DOMAIN 4

PROVEN FAST, EFFECTIVE & AFFORDABLE EXAM PREP

SECURITY+

EXAM

CRAM

CompTIA Security+

with Pete Zerger CISSP, vCISO, MVP

EXAM OBJECTIVES (DOMAINS)

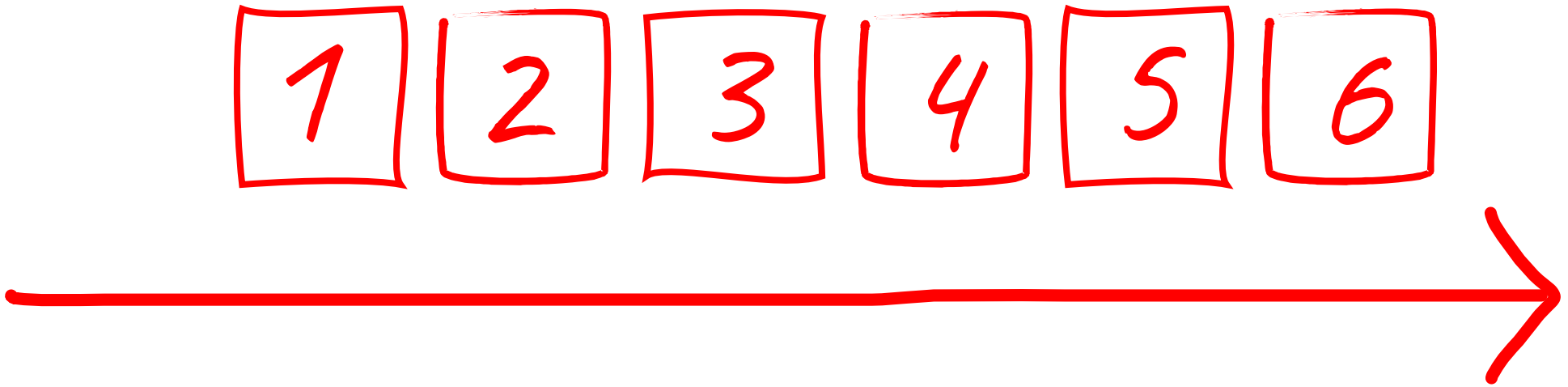
DOMAIN	WEIGHT
1.0 Attacks, Threats, and Vulnerabilities	24%
2.0 Architecture and Design	21%
3.0 Implementation	25%
4.0 Operations and Incident Response	16%
5.0 Governance, Risk, and Compliance	14%

EXAM OBJECTIVES (DOMAINS)

DOMAIN	WEIGHT
1.0 Attacks, Threats, and Vulnerabilities	24%
2.0 Architecture and Design	21%
3.0 Implementation	25%
4.0 Operations and Incident Response	**16%**
5.0 Governance, Risk, and Compliance	14%

INTRODUCTION: SERIES OVERVIEW

LESSONS IN THIS SERIES



Intro + one lesson for each exam domain

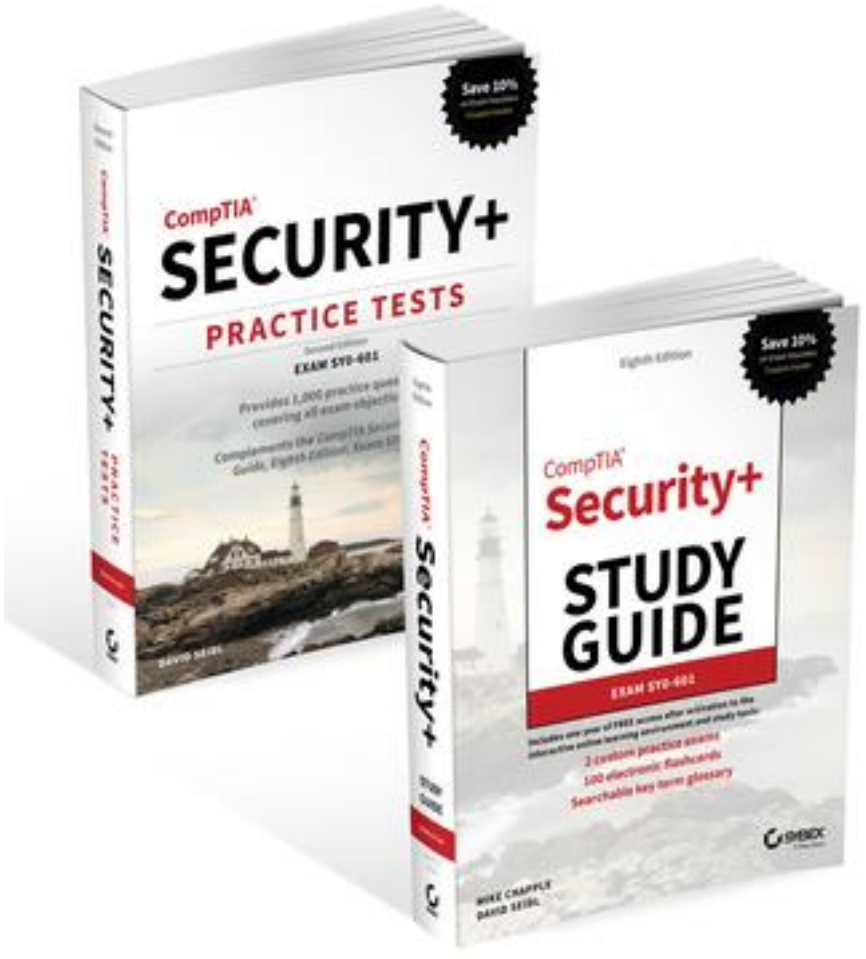
+ 5-10 shorter supplemental lessons

CompTIA Security+ Exam Cram

EXAM NUMBER: SY0-601

- 4.0 Operations and Incident Response

Covering all topics in the official Security+ exam objectives

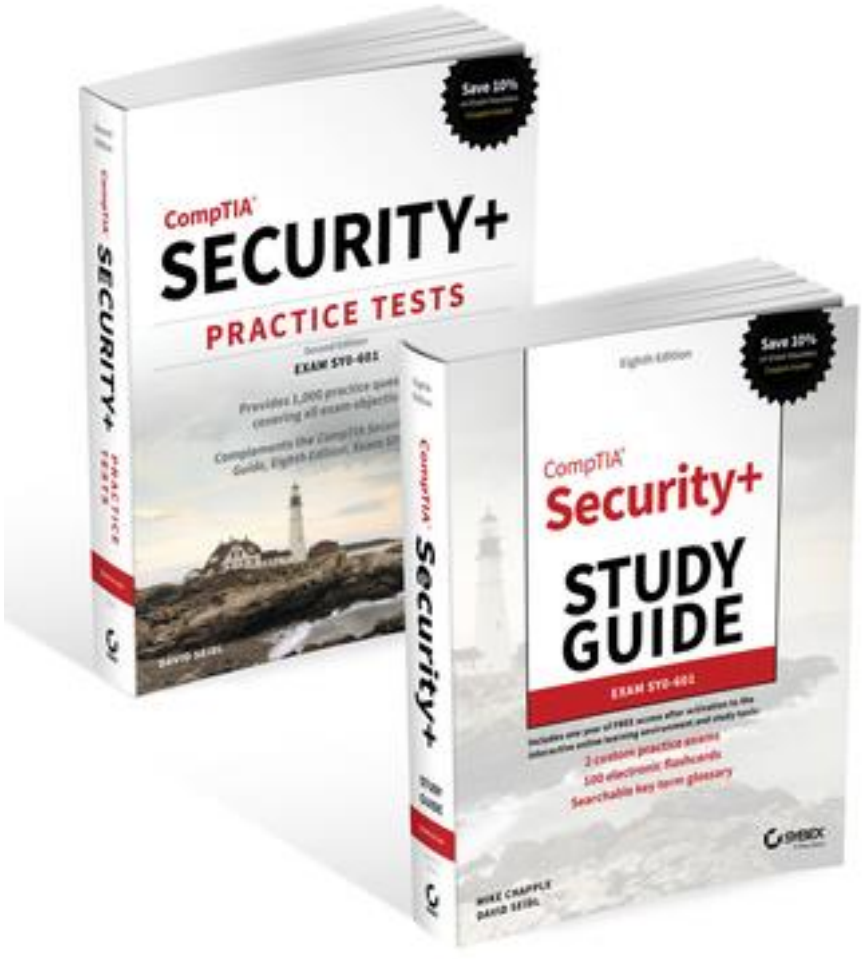


SECURITY+
EXAM STUDY GUIDE
& PRACTICE TESTS BUNDLE

1,000 flashcards

1,000 practice questions

2 practice exams



SECURITY+
EXAM STUDY GUIDE
& PRACTICE TESTS BUNDLE

1,000 flashcards

1,000 practice questions

2 practice exams

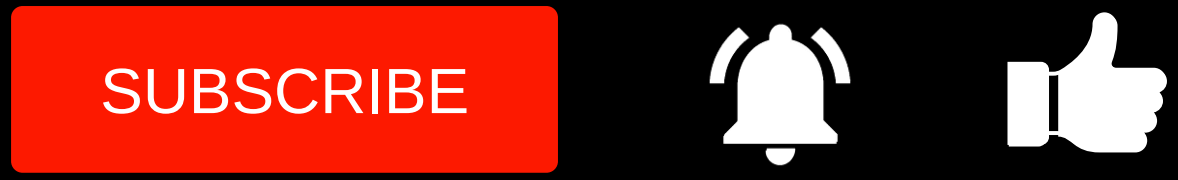
Includes 10% exam discount coupon

SECURITY+
EXAM STUDY GUIDE
& PRACTICE TESTS BUNDLE

BUY IT NOW AT amazon.com

link to the 2021 exam bundle in the video description!

A pdf copy of the presentation is available in the video description!



4.0 OPERATIONS AND INCIDENT RESPONSE

4.1 Given a scenario, use the appropriate tool to assess organizational security

- **Network reconnaissance and discovery**
  - tracert/traceroute
  - nslookup/dig
  - ipconfig/ifconfig
  - nmap
  - ping/pathping
  - hping
  - netstat
  - netcat
  - IP scanners
  - arp
  - route
  - curl
  - theHarvester
  - sn1per
  - scanless
  - dnsenum
  - Nessus
  - Cuckoo
- **File manipulation**
  - head
  - tail
  - cat
  - grep
  - chmod
  - logger
- **Shell and script environments**
  - SSH
  - PowerShell
  - Python
  - OpenSSL
- **Packet capture and replay**
  - Tcpreplay
  - Tcpdump
  - Wireshark
- **Forensics**
  - dd
  - Memdump
  - WinHex
  - FTK imager
  - Autopsy
- **Exploitation frameworks**
- **Password crackers**
- **Data sanitization**

Hands-on learning will be helpful!

Do NOT use active reconnaissance tools to explore or exploit resources without permission

NETWORK RECONNAISSANCE AND DISCOVERY

Tracert/Traceroute: This shows the route taken from a computer to a remote host such as a website.

It also shows response latency (in ms) at each hop.

Nslookup: Nslookup is a diagnostic tool for verifying the IP address of a hostname (A record by default) in the DNS server database.

Using the `set type=` command, you can change the type of records it searches. "Set type=MX" scopes search to mail exchange records

Dig: Dig is the equivalent of nslookup in a Linux/Unix environment.

ipconfig/ifconfig: These commands show the IP configuration. The Windows version is `ipconfig`, but Unix/Linux can use `ifconfig`.

Nmap: a free and open-source network mapper that can be used to create an inventory of devices on your network

Also good for banner grabbing (computer and service info).

NETWORK RECONNAISSANCE AND DISCOVERY

Pathping: has the functionality of both `ping` and `tracert`.

also calculates statistics after the trace, showing the packet loss at each router (each hop) it passes through.

Hping: an open-source packet generator and analyzer for the TCP/IP protocol, often used for auditing firewalls and networks.

for example, testing firewall rules and open ports, and analyzes network traffic, including packet formats and traceroute.

Netstat: a native tool on Windows operating system.

used to see the established connections, listening ports, and even running services.

Netstat shows listening ports and established connections, but if you reboot the computer, the established connections disappear.

NETWORK RECONNAISSANCE AND DISCOVERY

netcat: or `nc`, is a Linux/UNIX utility for showing network connections, port scanning, and even file transfer.

IP Scanners: the Angry IP scanner is a popular free and open-source, that will scan addresses in a range and ID open ports.

will export results to TXT, CSV, or XML format.

Comes in command line and GUI versions

Address Resolution Protocol (**ARP**): a protocol for mapping an IP address to a physical MAC address on a local area network.

the `arp -a` command shows the ARP cache.

route. enables listing existing routes in the local routing table, as well as adding manual entries into the network routing tables.

`route print` to view local route table, `route add` to add a route

NETWORK RECONNAISSANCE AND DISCOVERY

Curl: command-line tool used to transfer data using any of these supported protocols:

HTTP, FTP, IMAP, POP3, SCP, SFTP, SMTP, TFTP, TELNET, LDAP, or FILE

TheHarvester: This is a passive tool that comes with Kali Linux used to harvest the email addresses of an organization.

EXAMPLE: search for email addresses in kali.org domain, limiting results to 500, using Google:

```
theharvester -d kali.org -l 500 -b google
```

You can run Linux on Windows 10 or 11 using the Windows Subsystem for Linux (WSL). Includes a Kali Linux distribution

NETWORK RECONNAISSANCE AND DISCOVERY

Sn1per: a penetration test reconnaissance tool that can be used for automated tests.

can scan for vulnerabilities, open ports, web application vulnerabilities and perform attack surface discovery.

dynamic code analysis

used by pen testers, bug bounty researchers, and red teams.

all-in-one offensive security tool with free and paid versions

Scanless: pentesting tool to perform anonymous open port scans on target hosts, such as web servers. (free and open-source)

developed in Python, utilizes a number of port scanners, like ipfingerprints, pingeu, spiderip, portcheckers

NETWORK RECONNAISSANCE AND DISCOVERY

Dnsenum: is a command-line tool that automatically identifies basic DNS records and it has the ability to attempt reverse DNS resolution.

brute forces (queries for the existence of hostnames) in order to get their IP address of subdomains and hostnames.

used in web penetration testing to identify potential targets for further exploration.

Nessus: a network security (vulnerability) scanner. It utilizes plug-ins, which are separate files, to handle the vulnerability checks.

raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access.

Cuckoo: This tool creates a sandbox that can be used for analyzing files for malware inspection.

FILE MANIPULATION

You may want to look deeper into different files, including the log files that are produced. Here are a few tools in the **file manipulation** category.

Concatenate (cat): The `cat` command in Linux can be used to create files, view files, and also concatenate several files into another file.

To create a new file called `weblog`, we use the following syntax:

```
cat > weblog
```

You can also concatenate the contents of three files and combine them in an output file using the following syntax:

```
cat file1.txt file2.txt file3.txt | sort > samplefile.txt
```

Head: the `/var/log/messages` file is an important log file, which shows system events such as shutdown and reboot.

We can use the `head` command to check the top 10 messages from that log

```
head /var/log/messages -n 10
```

FILE MANIPULATION

Tail: views the last X lines at the end of a log file

EXAMPLE: view the last 10 messages in the `/var/log/messages` log file:

```
tail /var/log/messages -n 10
```

Grep: used to search text and log files for specific values.

EXAMPLE: search a file called **users.txt** for the name `PETE`, we would use the following syntax:

```
grep -f PETE users.txt
```

EXAMPLE: search a whole directory for the word `project`, we can use the following syntax:

```
grep -r project
```

FILE MANIPULATION

chmod: The `chmod` command is used to change the permission level, for example:

```
chmod 766
```

Linux permissions covered briefly in Domain 3

In example above, the *owner* has `rwx`, the *group* has `rw-`, and *others* have `rw-`.

Logger: can add a message to the local system log file or to a remote syslog server.

Frequently used to send log messages from automation scripts to record actions performed and errors encountered.

EXAMPLE:

```
logger -n 10.10.10.10 'hostname' found a potential backdoor attack
```

The tools in this category are core (everyday) commands present in just about any flavor of Linux

SHELL AND SCRIPT ENVIRONMENTS

SSH: created to serve as a secure alternative to telnet for running commands remotely; it is commonly used when you want remote access to network devices.

It can be used as a command-line tool or in a Graphical User Interface (GUI), but it is not browser-based. Unlike telnet, SSH traffic is encrypted

PowerShell: PowerShell can perform tasks in a Windows environment. Each command is known as a `cmdlet` and can be saved to a script with a `.ps1` extension.

Each PowerShell cmdlet is comprised of a noun and a verb.

EXAMPLE: `Get-Help` will show the help commands.

Python: a popular and powerful programming language used by open source developers, and data scientists. Widely used in cybersecurity

OpenSSL: a suite that can be used to create and manage Transport Layer Security (TLS) and Secure Socket Layer (SSL) protocol.

often used to generate private keys, create CSRs, install your SSL/TLS certificate, and identify certificate information. can create a self-signed certificate

PACKET CAPTURE AND REPLAY

A protocol analyzer can also be referred to as a *packet sniffer*.

Protocol analyzers can save the data that they collect to a packet capture file (PCAP).

tcpreplay: This is an open-source tool that can be used to analyze `.pcap` files generated by either Wireshark or `tcpdump`

It can then replay the traffic and send it to the NIPS.

tcpdump: a network packet analyzer command line tool on Linux/UNIX

EXAMPLE:

`tcpdump -i eth0` shows information on the first Ethernet adapter

Wireshark: a free and open-source packet analyzer, with command-line and GUI versions, available for Windows and Linux.

FORENSICS

Tools in the forensics category are often used in **forensic investigation**.

dd. when the forensics team needs to investigate an image on a desktop or laptop, the `dd` command can be used to clone a disk or copy a folder in a Linux/Unix environment.

In a SCSI environment, the first disk is `/dev/sda`, the second as `/dev/sdb`,
If the first disk has two partitions, they will be `sda1` and `sda2`.

The `if` command is the input file and the `of` command represents the output file.

Copy Entire Hard Disk: We are going to copy the first SCSI disk to the second SCSI disk. The syntax would be:

```
dd if = /dev/sda of = /dev/sdb
```

Create an Image: We are going to make a disk image of `/dev/sda`. We would use the this syntax:

```
dd if=/dev/sda of=~/sdadisk.img
```

FORENSICS

Tools in the forensics category are often used in **forensic investigation**.

WinHex: a hexadecimal editor that can be used on any version of Windows operating systems to help forensics teams find evidence.

can be used to find and recover deleted or lost data from a corrupt drive.

Capturing System Memory Dump Files:
When a computer system crashes (commonly known as the *blue screen of death*), all of the content of the memory is saved in a dump file (`.dmp`).

dump files can be analyzed by using a tool such as **`BlueScreenReview`**.

the Linux equivalent is **`memdump`**.

FTK imager: a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool is warranted.

Autopsy: can be used to analyze hard drives, smartphones, and media cards.

has a built-in translator to translate foreign languages into English.

EXPLOITATION FRAMEWORKS

Exploitation framework tools

such as the open-source **Metasploit Framework**, contain capabilities to detect and then exploit vulnerabilities on remote systems.

can be used to harden your IT systems before they are attacked.

use information from the National Vulnerability Database, which is comprised of **Common Vulnerabilities and Exposures** (**CVE**)

Uses the **Common Vulnerability Scoring System** (**CVSS**), to show the level of severity of each of the vulnerabilities.

MOST POPULAR EXPLOIT FRAMEWORKS

Metasploit Framework (http://www.metasploit.com)
CORE IMPACT (http://www.coresecurity.com)
Immunity CANVAS (http://www.immunitysec.com)

PASSWORD CRACKERS AND DATA SANITIZATION

Password Crackers

such as the **Cain** portion of Cain and Able or **LOphtcrack**, can be used to crack the passwords and create password hashes.

In the Security+ exam, when you see names in clear text followed by hashes, the hash is a password hash.

Data sanitization

the process of irreversibly removing or destroying data stored on a memory device (hard drives, flash memory, SSDs, etc.)

It is important to use the proper technique to ensure that all data is purged.

4.0 OPERATIONS AND INCIDENT RESPONSE

4.2 Summarize the importance of policies, processes, and procedures for incident response

- **Incident response plans**
- **Incident response process**
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons learned

- **Exercises**
  - Tabletop
  - Walkthroughs
  - Simulations
- **Attack frameworks**
  - MITRE ATT&CK
  - The Diamond Model of Intrusion Analysis
  - Cyber Kill Chain

- **Stakeholder management**
- **Communication plan**
- **Disaster recovery plan**
- **Business continuity plan**
- **Continuity of operations planning (COOP)**
- **Incident response team**
- **Retention policies**

PLAN, PROCESS, AND PROCEDURE

Plan vs Process vs Procedure: *What is the difference?*

Plan High-level (light on the details)

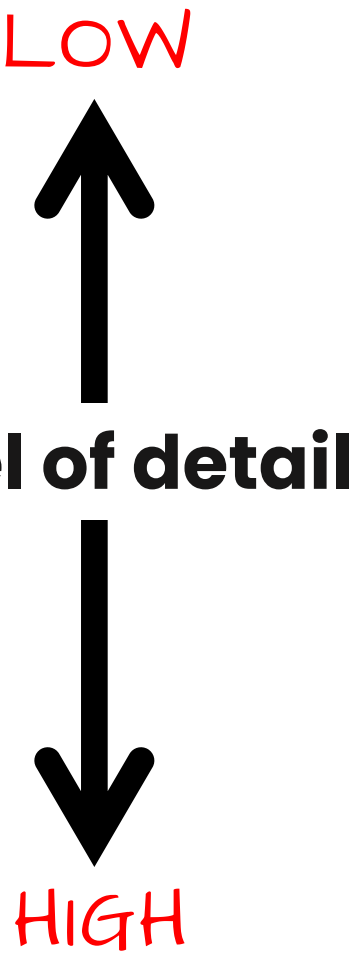
A set of intended actions, usually mutually related, through which one expects to achieve a goal.

Process Ordered task list or flow chart

A series of related tasks or methods that together turn inputs into outputs.

Procedure Task-level details (the "HOW")

A prescribed way of undertaking a process or part of a process. A particular method for performing a task



MANAGING INCIDENT RESPONSE

6 phases of incident response

1	**Preparation**	Where incident response plans are written, and configurations documented.
2	**Identification**	determining whether or not an organization has been breached. Is it really an incident?
3	**Containment**	Limiting damage (scope) of the incident.
4	**Eradication**	Once affected systems are identified, coordinated isolation or shutdown, rebuild, and notifications.
5	**Recovery**	Root cause is addressed and time to return to normal operations is estimated and executed.
6	**Lessons Learned**	Helps prevent recurrence, improve IR process.

Types of incident response exercises

Tabletop Paper-based, hypothetical

You distribute copies of incident response plans to the members of the incident response team for review.

Team members then provide feedback about any updates needed to keep the plan current.

Walkthrough Test team response without full simulation

Members of the incident response team gather in a large conference room and role-play an incident scenario.

Usually, the exact scenario is known only to the test moderator, who presents the details to the team at the meeting.

Can ensure needed tools and resources are available, and team members are familiar with their roles.

Types of incident response exercises

Simulation

Similar to structured walkthrough, except some of the response measures are then tested (on non-critical functions).

This one involves some form of 'doing'

MITRE ATT&CK Framework

An online framework that can be used by commercial organizations.

Developed by MITRE, a US Government-sponsored company whose aim is to help prevent cyber-attacks.

Provides information about adversaries and their attack methods.

Uses the acronym ATT&CK to better articulate the attack vectors used by attackers:

Adversarial **T**actics, **T**echniques, **& C**ommon **K**nowledge

Adversarial: This looks at the behavior of potential attackers who are put into different groups.

Tactics: the medium by which (how) the attack will be carried out.

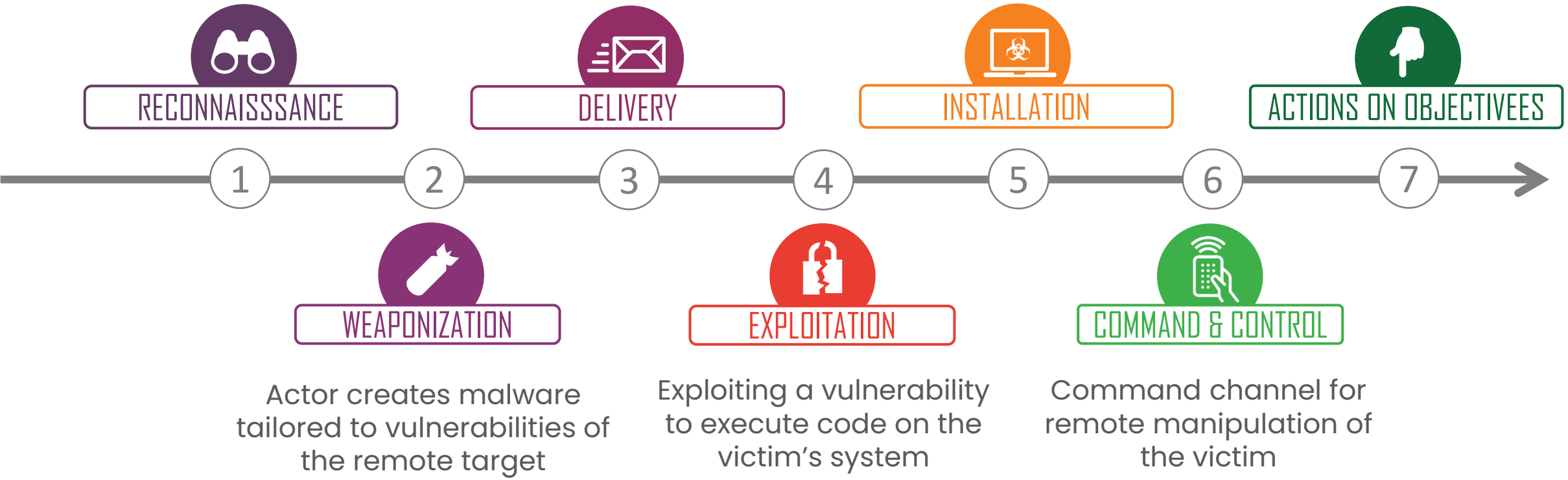
Techniques: a breakdown of the processes of how an attack will be launched.

Common Knowledge: documentation relating to the attackers' tactics and techniques that have been made available online to the general public.

The **Cyber Kill Chain**

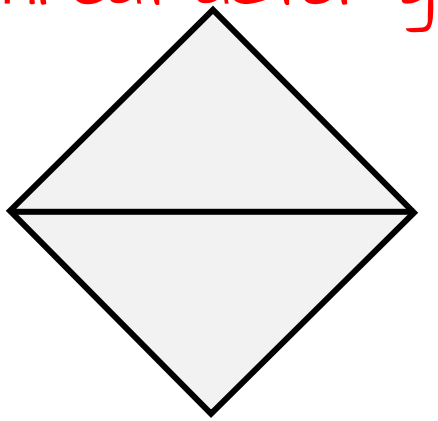
Lockheed Martin Edition

Traces stages of a cyberattack from early reconnaissance to the exfiltration of data



Diamond Model of Intrusion Analysis

A framework for gathering intelligence on network intrusion attacks, comprised four key elements:



Adversary
The threat actor group

Capabilities
where the adversary develops an exploit that they use to carry out the attack.

Infrastructure
This is how the attacker can get to the victim.

Victim
The person targeted by the adversary.

was used by the intelligence community until it was declassified in 2013.

Communication Plan

The plan that details how relevant stakeholders will be informed in event of an incident. (like a security breach)

Would include plan to maintain confidentiality, such as encryption to ensure that the event does not become public knowledge.

Contact list should be maintained that includes stakeholders from the government, police, customers, suppliers, and internal staff.

Compliance regulations, like GDPR, include notification requirements, relevant parties and timelines

Confidentiality amongst internal stakeholders is desirable so external stakeholders can be informed in accordance with the plan.

Stakeholder Management

When we have an incident, there are multiple groups of relevant stakeholders that we need to inform and manage, and may include:

- Internal stakeholders
- Cyber insurance provider
- Business partners
- Customers
- Law enforcement

A **stakeholder** is a party with an interest in an enterprise; corporate stakeholders include investors, employees, customers, and suppliers.

Regulated industries, such as banking and healthcare will have requirements driven by the regulations governing their industries.

BCP DEFINITIONS

Some BCP-related definitions worth knowing

BCP (Business Continuity Plan)
the overall organizational plan for "how-to" continue business.

DRP (Disaster Recovery Plan)

the plan for recovering from a disaster impacting IT and returning the IT infrastructure to operation.

COOP (Continuity of Operations Plan)

the plan for continuing to do business until the IT infrastructure can be restored.

BCP vs DRP

Business Continuity Planning (BCP) vs Disaster Recovery Planning (DRP) – What is the difference?

BCP focuses on the whole business

DRP focuses more on the technical aspects of recovery

BCP will cover communications and process more broadly

BCP is an umbrella policy and DRP is part of it

INCIDENT RESPONSE TEAM

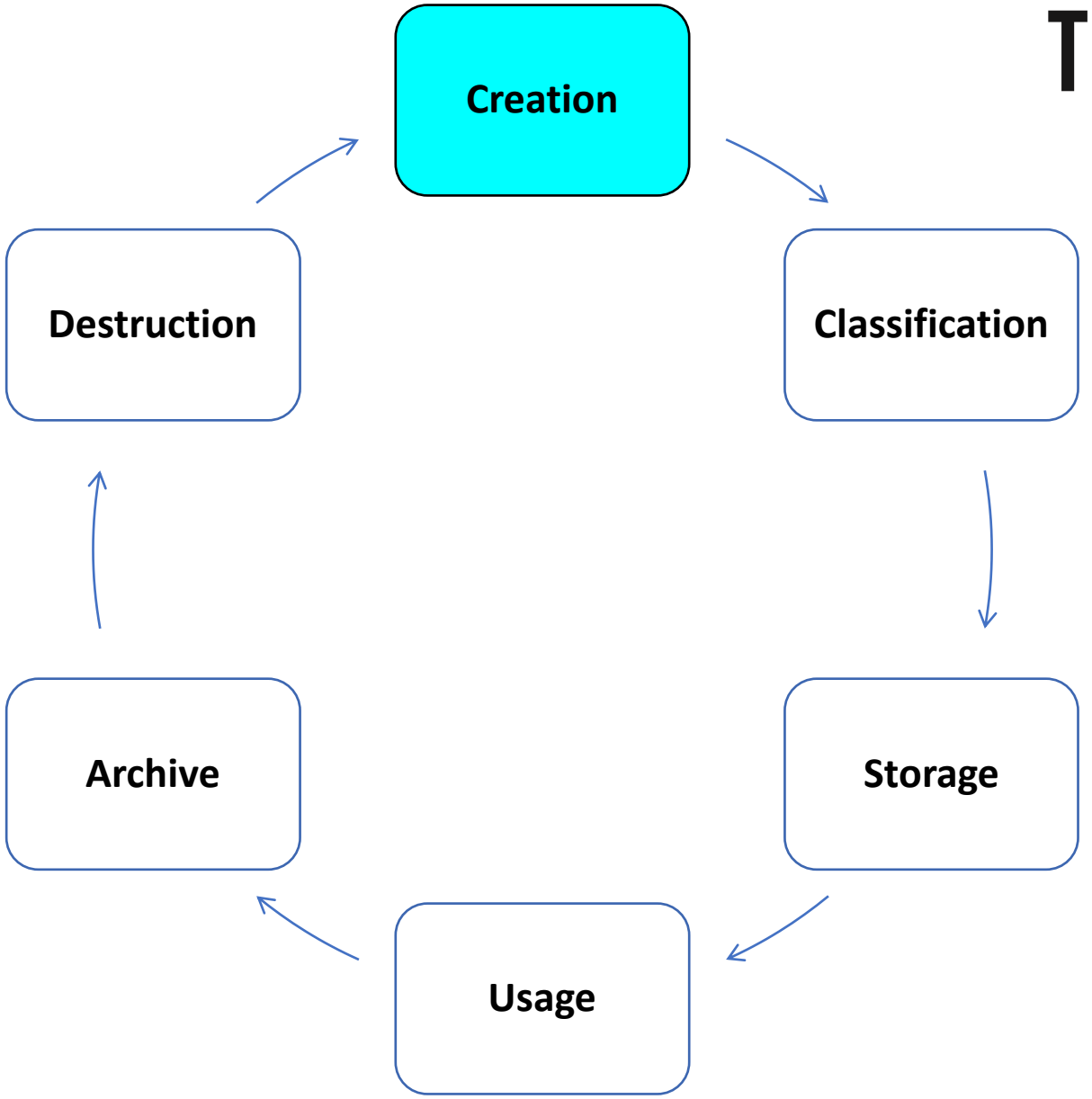
When an incident occurs, it is important to get an incident response team together to deal with the incident.

Includes the following roles:

Incident Response Manager: A top-level manager who takes charge.
Security Analyst: Technical support to the incident.
IT Auditor: Checks that the company is compliant.
Risk Analyst: Evaluates all aspects of risk.
HR: Sometimes employees are involved in the incident.
Legal: Gives advice and makes decisions on legal issues.
Public Relations: Deals with the press to reduce the impact.

THE INFORMATION LIFECYCLE

(from a functional perspective)



Can be created by **users**

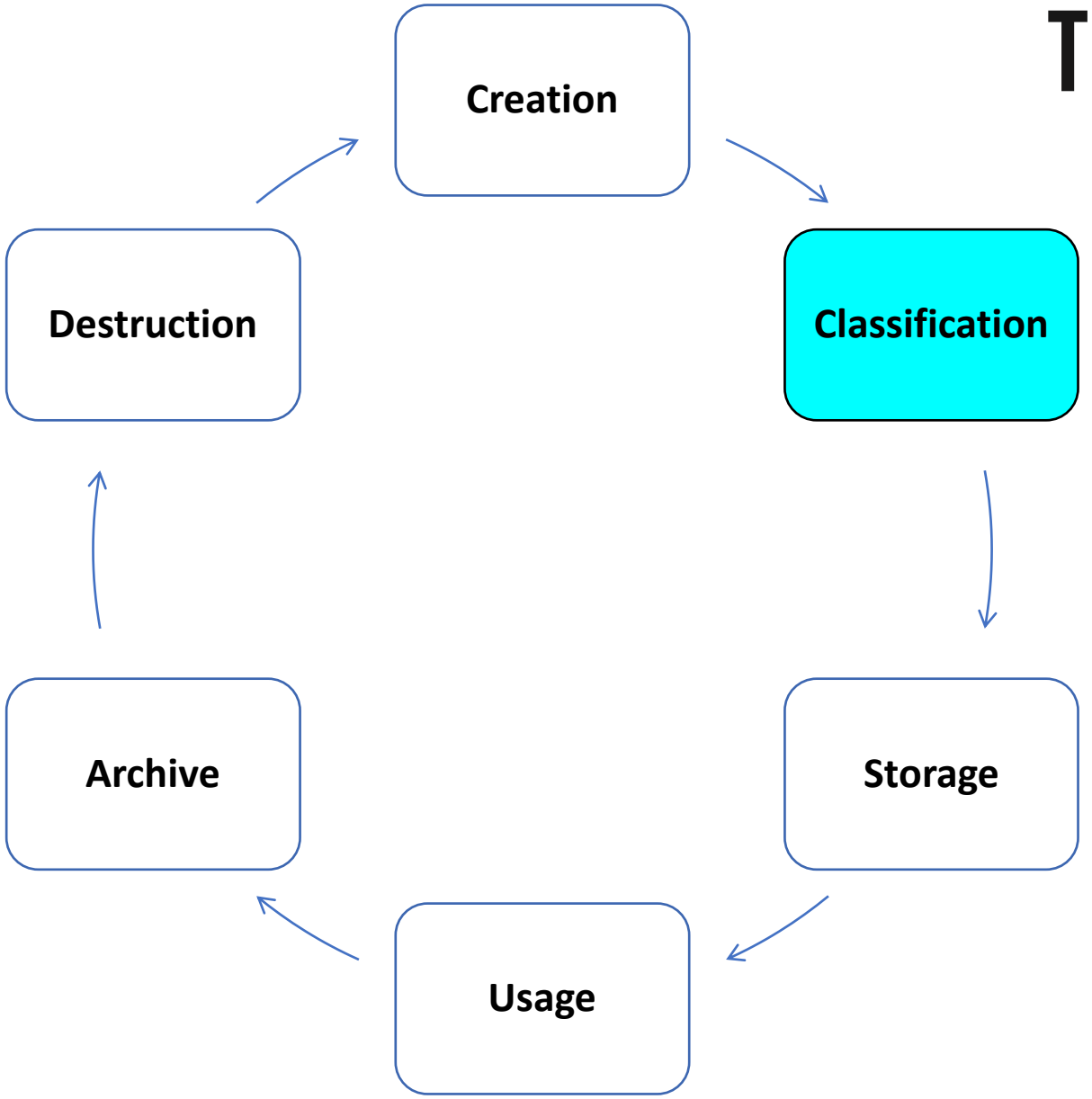
a user creates a file

Can be created by **systems**

a system logs access

THE INFORMATION LIFECYCLE

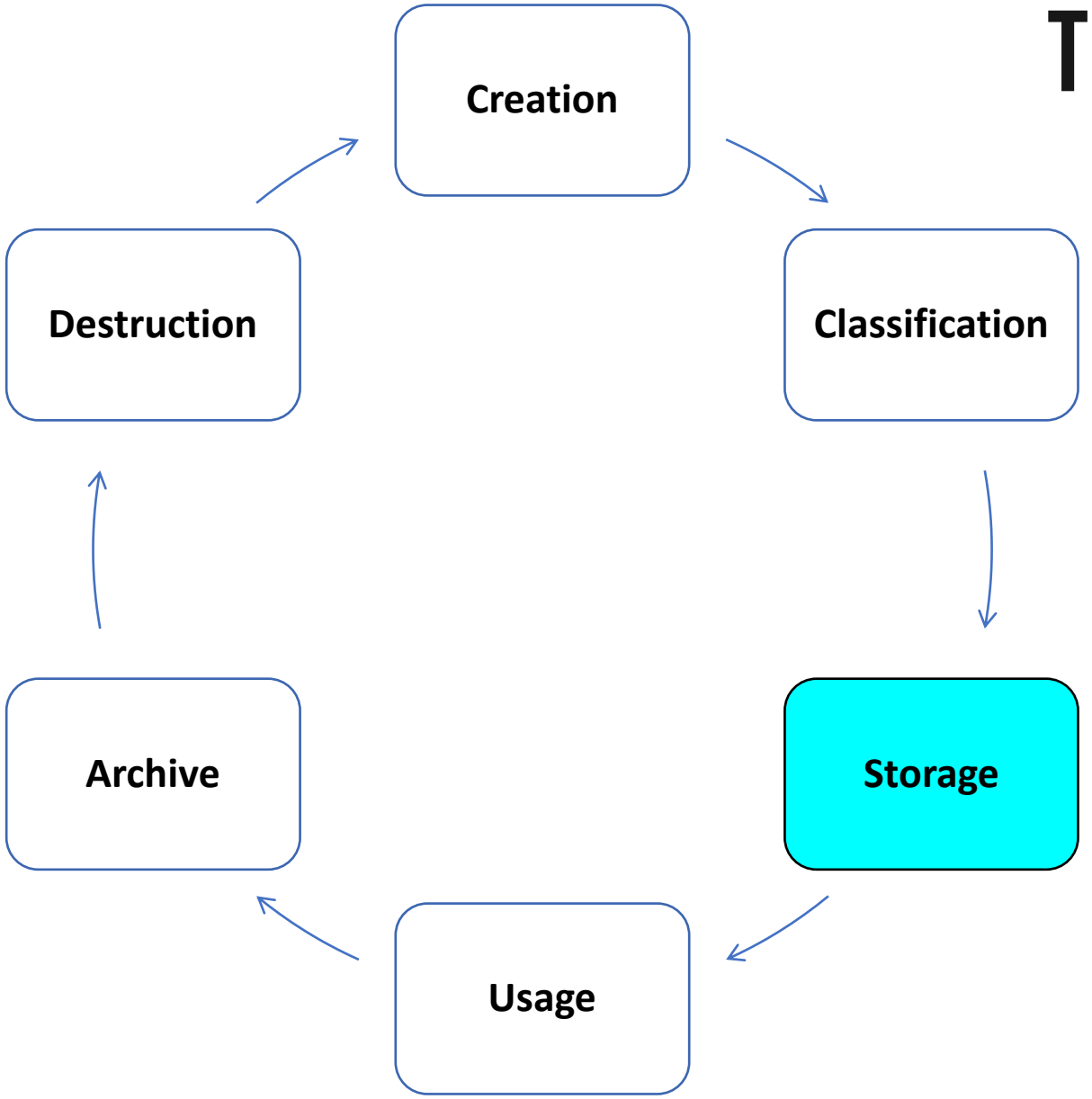
(from a functional perspective)



To ensure it's handled properly, it's important to ensure data is **classified** as soon as possible.

THE INFORMATION LIFECYCLE

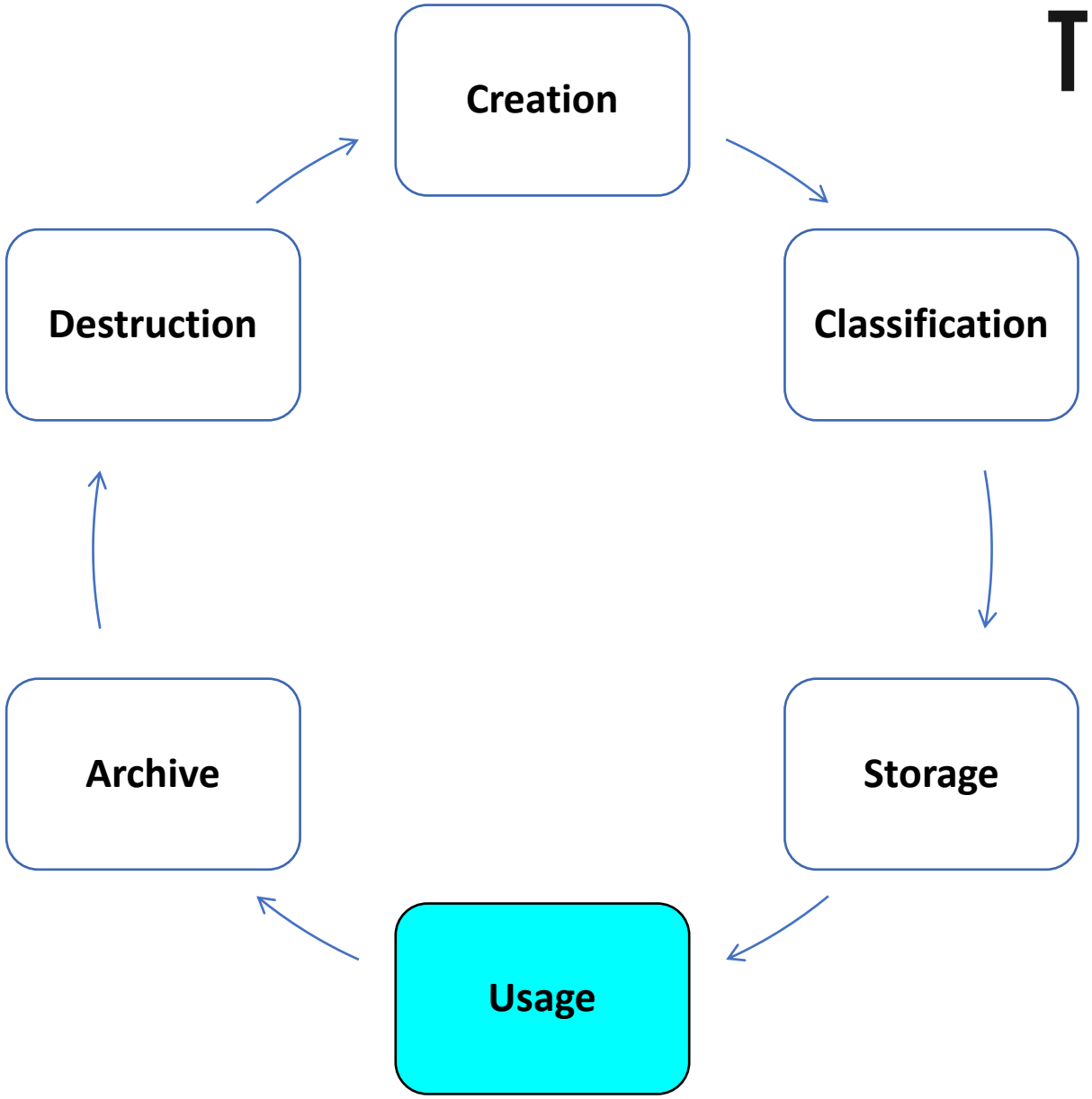
(from a functional perspective)



Data should be **protected** by adequate security controls based on its classification.

THE INFORMATION LIFECYCLE

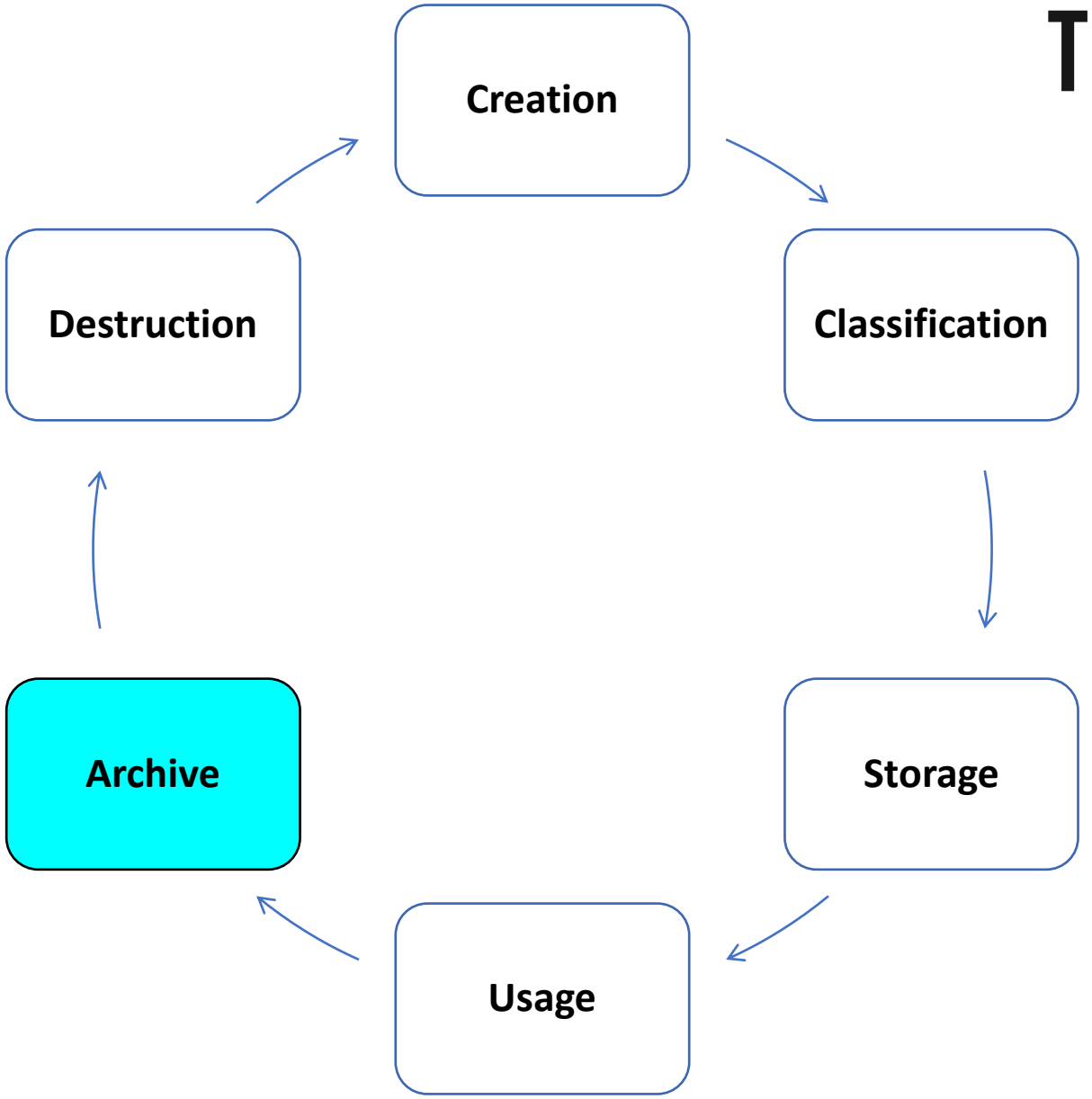
(from a functional perspective)



refers to anytime data is in use or in transit over a network.

THE INFORMATION LIFECYCLE

(from a functional perspective)



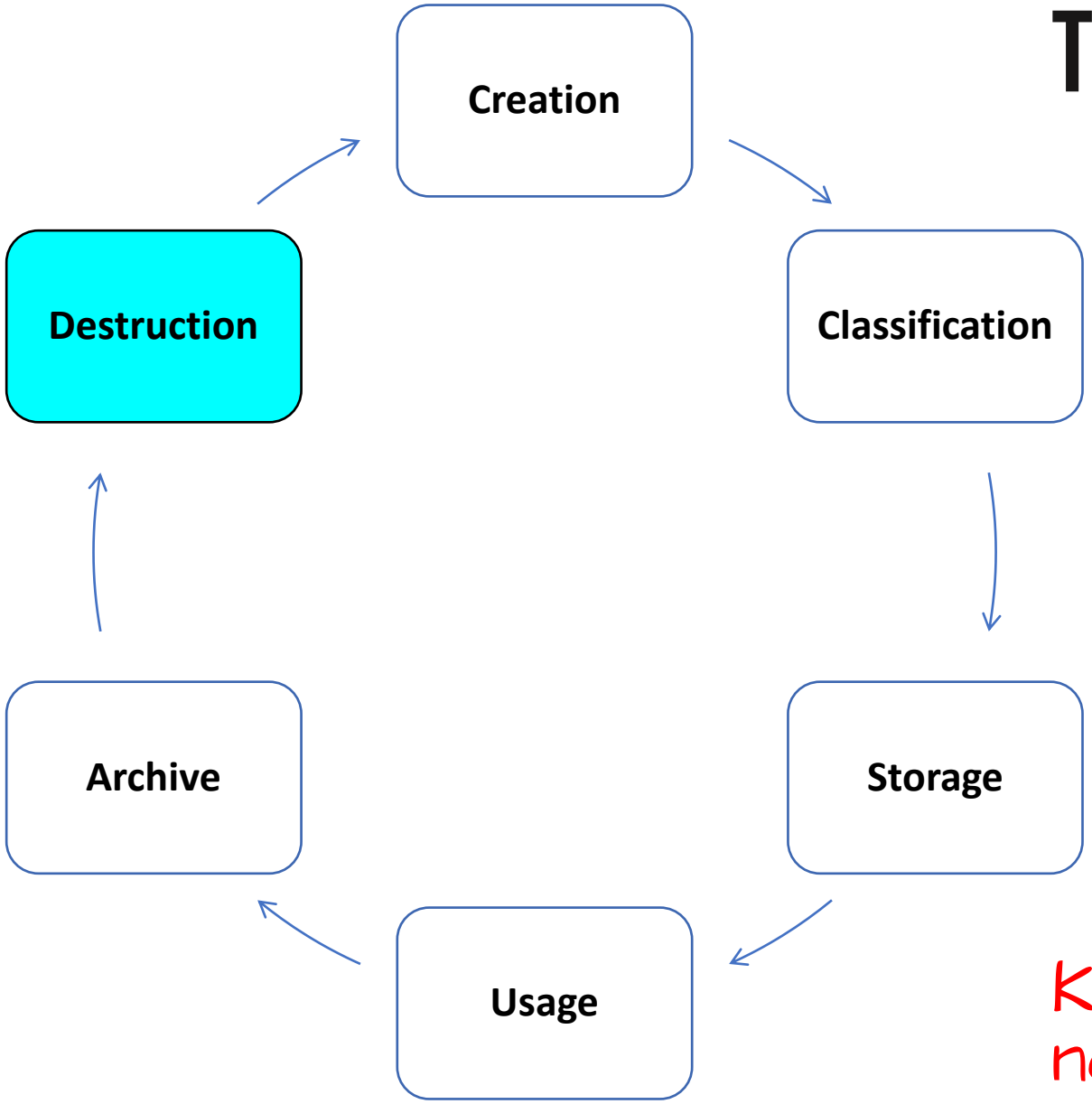
archival is sometimes needed to **comply** with laws or regulations requiring the retention of data.

a **data retention policy** ensures a company retains data as long as necessary.

"as long as necessary" is defined by company policies or regulatory requirements.

THE INFORMATION LIFECYCLE

(from a functional perspective)

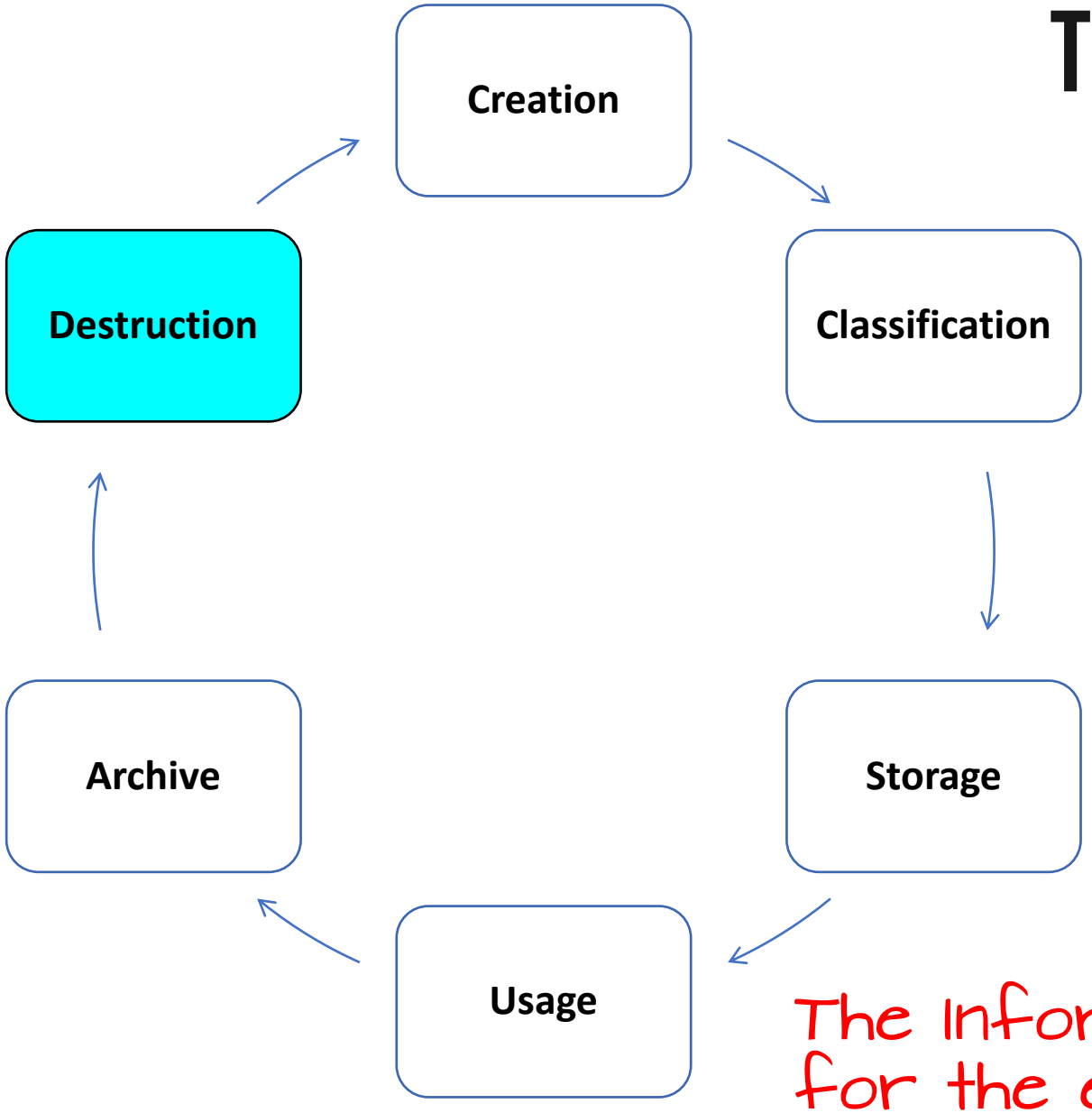


When data is no longer needed, it should be destroyed in such a way that it is not readable.

Keeping data longer than necessary increases risk

THE INFORMATION LIFECYCLE

(from a functional perspective)



When data is no longer needed, it should be destroyed in such a way that it is not readable.

The Information Lifecycle to know for the exam is covered in DOMAIN 5

RETENTION POLICY

Data classification

More on classifications in Domain 5

Labeling / tagging of data based on type, like personally identifiable info (PII), protected health info(PHI), etc.

Regulatory compliance

for legal and compliance reasons, you may need to keep certain data for different periods of time.

EXAMPLES:

some financial data needs to be retained for 7 years

Some medical data may need to be retained up to 20-30 years.

Data retention policy

ensure that legal and compliance issues are addressed.

4.0 OPERATIONS AND INCIDENT RESPONSE

4.3 Given an incident, utilize appropriate data sources to support an investigation

- **Vulnerability scan output**
- **SIEM dashboards**
  - Sensor
  - Sensitivity
  - Trends
  - Alerts
  - Correlation
- **Log files**
  - Network
  - System
  - Application
  - Security
  - Web
  - DNS
  - Authentication
  - Dump files
  - VoIP and call managers
  - Session Initiation Protocol (SIP) traffic
- **syslog / rsyslog / syslog-ng**
- **journalctl**
- **NXLog**
- **Bandwidth monitors**

Metadata
- Email
- Mobile
- Web
- File

Netflow / sFlow
- Netflow
- sFlow
- IPFIX

Protocol analyzer output

VULNERABILITY SCAN OUTPUT

A **vulnerability scanner** can identify and report various vulnerabilities before they are exploited, such as:

Examples include:
-software flaws
-missing patches
-open ports
-services that should not be running
-weak passwords

will help companies avoid known attacks such as SQL injection, buffer overflows, denial of service, and other type of malicious attacks.

A **credentialed vulnerability scan** is the most effective as it provides more information than any other vulnerability scan.

SIEM DASHBOARDS

dashboards are very useful to the security operations centers as they provide centralized visibility and information on threats in real time.

Sensor: Sensors are deployed across your network to monitor and collect changes in network patterns or monitor changes in log file entries as events occur.

Varies by solution and device. May be a sensor, syslog, text log, API or other format.

Sensitivity: can monitor PII, PHI, and other sensitive information to ensure regulatory compliance (HIPAA, PCI DSS, GDPR)

Trends: can identify trends in network traffic, event volume, or changes in activities/ activity levels across identities, endpoints, network and infrastructure.

Alerts: provide information about events on hosts and network devices.

Email notification and response automation (playbooks, SOAR) optional.

Correlation: correlates, aggregates, and analyzes the log files from multiple sources can generate a broad, centralized view.

Because sequence of events crosses multiple sources, time sync matters (NTP).

LOG FILES

Log files play a core role in providing evidence for investigations. You'll want to be familiar with the many different types of log files for the Security+ exam.

Network: This log file can identify the IP and MAC addresses of devices that are attached to your network. Usually sent to a central syslog server

NIDS/NIPS can be important in identifying threats and anomalies from these.

log files from a proxy server can reveal who's visiting malicious sites.

The collective insight may be useful in stopping DDoS attack

Web: web servers log many types of information about the web requests, so evidence of potential threats and attacks will be visible here.

information collected about each web session: IP address request, Date and time, HTTP method, such as GET/POST, Browser used, and HTTP Status code.

400 series HTTP response codes are client-side errors

500 series HTTP response codes are server-side errors

These logs must be fed to a SIEM, IDS/IPS or other system to analysis this data

LOG FILES

These files exist on client and server systems. Sending these to a SIEM can help establish a central audit trail and visibility into the scope of an attack.

System: contains information about hardware changes, updates to devices, and time synchronization, group policy application, etc.

Application: contains information about software applications, when launched, success or failure, and warnings about potential problems or errors.

Security: contains information about a successful login, as well as unauthorized attempts to access the system and resources.

can identify attackers trying to log in to your computer systems.

captures information on file access and can determine who has downloaded certain data.

You will find log files with these names in the Event Viewer on any Windows client or server

LOG FILES

Log files play a core role in providing evidence for investigations. You'll want go be familiar with the many different types of log files for the Security+ exam.

DNS: contains virtually all DNS server-level activity, such as zone transfer, DNS server errors, DNS caching, and DNSSEC.

DNS query logging often disabled by default due to volume.

Authentication: information about login events, logging success or failure.

multiple sources authenticating log files in a domain environment, including RADIUS, Active Directory, and cloud providers Azure Active Directory.

Dump Files: file generated when a computer crashes, with contents in the memory are saved in a dump file (.dmp).

dump files can be analyzed by using a tool such as the BlueScreenReview, Windows Debugger, and Kernel Debugger.

LOG FILES

VoIP phones are embedded systems that must be secured

Log files related to voice applications can be valuable in identifying anomalous activity, unauthorized users, and even potential attacks

VoIP and Call Managers: These systems provide information on the calls being made and the devices that they originate from.

may also capture call quality by logging the Mean Optical Score (MOS), jitter, and loss of signal. Significant loss in quality may indicate attack

each call is logged (inbound and outbound calls), the person making the call, and the person receiving the call. Including long-distance calls

Session Initiation Protocol (SIP) Traffic: SIP is used for internet-based calls and the log files generally show:

the 100 events, known as the INVITE, the initiation of a connection, that relates to ringing.

the 200 OK is followed by an acknowledgement.

Large number of calls not connecting may indicate attack

SYSLOG / RSYSLOG / SYSLOG-NG

These log management solutions all perform the same basic functions – SYSLOG

Linux solutions

Syslog the original

is known as a log collector as it collects event logs from various devices and often sent to a central syslog server.

in the Linux version, it is implemented as syslogd or syslog daemon, which stores the log files in the `var/log/syslog` directory.

Rsyslog

called rocket-fast as it has a high performance.

receives data, transforms, and can send output to destinations such as a SIEM server or other syslog. Log forwarding

Syslog-ng

an open-source logging solution for Unix and Linux systems.

broader platform support than Rsyslog.

Great open-source options that came later

JOURNALCTL AND NXLOG

Other logging solutions

provides several system components for Linux

journalctl

a utility for querying and displaying logs from journald, which is **systemd's** logging service.

`journald` collects and stores log data in binary format.

`journalctl` is used to query and display these logs in a readable format.

NXLog

an open-source log management tool that helps identify security risks in a Linux/ Unix environment.

a multi-platform log collection and centralization tool that offers log processing features, including log enrichment and log forwarding.

similar to syslog-ng or Rsyslog but it is not limited to UNIX and syslog only.

Supports Linux, Windows, and Android

BANDWIDTH MONITORS

Bandwidth Monitors

can be used to understand your network traffic flow.

monitor changes in traffic patterns and identify devices on the network that are causing bottlenecks.

can detect broadcast storms and potential denial-of-service attacks.

a way for IT professionals to determine actual bandwidth availability on your systems.

METADATA

data that provides information about other data.

Email: headers contain detailed information, including source, destination, and route through the email providers to the recipient.

can be used when phishing emails are received to identify the bad actor

Mobile: Telecom providers retain information about phone calls, including calls made, calls received, text messages, internet usage, and location information.

can be used in an investigation to provide evidence of suspect's location

Web: Website metadata provides information about every page created on a website, including author, date created, images, and other files (videos, pdfs, etc.)

File: When investigations are being carried out, the file metadata can be used to track information such as the author, date created, date modified, and file size.

file metadata does not include info on actions like printing or copying

Photograph: When someone takes a photograph, the metadata might include geo-tagging that documents the location in which a photograph was taken.

you cannot get metadata from a deleted file after recovery

NETFLOW, SFLOW, IPFIX

Network monitoring solutions

Netflow

Proprietary

a CISCO product that monitors network traffic

can identify the load on the network.

in an investigation, it can help identify patterns in network traffic.

Sflow

Supports a wide variety of network hardware vendors

a multi-vendor product that provides visibility into network traffic patterns.

can help identify malicious traffic to help in securing the network.

IP Flow Information Export (IPFIX)

Open source, similar to and patterned after Netflow

can be used to capture traffic from the node itself.

data can then be exported to a collector within the node.

can be used to identify data traveling through a switch to facilitate billing.

can format IP Flow data and forward it to a collector.

PROTOCOL ANALYZER OUTPUT

Details on output format, compatibility and use in forensic investigation

A protocol analyzer can also be referred to as a *packet sniffer*.

Protocol analyzers can save the data that they collect to a packet capture file (.PCAP).

PCAP file format is a binary format, with support for nanosecond-precision timestamps

Wireshark, **Tcpreplay**, and **tcpdump** all support .PCAP format

Can be used for forensics by replaying network traffic sent to network devices from which they capture traffic.

Law enforcement has used PCAP data successfully in prosecuting cybercrime

4.0 OPERATIONS AND INCIDENT RESPONSE

4.4 Given an incident, apply mitigation techniques or controls to secure an environment

- **Reconfigure endpoint security solutions**
  - Application approved list
  - Application blocklist/deny list
  - Quarantine
- **Configuration changes**
  - Firewall rules
  - MDM
  - DLP
  - Content filter/URL filter
  - Update or revoke certificates
- **Isolation**
- **Containment**
- **Segmentation**
- **SOAR**
  - Runbooks
  - Playbooks

RECONFIGURE ENDPOINT SECURITY SOLUTIONS

When technologies change or we suffer a data breach, we might have to reconfigure the endpoint security solutions.

Approved Applications List

Where the approved applications are listed. If an application is not listed, it cannot be launched.

Application Block List/Deny List

List of apps deemed dangerous, such as certain offensive security tools. If the app is on the blocklist, the app cannot run.

Quarantine

When a device has been infected with a virus, it is removed from the network.

With Network Access Control (NAC) user is authenticated and device checked to confirm patched and compliant before being granted access.

Will be blocked and may be placed in a quarantine network for remediation.

CONFIGURATION CHANGES

As new attacks emerge, configuration changes may be necessary to secure the environment.

Firewall Rules will vary for network and host-based firewalls

can be used to block traffic and we can use either an MDM solution or group policy to change the configuration on endpoint devices.

Mobile Device Management (MDM)

can be used to push configuration changes to mobile devices.

can enforce device settings from password policy to blocking camera.

Data Loss Prevention (DLP)

policy-based protection of sensitive data, usually based on labels or pattern match. new patterns to identify sensitive data may emerge

Protects data at-rest or in-transit, in email, Intranet, cloud drives, etc.

CONFIGURATION CHANGES

As new attacks emerge, configuration changes may be necessary to secure the environment.

Content Filter/URL Filter

Changes in attacks, might require an update to the content filters on either a proxy server or a UTM firewall.

Some devices, like a NGFW, may automatically detect new threats and adjust accordingly

Update or Revoke Certificates:

Endpoints reporting a host or trust error may indicate a certificate problem.

This may require updating a certificate that has expired or revoke a certificate because it has been compromised.

Internet-facing services need a certificate issued by a commercial CA

ISOLATION

Isolation means blocking access altogether

Air gap endpoints are used to view classified data to isolate the endpoint from the network to protect against a network-based attack.

Air gap eliminates all network connectivity (wired, wi-fi)

The only way to add or extract data from an air gapped computer is by using a removable device such as a USB drive.

Requiring users entering an area for confidential meetings or to view secret research to place their phones in a faraday cage.

It blocks electromagnetic signals from entering or exiting the cage, rendering cellular signals useless

CONTAINMENT

Containment is about minimizing damage and limiting the scope of an incident.

Examples of containment

If an endpoint has been compromised and may be infected by a virus, IT Security will contain to stop the malware spreading.

removing infected machines from the network.

disabling user accounts that have been used to breach your network.

A containment process that minimizes downtime and disruption is preferable

Remember the incident response process. Containing the incident comes before finding root cause and full remediation.

SEGMENTATION

There are several ways to look at segmentation

Mobile device management. in a BYOD mobile device scenario, mobile app management (MAM) will keep personal and business data separate.

Prevents personal data from being removed in remote wipe.

Endpoints. segment devices that have become vulnerable, such as an unpatched printer where there are no updates.

You could place these printers in a VLAN.

Non-compliant devices can be quarantined until remediated.

This is possible with network access control (NAC)

Applications. Within a private subnet, VLANs can be used to carry out segmentation and traffic filtering for sensitive apps and data.

These rules could be enforced with subnets and firewalls

SIEM AND SOAR

often use AI, ML, and threat intelligence

SIEM

Security Information Event Management

system that collects data from many other sources within the network.

provides real-time monitoring, traffic analysis & notification of potential attacks.

SOAR

Security Orchestration Automation, & Response

centralized alert and response automation with threat-specific playbooks.

response may be fully automated or single-click.

these capabilities are commonly delivered together in a single solution

SOAR PLAYBOOKS AND RUNBOOKS

Runbooks

- documents with info on events and the necessary actions to stop threats.
- can be used to configure automated response in a playbook.

Documents the human analyst response steps

Playbooks

- contain a set of rules and actions to identify incidents and take preventative action.
- may need to be amended for better automated response as threats evolve.

This is the response automation

4.0 OPERATIONS AND INCIDENT RESPONSE

4.5 Explain the key aspects of digital forensics

- **Documentation/evidence**
  - Legal hold
  - Video
  - Admissibility
  - Chain of custody
  - Timelines of sequence of events
    - Time stamps
    - Time offset
  - Tags
  - Reports
  - Event logs
  - Interviews
- **Acquisition**
  - Order of volatility
  - Disk
  - Random-access memory (RAM)
  - Swap/pagefile
  - OS
  - Device
  - Firmware
  - Snapshot
  - Cache
  - Network
  - Artifacts
- **On-premises vs. cloud**
  - Right-to-audit clauses
  - Regulatory/jurisdiction
  - Data breach notification laws
- **Integrity**
  - Hashing
  - Checksums
  - Provenance
- **Preservation**
- **E-discovery**
- **Data recovery**
- **Non-repudiation**
- **Strategic intelligence/ counterintelligence**

DOCUMENTATION AND EVIDENCE

Legal Hold

protecting any documents that can be used in evidence from being altered or destroyed.

sometimes called litigation hold

Chain of Custody

tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle

documents each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

Confirms appropriate collection, storage, and handling

EVIDENCE ADMISSIBILITY

Requirements for evidence to be **admissible in a court of law**:

TO BE ADMISSIBLE:

Evidence must be relevant to a fact at issue in the case. makes a fact more or less probable than without the evidence

The fact must be material to the case. Is important in proving a case

The evidence must be competent or legally collected. competent means "reliable" here

Must be obtained by legal means.

To prevail in court, evidence must be **sufficient**, which means “convincing without question, leaving no doubt”

DOCUMENTATION/EVIDENCE

Video

CCTV can be a good source of evidence for helping to identify attackers and the time the attack was launched.

Can be vital in apprehending suspects and reconstructing timeline of events.

Timelines of sequence of events

Time stamps. Each file has timestamps showing when files were created, last modified, and last accessed

Time offset. where evidence is collected across multiple time zones, you must record offset based on time zone.

For example, recording the time offset, it looks as if it started in Chicago, but if we apply time normalization, when it is 4 a.m. in London, the time in Chicago is 10 p.m.

Tags

eDiscovery tags virtual are virtual 'sticky notes' or labels attached to documents, making them easier to search/find.

Helps legal team stay organized and build a defensible case.

DOCUMENTATION/EVIDENCE

Reports

To support an effective post incident review, all key discussions and decisions made during the eradication event should be well documented.

A report should be produced from the post incident review and presented to all relevant stakeholders.

Event logs

Provide a means to reconstruct sequence of events.

Centralized log collection helpful here, and audit trail a requirement.

Maintaining audit trail is a legal requirement in some cases

To track incidents, we need to be actively monitoring and actively logging changes to patterns in our log files or traffic patterns in our network.

SIEM can help with log collection, aggregation, and analysis

Interviews

A photofit is a reconstructed picture of a suspect

The police may also take witness statements to try and develop a picture of who was involved and maybe then use photofits so that they can be apprehended.

TYPES OF EVIDENCE

EXTRA CREDIT

Best. Original, preferred by courts.

Secondary evidence. Copy.

Direct. Proves or disproves an act based on the five senses.

Conclusive. Incontrovertible, overrides all other types.

Circumstantial. Inference from other info.

Corroborative. Supporting evidence but cannot stand on its own.

Opinions. Expert and non-expert.

Hearsay. Not based on first-hand knowledge.

Evidence must be **relevant**, **complete**, **sufficient** and **reliable**

ACQUISITION OF EVIDENCE

Importance of collecting

EVIDENCE

As soon you discover an incident...

You must begin to collect evidence and as much information about the incident as possible.

Evidence can be used in a subsequent legal action or in finding attacker identity.

Evidence can also assist you in determining the extent of damage.

EVIDENCE STORAGE

Understand the concerns for **evidence storage**

How to retain logs, drive images, VM snapshots, and other datasets for recovery, internal and forensic investigations.

Protections for evidence storage include:

- locked cabinets or safes
- dedicated/isolated storage facilities
- offline storage
- access restrictions and activity tracking
- hash management and encryption

ACQUISITION

Areas and considerations in evidence acquisition.

Disk aka hard drive. Was the storage media itself damaged?

Random-access memory (RAM). Volatile memory used to run applications.

Swap/Pagefile. used for running applications when RAM is exhausted.

OS (operating system). Was there corruption of data associated with the OS or the applications?

Device. When the police are taking evidence from laptops, desktops, and mobile devices they take a complete system image.

The original image is kept intact, installed on another computer, hashed, then analyzed to find evidence of any criminal activity.

ACQUISITION

Firmware. embedded code, could be reversed engineered by an attacker, so original source code must be compared to code in use.

a coding expert to compare both lots of source code in a technique called regression testing. rootkits and backdoors are concerns

Snapshot. If the evidence is from a virtual machine, a snapshot of the virtual machine can be exported for investigation.

Cache. special high-speed storage that can be either a reserved section of main memory or an independent high-speed storage device.

memory cache AND disk cache, both are volatile

Network. OS includes command-line tools (like netstat) that provide information that could disappear if you reboot the computer.

Like RAM, connections are volatile and lost on reboot.

Artifacts. any piece of evidence, including log files, registry hives, DNA, fingerprints, or fibers of clothing normally invisible to the naked eye.

ORDER OF VOLATILITY

To determine what happened on a system, you need a copy of the data. **What evidence you collect first?**

most volatile (perishable) information should be collected first.

If it disappears with a system reboot or passage of time, it is volatile

In approximate order:

1. CPU, cache, and register contents
2. Routing tables, ARP cache, process tables, kernel statistics
3. Live network connections and data flows
4. Memory (RAM)
5. Temporary file system and swap/pagefile
6. Data on hard disk
7. Remotely logged data
8. Data stored on archival media and backups

Collection must also consider questions of **storage** and **chain of custody**!

ON PREMISES VS CLOUD

Customer rights and capabilities to perform forensic investigation varies in the cloud versus on-premises.

Right-to-Audit Clauses

written into supply chain contracts, allow an auditor can visit the premises to inspect and ensure that the contractor is complying with contractual obligations.

This would help an auditor identify:

- Faulty or inferior quality of goods
- Short shipments
- Goods not delivered
- Kickbacks
- Gifts and gratuities to company employees
- Commissions to brokers and others
- Services allegedly performed that were not actually necessary

ON PREMISES VS CLOUD

Customer rights and capabilities to perform forensic investigation varies in the cloud versus on-premises.

Regulatory and Jurisdiction

Cloud data should be stored and have data sovereignty in region stored.

Many countries have laws requiring businesses to store data within their borders.

The US introduced the **Clarifying Lawful Overseas Use of Data (CLOUD) Act** in 2018 due to the problems that FBI faced in forcing Microsoft to hand over data stored in Ireland.

Aids in evidence collection in investigation of serious crimes

In 2019, the US and the UK signed a data-sharing agreement to give law enforcement agencies in each country faster access to evidence held by cloud service providers.

Verifying right-to-audit and audit procedures with your cloud provider to ensure you understand your rights and their legal obligations before you sign contracts is critical.

ON PREMISES VS CLOUD

Cloud considerations (cont)

Forensic investigators should know their legal rights in every jurisdiction (region or country) where the organization hosts data in the cloud.

Some countries will not allow eDiscovery from outside their borders

Chain of custody

In traditional forensic procedures, it is "easy" to maintain an accurate history of time, location, and handling.

In the cloud, physical location is somewhat obscure. However, investigators can acquire a VM image from any workstation connected to the internet.

Time stamps and offsets can be more challenging due to location.

Maintaining a proper chain of custody is more challenging in the cloud.

Breach notification laws

Varies by country and regulations. For example, GDPR requires notification within 72 hours. and applies to ANY company with customers in the EU !

INTEGRITY

Hashes

When either the forensic copy or the system image is being analyzed, the data and applications are **hashed** at collection.

It can be used as a **checksum** to ensure integrity later.

File can be hashed before and after collection to ensure a match on the original hash value to prove data integrity.

Provenance

Data provenance effectively provides a historical record of data and its origin and forensic activities performed on it.

Similar to **data lineage**, but also includes the inputs, entities, systems and processes that influenced the data

Preservation

Data needs to be preserved in its original state so that it can be produced as evidence in court.

original data must remain unaltered and pristine.

What is a "forensic copy" of evidence?

an image or exact, sector by sector, copy of a hard disk or other storage device, taken using specialized software, preserving an exact copy of the original disk.

Deleted files, slack space, system files and executables (and documents renamed to mimic system files and executables) are all part of a forensic image.

Putting a copy of the most vital evidence in a WORM drive will prevent any tampering with the evidence (you cannot delete data from a WORM drive.)

You could also write-protect/put a legal hold on some types of cloud storage.

E-DISCOVERY (ELECTRONIC DISCOVERY)

eDiscovery e-discovery is about gathering the data.

the process of **identifying, preserving, collecting, processing, reviewing,** and **producing electronically stored information (ESI)** in litigation.

The **digital forensics** process involves identifying, preserving, collecting, recovering, analyzing, and reporting on digital information.

During e-discovery, Cloud Service Providers (CSP) may be subpoenaed to allow collection, review, and interpretation of electronic documents and data.

Digital forensics vs eDiscovery: what's the difference?

computer forensics involves the use of a forensic expert to protect data integrity and to copy/capture/recover the data stored on a device.

eDiscovery firms typically do not analyze the data they collect.

Forensic investigators have specialized training enabling them to analyze data, protect data integrity, and recover missing or deleted data.

DATA RECOVERY

requires specialized training and knowledge

Forensic data recovery

A process used to retrieve data which will be used for legal purposes.

Investigators must work with information in a way that will not change or compromise the original source.

They can use a variety of techniques to fill in missing pieces or make information meaningful.

EXAMPLE: restoring a damaged or deleted partition, looking for traces of information which could reveal how and when the partition was used.

may be working with computers which have been seeded with safety measures to prevent legal investigations, requiring special procedures.

E-discovery works in conjunction with digital forensics - their functions are complementary.

NON-REPUDIATION

Non-repudiation is **the guarantee that no one can deny a transaction.**

Methods to provide non-repudiation

Digital Signatures prove that a digital message or document was not modified—intentionally or unintentionally—from the time it was signed.

based on asymmetric cryptography (a public/private key pair)

the digital equivalent of a handwritten signature or stamped seal.

message authentication code (MAC). the two parties that are communicating can verify non-repudiation.

is generated via a cryptographic algorithm that depends on both the message and session key known only to the sender and receiver

Digital signatures are covered in more detail in Domain 2

STRATEGIC INTELLIGENCE/ COUNTERINTELLIGENCE

Historically, when governments gather (and potentially exchange) data about cyber criminals so that they can work together to reduce threats.

In the context of forensic investigation, gathering evidence can also be performed using strategic intelligence methods.

Focuses gathering threat information about a domain, including business info, geographic info, or other details on a specific country.

Counterintelligence

The target of someone's strategic intelligence may want to prevent that intelligence gathering from occurring.

The target may perform strategic counterintelligence (CI) to identify and disrupt the adversary gathering intelligence.

THANKS

FOR WATCHING!