business
MIM PAM
Azure ATP
Active Directory
ESAE Admin Forest
Windows 10 Enterprise Security
Network protection
Credential protection
Exploit protection
Reputation analysis
Full Disk Encryption
Attack surface reduction
App control
Isolation
Antivirus
Behavior monitoring
S Mode
IoT and Operational Technology
Windows 10 IoT
Azure IoT Security
Azure Sphere
IoT Security Maturity Model
IoT Security Architecture
Included with Azure (VMs/etc.) Premium Security Feature
Compliance Manager
Security Development Lifecycle (SDL)
Trust Center
Intelligent Security Graph
Microsoft

Investigation Steps

Stage 1 Investigation preparation	a) Identify the purpose of the investigation b) Identify resources required
Stage 2 Evidence Acquisition	a) Identify sources of digital evidence b) Preserve digital evidence
Stage 3 Analysis of evidence	a) Identify tools and techniques to use b) Process data c) Interpret analysis results
Stage 4 Results dissemination	a) Report findings b) Present findings

Testing of the Procedure Used

1. Error Rate

Is there a known error rate of the procedure?

2. Publication

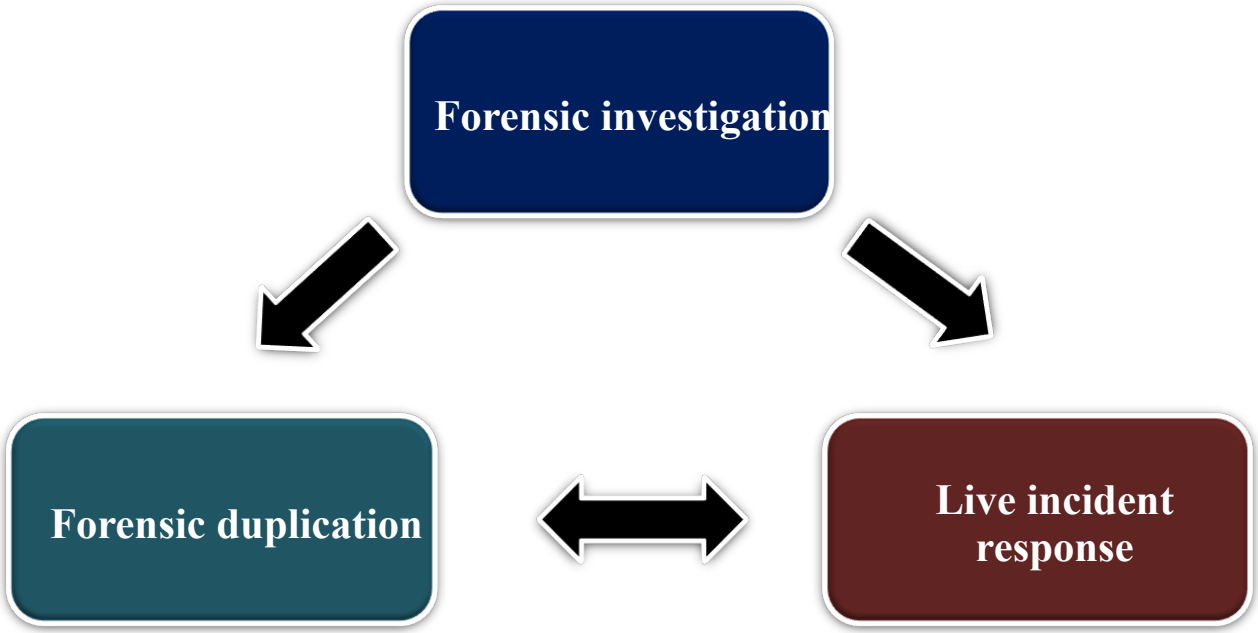
Has the procedure been published and subject to peer review?

3. Acceptance

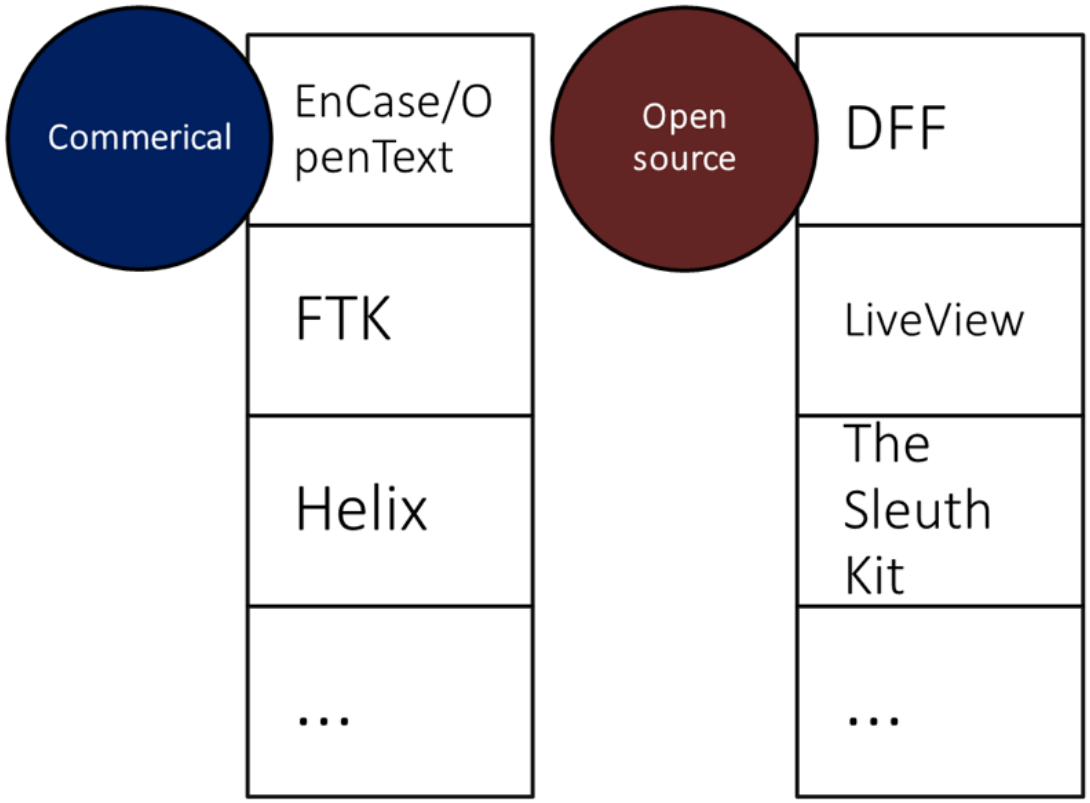
Is the procedure generally accepted in the relevant scientific community?

Techniques Used

- Main techniques used are **forensic duplication** and **live incident response**



Digital Forensics Tools



Thank You