SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Simone **Soderi**

M3.3 - Cybersecurity Operations and Management

Contents (1/2)

1. **People Management**
    - Human Factor
    - Cybersecurity Awareness and Education
2. **Physical Asset Management**
    - Hardware
    - Office equipment
    - Industrial Control Systems (ICSs)
    - Mobile Devices
3. **System Access and Management**
    - Authentication
    - Access Control
4. **Computer Security Incident Response Teams (CSIRT)**
    - Terminology
    - Triage
    - Incident Report
    - Handling
    - Resolution

Contents (2/2)

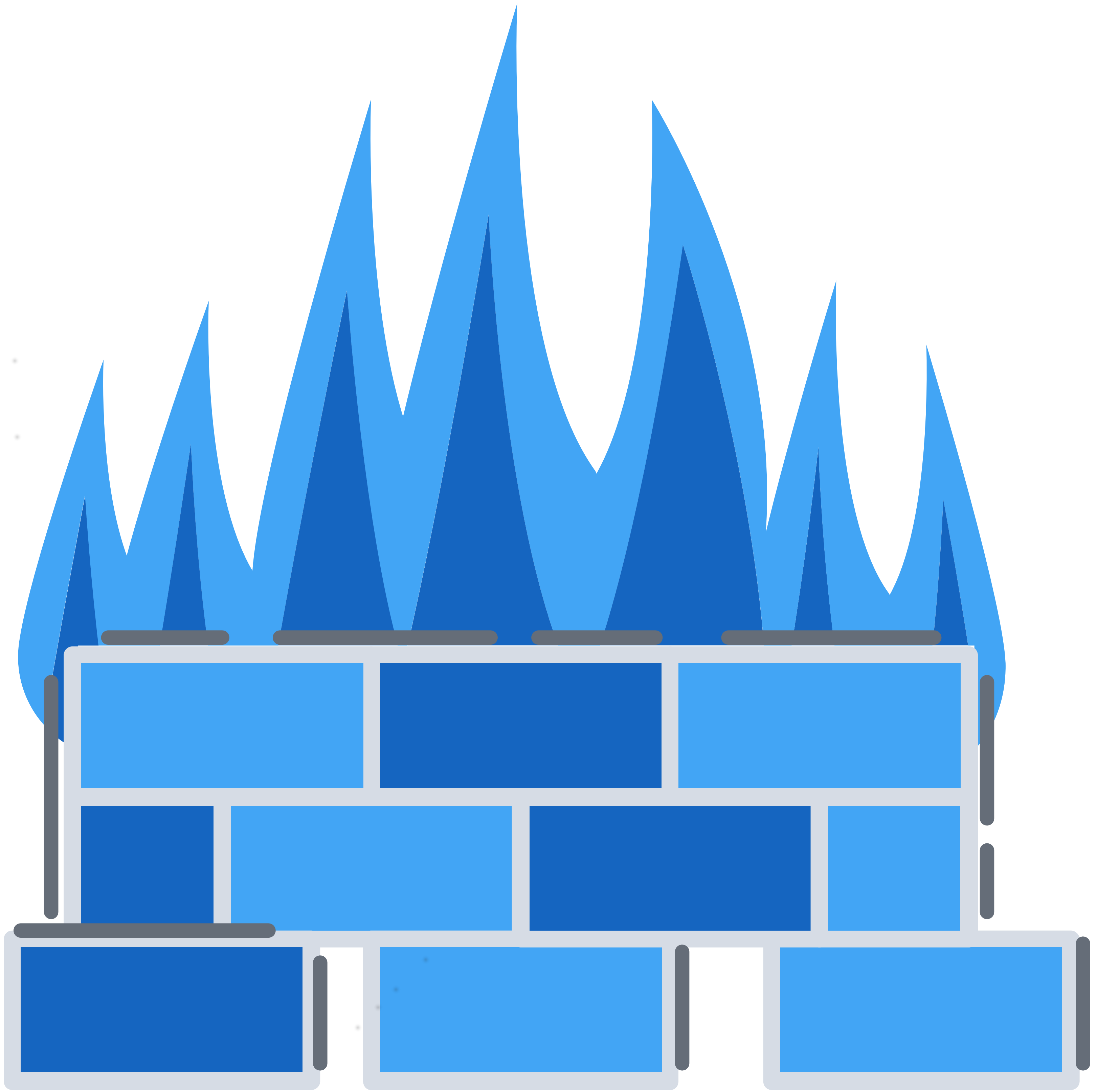
5. **Technical Security Management**
   - Malware Protection
   - Intrusion Detection
   - Data Loss Prevention
6. **Network Security**
   - Network Fundamentals
   - Network Security Concepts
   - Network Protection
7. **Threat and Incident Management**
   - Vulnerabilities Management
   - Security Event Logging
   - Threat Intelligence
   - Incident Management Workflow
8. **Physical and Infrastructure Security**
   - Threats
   - Recovery
   - Integration with Logical Security
9. **Business Continuity and Recovery Plan**
   - Concepts
   - Management
   - Costs

Contents

4. **Computer Security Incident Response Teams (CSIRT)**
    - Terminology
    - Triage
    - Incident Report
    - Handling
    - Resolution

Computer Security Incident Response Team (CSIRT)

For large and medium-sized organizations, a **computer security incident response team** (**CSIRT**) is **responsible** for **rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses** that were exploited, and **restoring computing services**.



Security Incidents

CSIRT

Security incidents:

“**Any action that threatens one** or **more** of the classic **security services** of confidentiality, integrity, availability, accountability, authenticity, and reliability in a system”

Unauthorized access to a system

- Accessing information not authorized to see
- Passing information on to a person not authorized to see it
- Attempting to circumvent the access mechanisms
- Using another person’s password and user id

Unauthorized modification of information on the system

- Attempting to corrupt information that may be of value
- Attempting to modify information without authority
- Processing information in an unauthorized manner

Managing Security Incidents

ACTIONS AND TERMINOLOGY

- **Managing** security incidents **involves procedures** and controls that address:
  - **Detecting** potential security incidents
  - **Sorting**, categorizing, and prioritizing incoming incident reports
  - **Identifying** and responding to breaches in security
  - **Documenting** breaches in security for future reference
- Here we **list key terms related to computer security incident response**.

Artifact
Any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artifacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits.

Computer Security Incident Response Team (CSIRT)
......A capability set up for the purpose of assisting in responding to computer security-related incidents that involve sites within a defined constituency; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).

Constituency
..The group of users, sites, networks or organizations served by the CSIRT.

Incident
...... A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Triage
The process of receiving, initial sorting, and prioritizing of information to facilitate its appropriate handling.

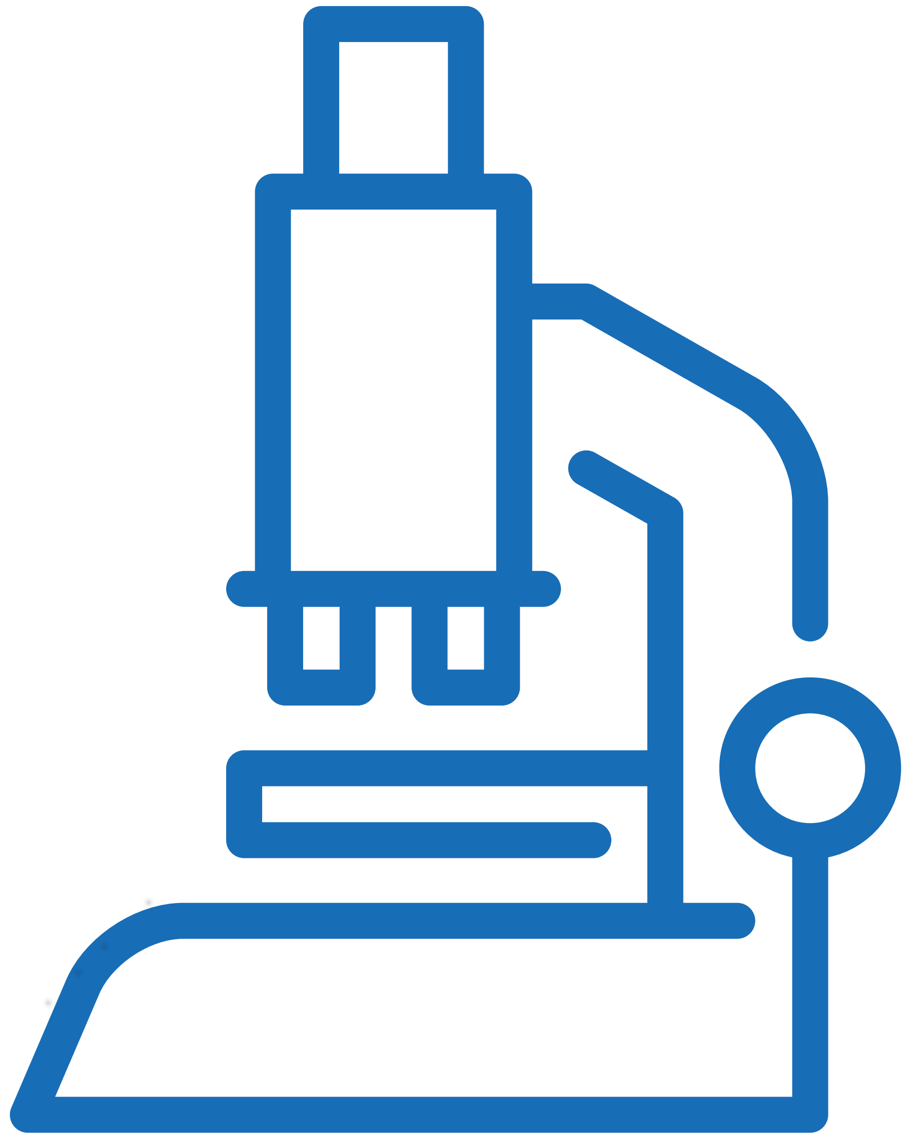
Vulnerability
.. A characteristic of a piece of technology which can be exploited to perpetrate a security incident. For example, if a program unintentionally allowed ordinary users to execute arbitrary operating system commands in privileged mode, this "feature" would be a vulnerability.

Detecting Incidents

CSIRT

- **Incidents may be detected by users or administration staff**
  - Staff should be encouraged to **make reports** of system malfunctions or anomalous behaviours

- **Automated tools**
  - System integrity verification tools
  - Log analysis tools
  - Network and host intrusion detection systems : NIDS/IDS
  - Intrusion prevention systems (IPS)



Incidents Triage

CSIRT

Triage Function Goal:

- Ensure that all information designed for the **incident handling service is channeled through a single focal point** regardless of the method by which it arrives (e.g., by e-mail, hotline, helpdesk, IDS) for appropriate redistribution and handling within the service.

- Commonly achieved by advertising **the triage function as the single point of contact for the whole incident handling service**

Responds to incoming information by:

- Requesting **additional information in order to categorize** the incident
- **Notifying the various parts of the enterprise** or constituency about the **vulnerability** and shares information about how to fix or mitigate the vulnerability
- Identifies the **incident as either new or part of an ongoing incident** and passes this information on to the incident handling response function

Responding to Incidents

CSIRT

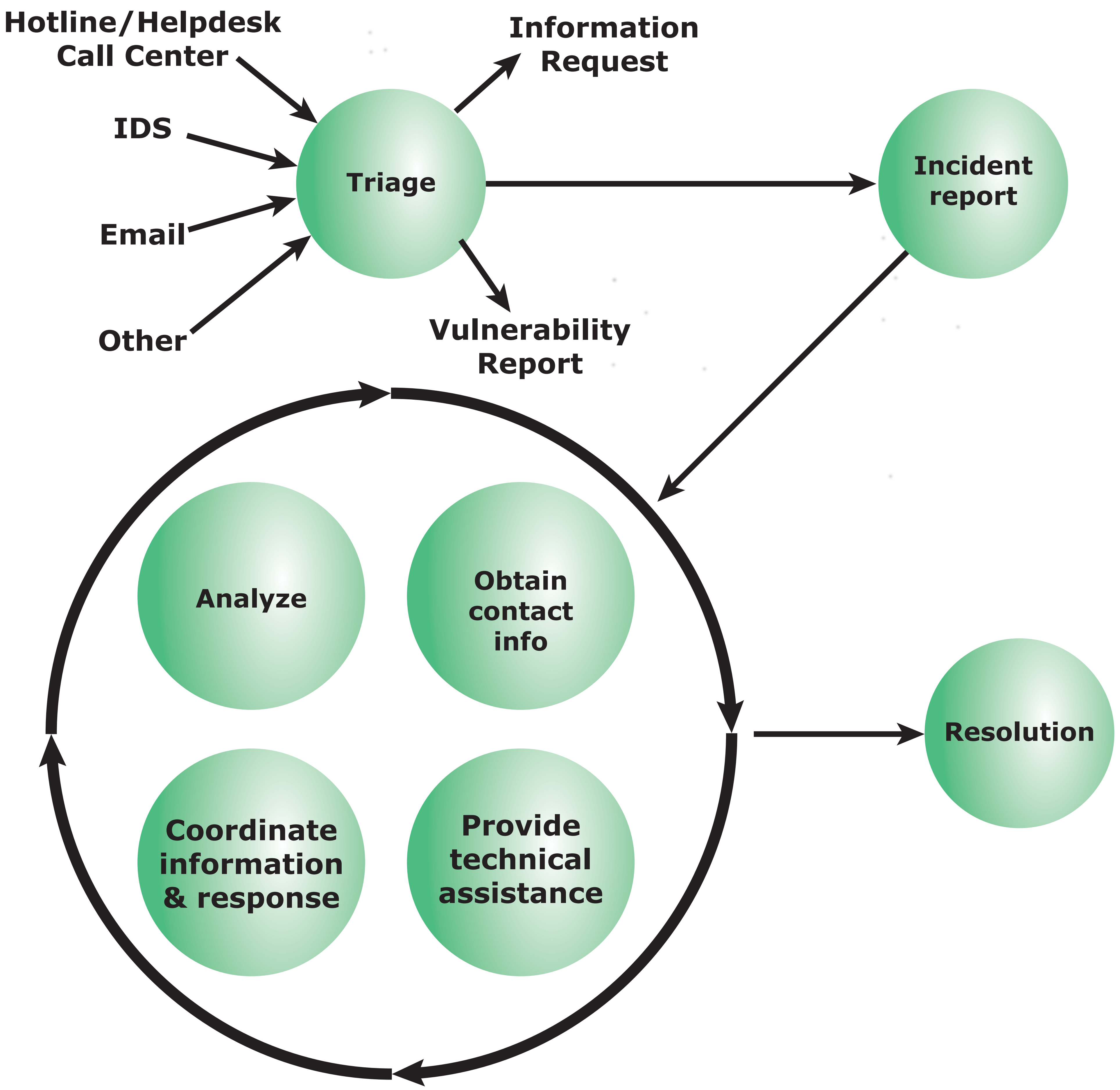
Once a potential incident is detected, **we must have documented procedures to respond to incidents**

Procedures should:

1. **Detail** how to identify the cause
2. **Describe** the action taken to recover from the incident
3. **Identify typical categorie**s of incidents and the approach taken to respond to them
4. **Identify management personnel** responsible for making critical decisions and how to contact them
5. **Identify** the **circumstances** when security breaches should be reported to third parties such as the police or relevant CERT

Incidents Handling Life Cycle

CSIRT



Once an incident is opened, it transitions through a number of states, with all the information relating to the incident (its change of state and associated actions), **until no further action is required from the team's perspective and the incident is finally closed.**

The cyclical portion indicates those states that may be visited multiple times during the activity's life cycle.

Documenting Incidents

CSIRT

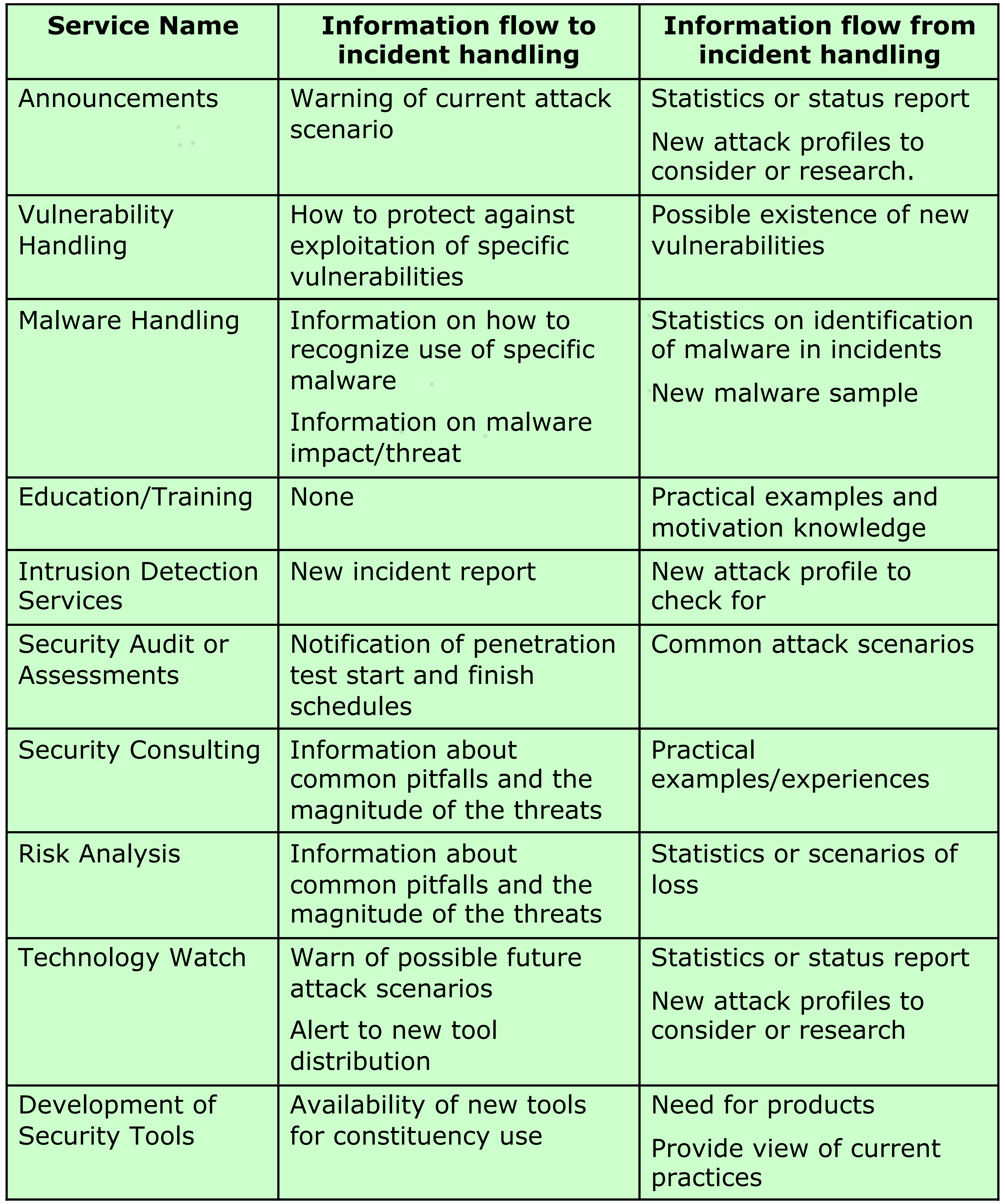
- Should **immediately follow a response to an incident**
  - Identify **what** vulnerability led to its occurrence
  - **How** this might be addressed to prevent the incident in the future
  - **Details** of the incident and the response taken
  - **Impact** on the organization’s systems and their risk profile

- More generally, though, a **security incident reflects a change in the risk profile** of the organization that needs to be addressed. This could involve **reviewing the risk assessment** of the relevant systems and either changing or extending this analysis.

- It could involve **reviewing controls identified for some risks, strengthening existing controls, and implementing new controls.** This reflects the cyclic process of IT security management.

Example of Info Flow and Incidents Handling

CSIRT



Service Name	Information flow to incident handling	Information flow from incident handling
Announcements	Warning of current attack scenario	Statistics or status report New attack profiles to consider or research.
Vulnerability Handling	How to protect against exploitation of specific vulnerabilities	Possible existence of new vulnerabilities
Malware Handling	Information on how to recognize use of specific malware Information on malware impact/threat	Statistics on identification of malware in incidents New malware sample
Education/Training	None	Practical examples and motivation knowledge
Intrusion Detection Services	New incident report	New attack profile to check for
Security Audit or Assessments	Notification of penetration test start and finish schedules	Common attack scenarios
Security Consulting	Information about common pitfalls and the magnitude of the threats	Practical examples/experiences
Risk Analysis	Information about common pitfalls and the magnitude of the threats	Statistics or scenarios of loss
Technology Watch	Warn of possible future attack scenarios Alert to new tool distribution	Statistics or status report New attack profiles to consider or research
Development of Security Tools	Availability of new tools for constituency use	Need for products Provide view of current practices

Incident handling function:

An **example of the information flow to and from an incident handling service.**

This type of breakdown is **useful in organizing and optimizing the incident handling service and in training personnel** on the requirements for incident handling and response.

Remarks on the CSIRT

- ✓ The **CSIRT** is typically the team that **works hand in hand with the information security teams.**
  - ◉ In **smaller** organizations, security team and CSIRT functions may be combined and provided by the same team.
  - ◉ In **large** organizations, the **CSIRT** focuses on the investigation of computer security incidents, whereas the **security team** is tasked with the implementation of security configurations, monitoring, and policies within the organization.

- ✓ It is important to recognize that every organization is different. However, **defining the constituency of a CSIRT** is certainly one of the first steps in the process.

- ✓ The **main goals of the CSIRT are** to **minimize** risk, **contain** cyber damage, and **save money** by preventing incidents from happening—and when they do occur, to mitigate them efficiently.
  - ◉ It is a good practice to review and **calculate the "value add" of the CSIRT**. This calculation **can be used to determine when to invest more, not only in a CSIRT, but also in operational best practices.** In some cases, an organization might even outsource some of the cybersecurity functions to a managed service provider, if the organization cannot afford or retain security talent.

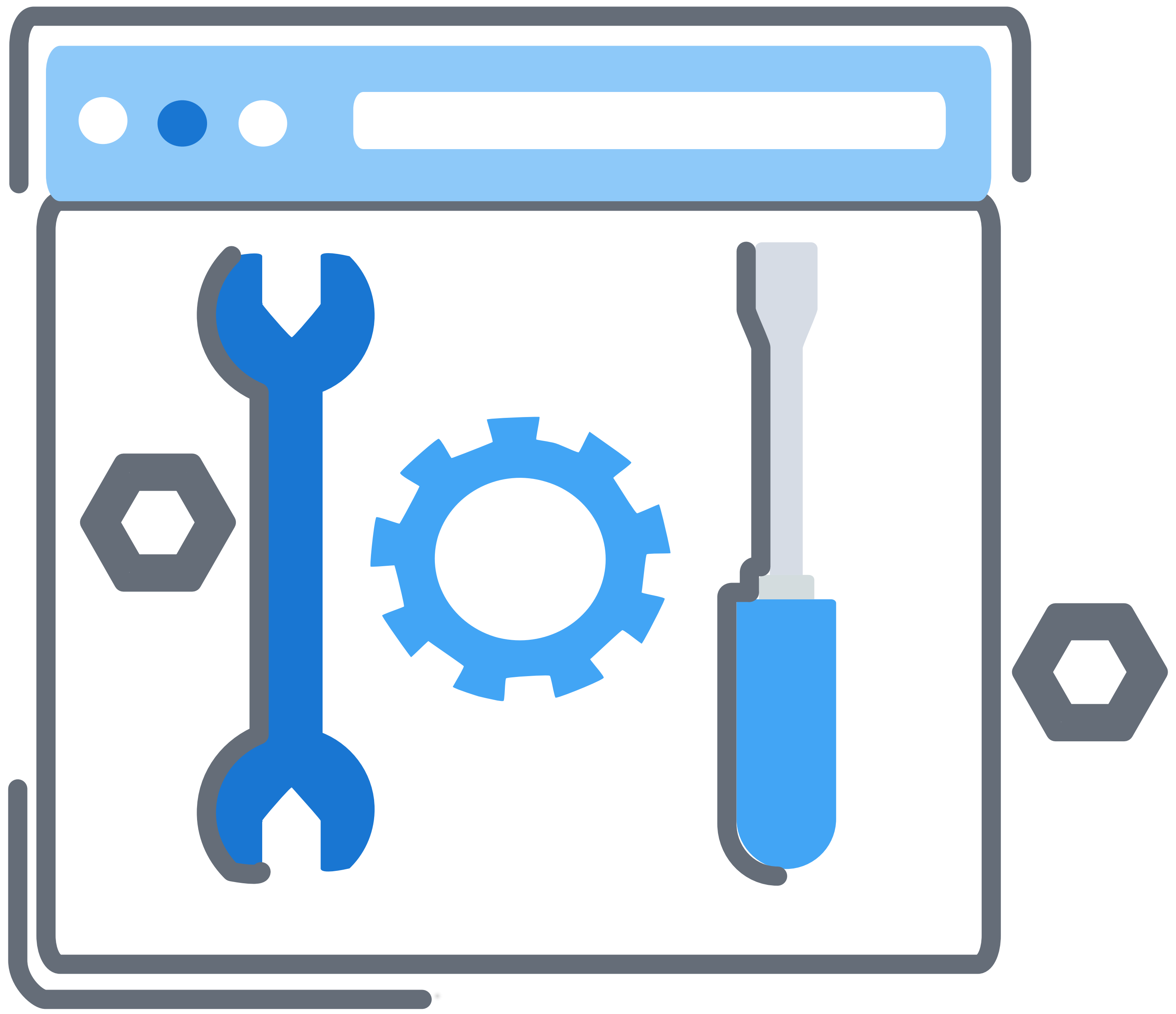
Contents

5. Technical Security Management

- Malware Protection
- Intrusion Detection
- Data Loss Prevention

Technical Security Controls

Security controls (that is, safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through **mechanisms contained in the hardware, software, or firmware** components of the system



Malware Protection Activities

Malicious software (**malware**) is perhaps the most **significant security threat to organizations**

NIST SP 800-83, *"Guide to Malware Incident Prevention and Handling for Desktops and Laptops"*, **defines malware** as follows:

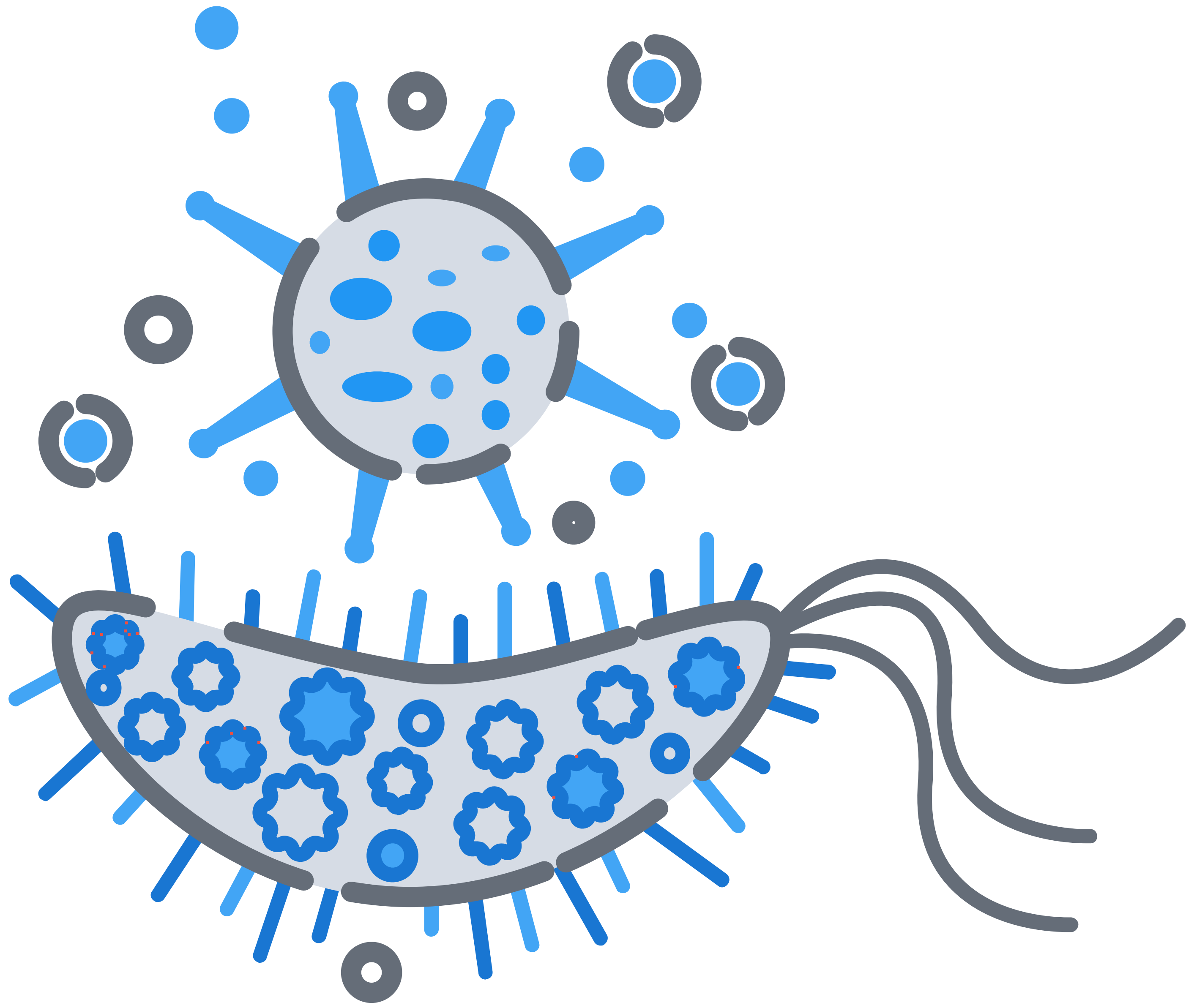
- "A program that is **covertly inserted into another program** with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system"

Malware can **pose a threat to application** programs, to **utility** programs, and to **kernel-level** programs

Malware is also used on compromised or malicious **websites** and servers, or in especially **crafted spam emails** or other messages, which aim to trick users into revealing sensitive personal information.

Types of Malware (1/2)

A SELECTION



Zombie, bot

A program that is activated on an infected machine to launch attacks on other machines

Ransomware

A type of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim.

Spyware

Software that collects information from a computer and transmits it to another system.

Flooder

A tool used to attack networked computer systems with a large volume of traffic to carry out a denial-of-service (DoS) attack.

Logic bomb

A program inserted into software by an intruder. A logic bomb lies dormant until a predefined condition is met, at which point the program triggers an unauthorized act.

Remote Access Trojan

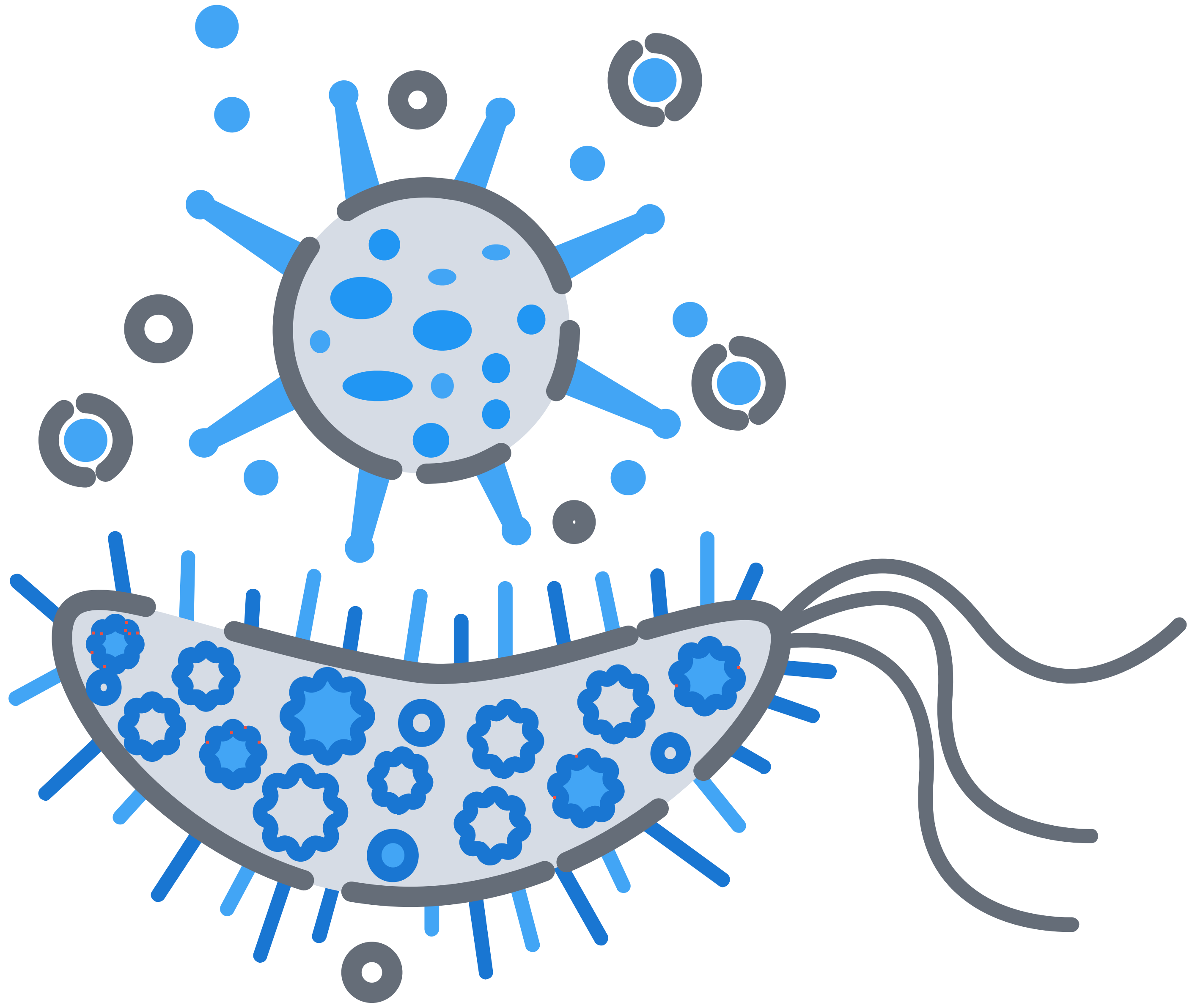
RAT is a malware program that includes a back- door for administrative control over the target computer. RATs are usually downloaded invisibly with user-requested programs—such as games—or sent as email attachments.

Worm

A computer program that runs independently and propagates a complete working version of itself onto other hosts on a network.

Types of Malware (2/2)

A SELECTION



Backdoor

Any mechanisms that bypasses a normal security check; it may allow unauthorized access to functionality.

Spammer

Programs used to send large volumes of unwanted email.

Keyloggers

A software tool that captures keystrokes on a compromised system.

Scraper

A simple program that searches a computer's memory for sequences of data that match particular patterns, such as credit card numbers.

Malware as a Service

A web-based provider of malware. MaaS may provide access to botnets, support hotlines, and servers that regularly update and test malware strains for efficacy.

Virus

Malware that, when executed, tries to replicate itself into other execut- able code; when it succeeds, the code is infected. When the infected code is executed, the virus also executes.

Exploit

Code specific to a single vulnerability or set of vulnerabilities.

The Nature of the Malware Threat

The **ENISA's annual threat report lists malware** as the top cyber threat for 2016 and 2017. Key findings of the report include the following:

- **Businesses experienced far more malware threats** in 2017 compared to 2016.
- **Ransomware continues to dominate the Windows malware scene**, with an evolution from 55% in January 2017 to 75% in July 2017.
- There is increasing threat from **clickless malware**, which is automated malware injection programs that do not require user action to activate.
- There is also a rise in **fileless malware**, which is malware code that resides in RAM (random access memory) or propagates through the use of carefully crafted scripts, such as PowerShell, to infect its host.
- There has been a growth of malicious functions being packaged within **Potentially Unwanted Programs (PUPs)**. While legitimate browser developers like Firefox and Chrome are making efforts to improve security, the **adware industry is creating its own custom browsers** without any built-in security features and bundling them along with adware applications. **They will replace your own browser** as the default browser and expose you to the greater risks of using such a browser.

Practical Malware Protection (1/3)

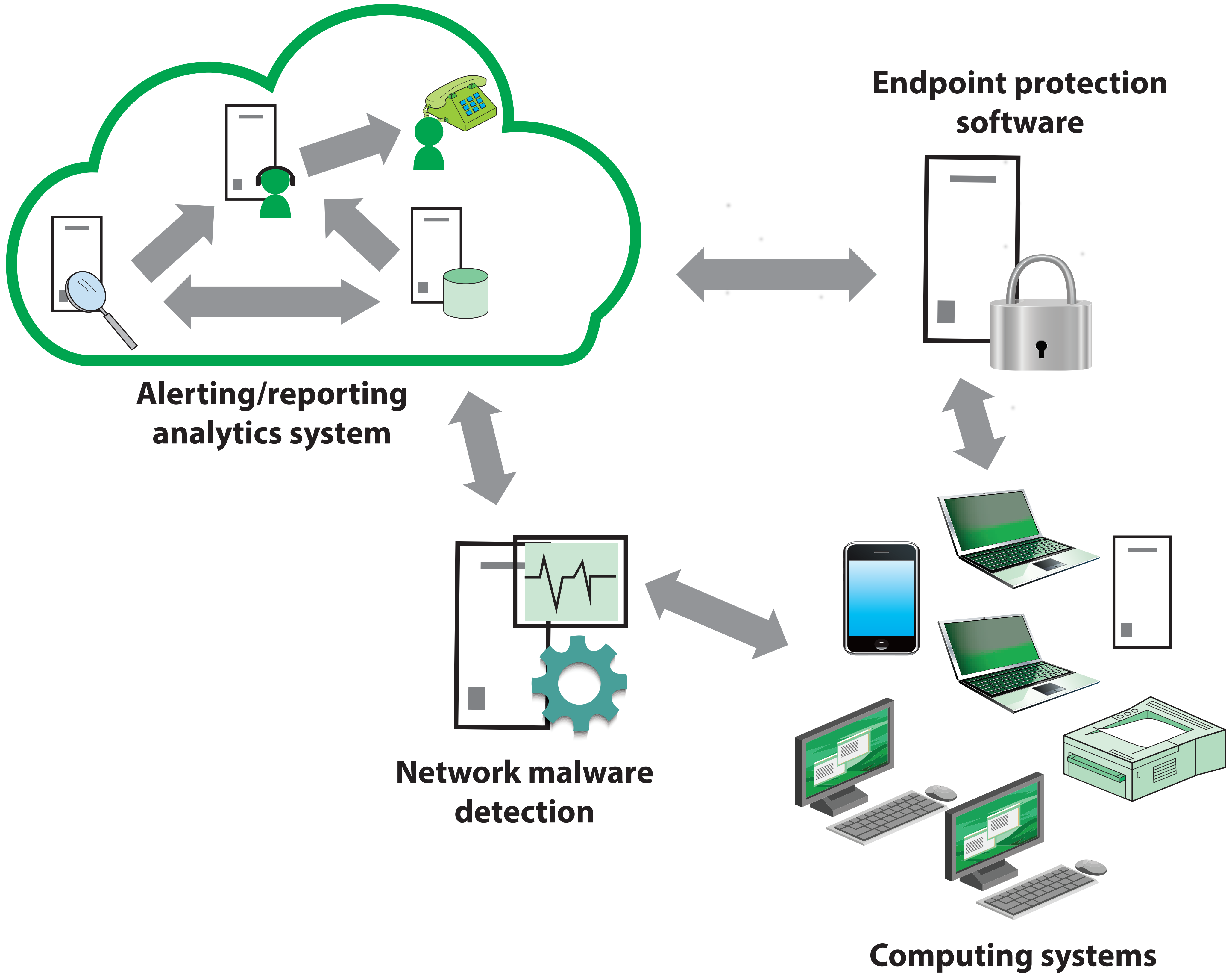
- The **battle against malware is never-ending**. It is an ongoing arms race between malware producers and defenders. As effective countermeasures are developed for existing malware threats, newer types and modifications of existing types are developed.

- **Malware enters through a variety of attack surfaces**, including end-user devices, email attachments, web pages, cloud services, user actions, and removable media.

- **Malware is designed to avoid, attack, or disable defenses.** And malware is constantly evolving to stay ahead of existing defenses.

Practical Malware Protection (2/3)

Organizations need to **automate anti-malware actions as much as possible**



Endpoint protection software
Alerting/reporting analytics system
Network malware detection
Computing systems

Effective **malware protection** must be deployed at **multiple** potential points of attack.

Enterprise endpoint security suites should provide **administrative features to verify that all defenses** are active and current on every managed system.

There should be **systems in place to collect ongoing incident results**, with appropriate analysis and automated corrective action.

Practical Malware Protection (3/3)

IT management can take a number of practical steps to provide the best possible **protection**, including:

1. Define **procedures** and responsibilities to deal with malware protection on systems
2. Where practical, **do not grant administrative** or root/superuser **privileges** to end users
3. Have a system and policies in place to keep track of where sensitive data is located, to erase data when no longer needed, and contain sensitive data
4. Conduct **regular reviews of the software and data content** of systems supporting critical business processes
5. Ensure that user and **server platforms are well managed**
6. Key staff should **regularly participate in security training and awareness** events that cover malware
7. Establish a formal policy **prohibiting the use of unauthorized software**
8. Install and appropriately maintain endpoint defenses
9. Use Domain Name System (DNS) based protection where practicable
10. Use **web filtering software,** services, or appliances where practical
11. Implement **application whitelisting** where practical to allow systems to run software only if it is included on the whitelist
12. Implement **controls that prevent or detect the use of known or suspected malicious websites**
13. Employ software or services that enable you to know where you are vulnerable
14. Gather vulnerability and threat information from online sources
15. **Monitor available logs and network activity** for indicators of malicious software
16. Have a **backup strategy** for your systems; ensure that the backup stream is encrypted over the Internet and enterprise networks
17. Enable **employees to report problems to IT security**

Capabilities of Malware Protection Software (1/2)

- There are **numerous open source and commercial malware protection software** packages available for enterprise use, and most of them have similar capabilities.

- NIST SP 800-83 lists the following as **desired capabilities in malware protection software**:
  - **Scanning** critical host components such as startup files and boot records
  - **Watching real-time** activities on hosts to check for suspicious activity
  - **Monitoring** the behavior of common applications
  - **Scanning files** for known malware
  - **Identifying** common types of malware as well as attacker tools
  - **Disinfecting files**, (removing malware from within a file), and quarantining files, (files containing malware are stored in isolation for future disinfection or examination)

Capabilities of Malware Protection Software (2/2)

- Malware protection software **does not provide the same level of protection against previously unknown viruses** or other malware as it does against known threats and attack signatures

- Accordingly, you should **also have in place other measures**, including:
  - ◉ Application **sandboxing**
  - ◉ **Intrusion detection software** to scan for anomalous behavior
  - ◉ **Awareness training** that provides guidance to users on malware incident prevention
  - ◉ **Firewalls** that by default deny unexpected behavior patterns
  - ◉ **Application whitelisting** to prevent intrusion of unknown software
  - ◉ **Virtualization and container techniques** to segregate applications or operating systems from each other

Intrusion Detection Basic Principles

Authentication facilities, **access control** facilities, and **firewalls** all play roles in countering intrusions.

Another line of defense is intrusion detection, and it has been the focus of much research in recent years. This interest has been motivated by several considerations, including the following:

- ◉ If an intrusion is **detected quickly enough**, the intruder is identified and ejected from the system before any damage is done or any data are compromised. Even if the detection is not timely enough to preempt the intruder, **the sooner the intrusion is detected, the less damage can be done** and the more quickly recovery can be achieved.
- ◉ An effective intrusion detection system (IDS) serves as a deterrent, acting to prevent intrusions.
- ◉ Intrusion detection **enables the collection of information about intrusion techniques** used to strengthen intrusion prevention measures.

Intrusion Detection

USEFUL TERMS

- **Intrusion**

  Violations of security policy, usually characterized as attempts to affect the confidentiality, integrity, or availability of a computer or network

- **Intrusion detection**

  The process of collecting information about events occurring in a computer system or network and analyzing them for signs of intrusions

- **Intrusion detection system (IDS)**

  Hardware or software products that gather and analyze information from various areas within a computer or a network for the purpose of finding and providing real-time or near-real-time warning of attempts to access system resources in an unauthorized manner

- **Host-based IDS**

  Monitors the characteristics of a single host and the events occurring within that host for suspicious activity

- **Network-based IDS**

  Monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity

Intrusion Detection System

USEFUL TERMS

An IDS comprises three logical components:

✓ **Sensors**

- Sensors are responsible for **collecting** data
- The input for a sensor is any part of a system that contains evidence of an intrusion
- **Types of input to a sensor** include network packets, log files, and system call traces
- Sensors collect and forward this information to an analyzer

✓ **Analyzers**

- Analyzers **receive input from one or more sensors** or from other analyzers
- The analysis engines are responsible for **determining if an intrusion** has occurred
- The output of this component may include **evidence supporting the conclusion** that an intrusion occurred
- The analyzer **provides guidance** about what actions to take as a result of an intrusion

✓ **User interface**

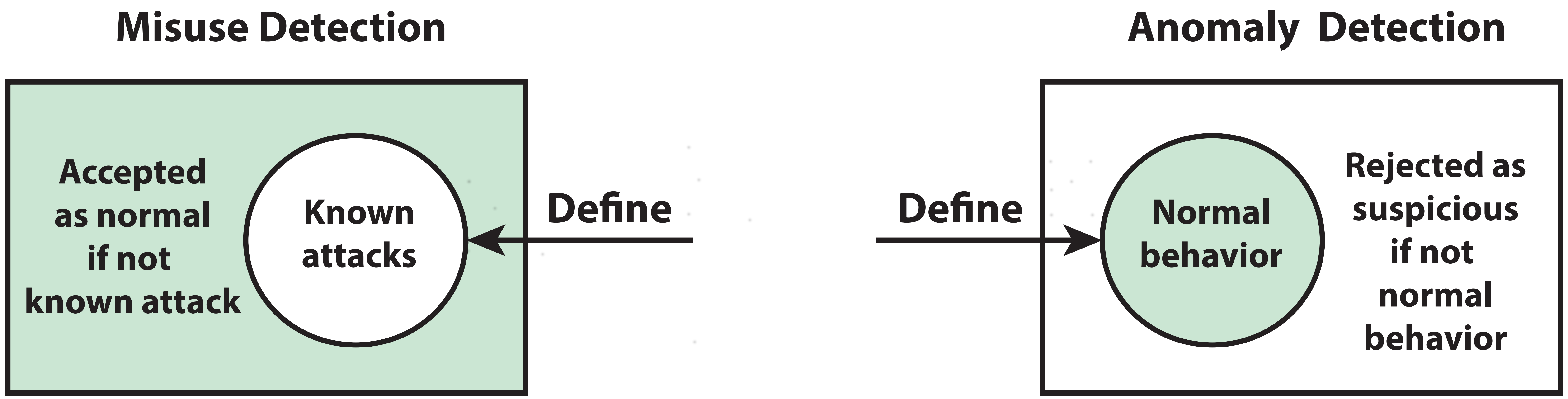
- The user interface to an IDS **enables a user to view output from the system or control the behavior of the system**
- In some systems, the user interface may equate to a manager, director, or console component

Approaches to Intrusion Detection (1/2)

- ✓ Intrusion detection assumes that the **behavior of the intruder differs from that of a legitimate user in ways that are quantifiable.**
- ✓ Of course, **you cannot expect that there will be an exact distinction between an attack by an intruder and the normal use of resources by an authorized user**.
- ✓ Rather, you must expect that there will **be some overlap**.

Approaches to Intrusion Detection (2/2)

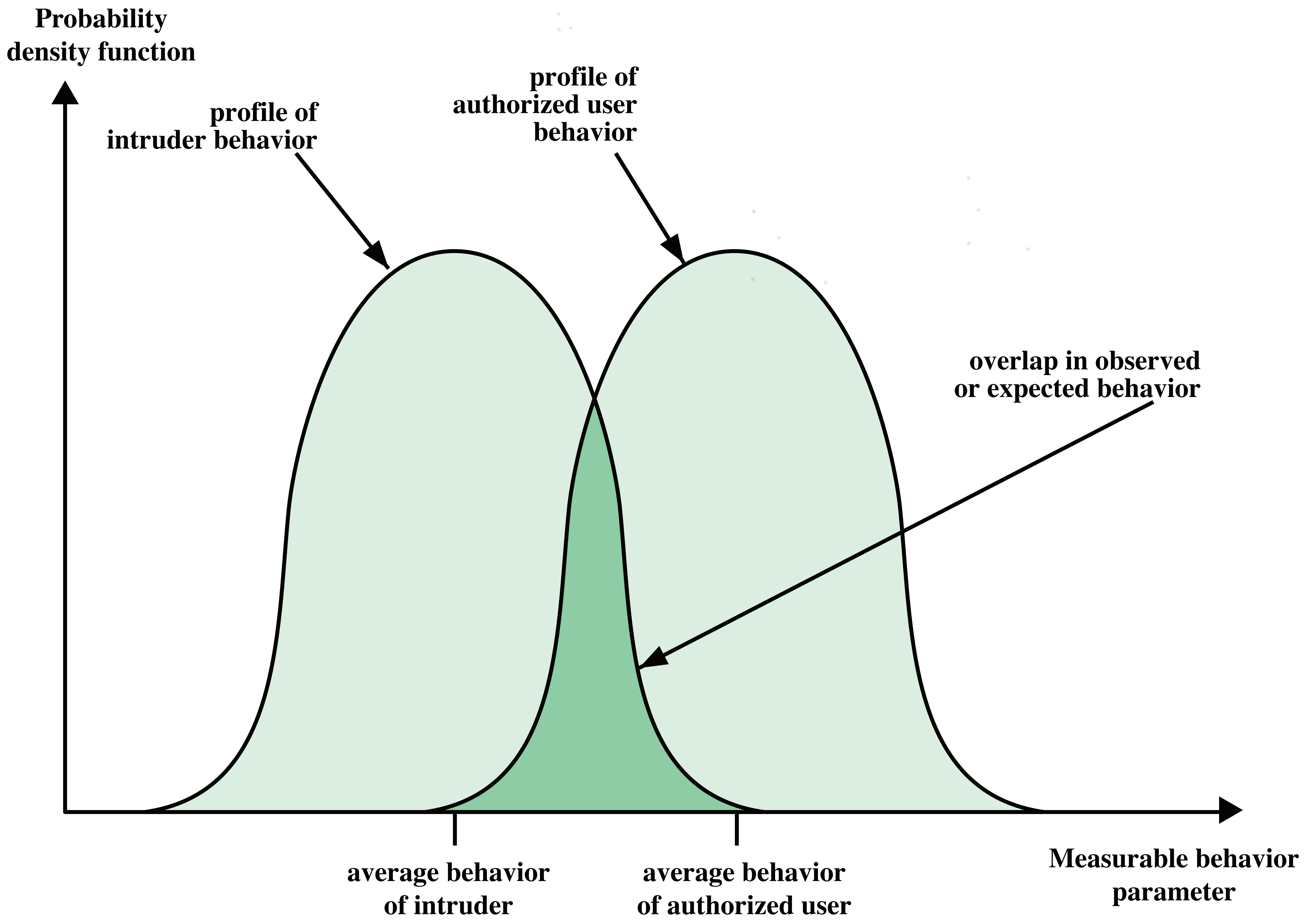
There are **two general approaches** to intrusion detection: **misuse** detection and **anomaly** detection


Misuse Detection
Accepted as normal if not known attack
Known attacks
Define
Anomaly Detection
Define
Normal behavior
Rejected as suspicious if not normal behavior

Misuse detection is based on **rules** that specify system events, sequences of events, or observable properties of a system that are believed to be symptomatic of security incidents. Misuse detectors use various **pattern-matching algorithms**, **operating on large databases of attack patterns, or signatures.** An advantage of misuse detection is that it is accurate and generates **few false alarms**. A disadvantage it that **it cannot detect novel or unknown attacks.**

Anomaly detection involves **searching for activity that is different from the normal behaviour** of system entities and system resources. An advantage of anomaly detection is that it **is able to detect previously unknown attacks** based on an audit of activity. A disadvantage is that there is a **significant trade-off between false positives and false negatives.**

Anomaly Detection System



ANOMALY DETECTION SYSTEM

Although the typical behaviour of an intruder differs from the typical behaviour of an authorized user, **there is some overlap in these behaviors.**

Thus, a loose interpretation of intruder behaviour, which **catches more intruders**, also leads to a number of false positives, or authorized users identified as intruders.

On the other hand, a tentative to limit false positives by a close interpretation of intruder behaviour **leads to an increase in false negatives**, or intruders not identified as intruders.

Thus, there is an element of compromise and art in the practice of anomaly detection.

Host-Based Intrusion Detection Techniques

HOST-BASED IDS:

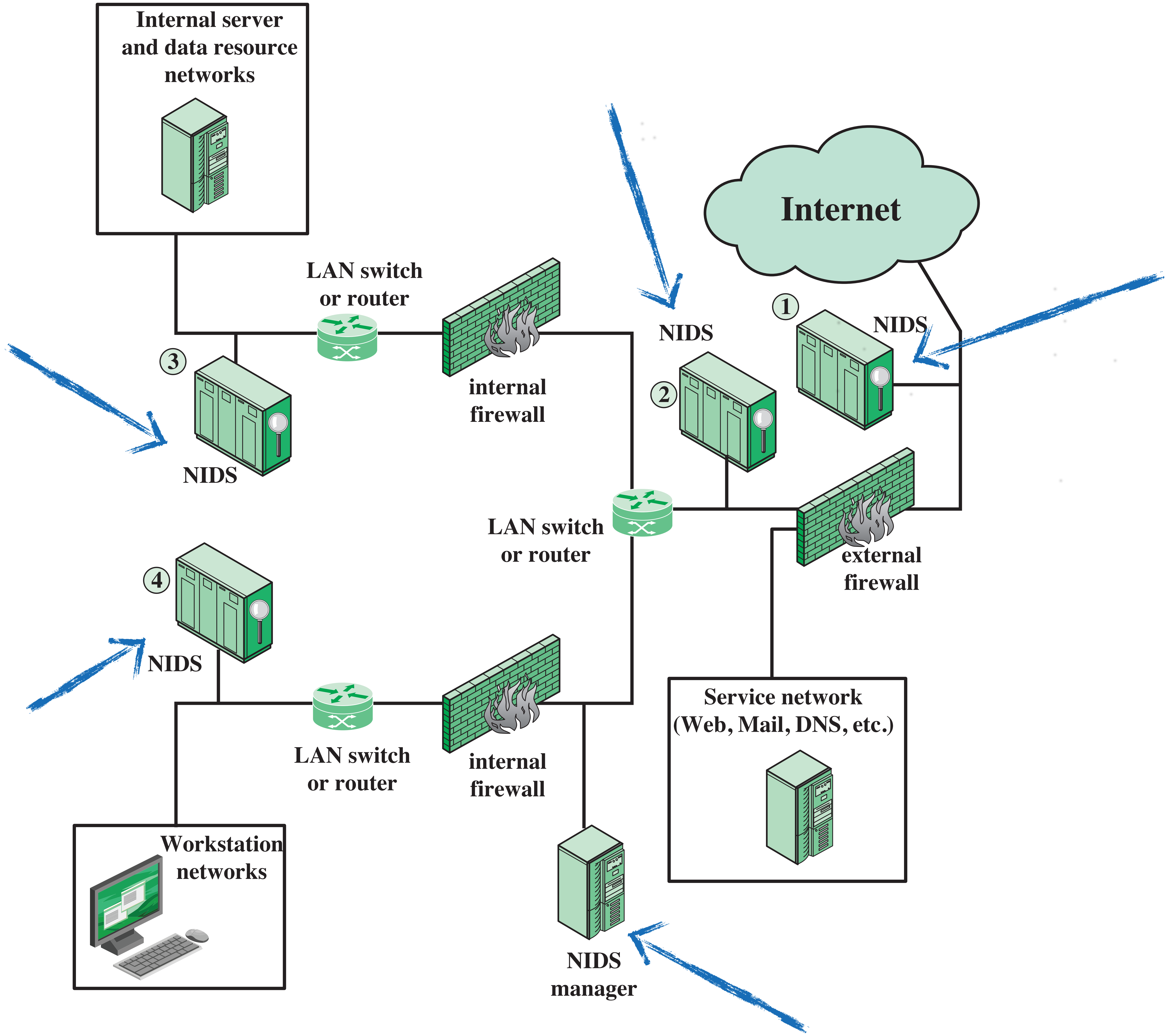
- Add **a specialized layer of security software** to vulnerable or sensitive systems
- Monitors activity on a system in a variety of ways to detect suspicious behavior
- The **primary purpose is to detect intrusions, log suspicious events, and send alerts**
- The **primary benefit is that it detects both external and internal intrusions**—something that is not possible either with network-based IDSs or firewalls
- Use either anomaly or misuse protection or a combination of the two
- For **anomaly detection, two common strategies** are:
  - **threshold detection:** this approach involves defining thresholds, independent of the user, for the frequency of occurrence of various events;
  - **profile based:** A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts

Network-Based Intrusion Detection Techniques

NETWORK-BASED IDS (NIDS):

- A network-based IDS (NIDS) **monitors the traffic on the network segment** as a data source
- Network-based intrusion detection **involves looking at the packets on a network as they pass by some sensor (or probes)**
- Packets are considered to be of interest **if they match a signature**
- **Three primary types of signatures** are:
  - **String signatures:** looks for a text string that indicates a possible attack
  - **Port signatures:** watches for connection attempts to well-known, frequently attacked ports
  - **Header condition signatures:** watches for dangerous or illogical combinations in packet headers

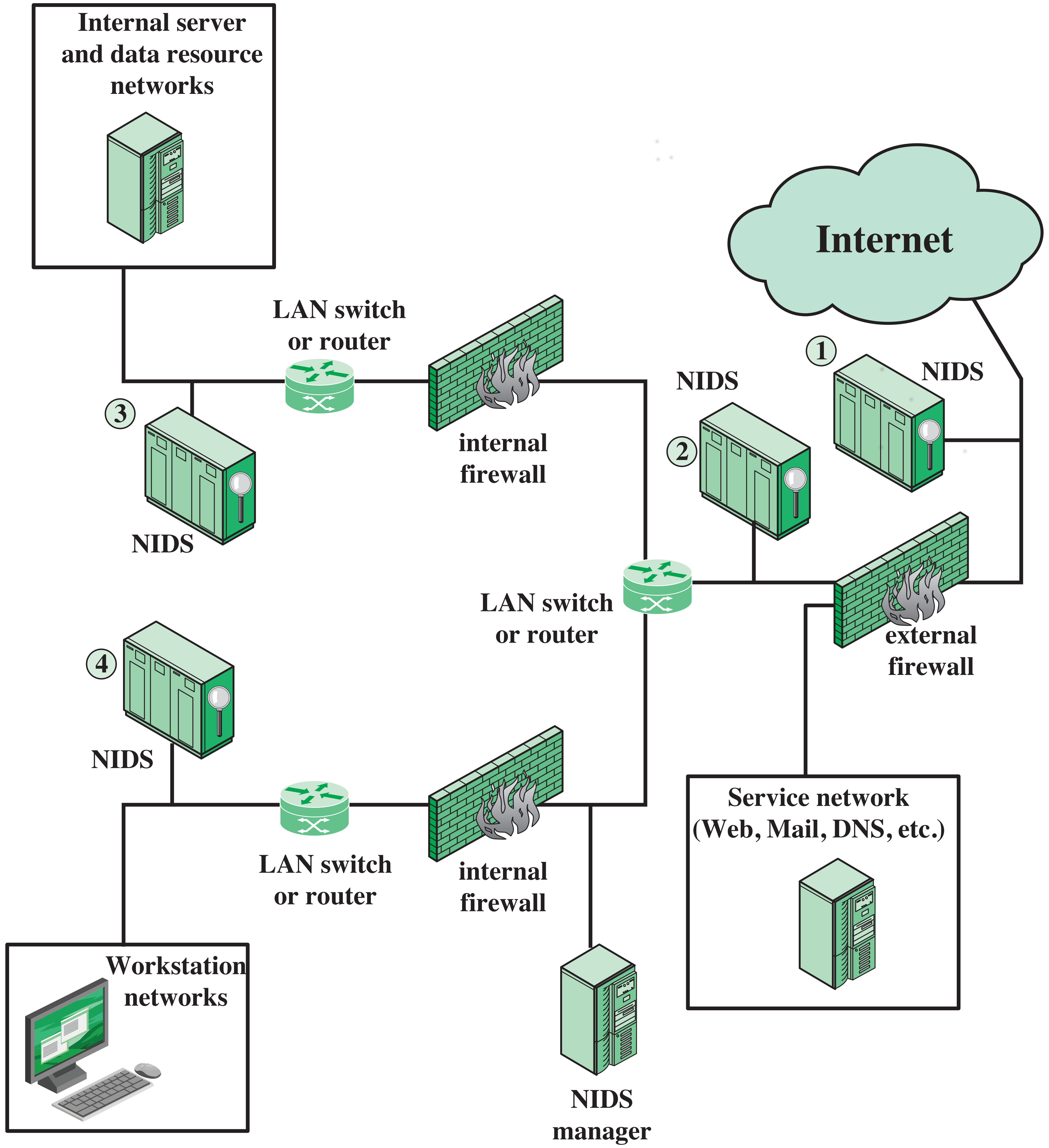
Network Intrusion Detection System (NIDS) (1/2)



A **NIDS sensor sees** only the packets that are carried on the network segment to which it is attached.

Accordingly, a **NIDS** deployment is typically set up as a **number of sensors distributed on key network points to passively gather traffic data and feed information** on potential threats to a central NIDS manager.

Network Intrusion Detection System (NIDS) (2/2)



There are **four types of locations** for the sensors:

1. **Outside the main enterprise firewall:** This placement is useful for establishing the level of threat for a given enterprise network. Those responsible for winning management support for security efforts find this placement valuable.

2. **In the network demilitarized zone (DMZ), inside the main firewall but outside internal firewalls:** This location monitors for penetration attempts that target web and other services that are generally open to outsiders.

3. **Behind internal firewalls to monitor the backbone:** A sensor can be positioned to monitor major backbone networks, such as those that support internal servers and database resources.

4. **Behind internal firewalls to monitor LAN:** A sensor can be positioned to monitor LANs that support user workstations and servers specific to single departments. Locations 3 and 4 can monitor for more specific attacks at network segments, as well as attacks originating from inside the organization.

Data Loss Prevention (DLP)

✓ **Data loss** is **intentional** or **unintentional** release of information to an **untrusted environment**

Data loss prevention (DLP), also referred to as **information leakage**, refers to a comprehensive approach covering people, processes, and systems that identify, **monitor, and protect data in use and data at rest through deep content inspection** and with a centralized management framework

DLP controls are based on policy and **include classifying sensitive data**, discovering data across an enterprise, enforcing controls, and reporting and auditing to ensure policy compliance

✓ **Sensitive information that is at risk of leakage** or is actually leaked **often includes** shared and unencrypted content such as word processing documents, presentation files, and spreadsheets that could leave an organization via many different points or channels (for example, via email, instant messaging, Internet browsing, mobile devices, or on portable storage devices).

Data Classification and Identification

All sensitive data within an enterprise needs to be protected at all times and in all places. As a first step, an **enterprise needs to define what is sensitive data** and, if necessary, establish different levels of sensitive data. Then **there is a need to recognize sensitive data wherever it is encountered in the enterprise**. Finally, there must be applications that recognize sensitive data in real time.
The following are common approaches to the recognition task:

- **Rule-based recognition:** Regular expressions, keywords, and other basic pattern-matching techniques are best suited for basic structured data, such as credit card and Social Security numbers. This technique efficiently identifies data blocks, files, database records, and so on that contain easily recognized sensitive data.

- **Database fingerprinting:** This technique searches for exact matches to data loaded from a database, which can include multiple field combinations, such as name, credit card number, and CVV number. For example, a search could look only for credit card numbers in the customer base, thus ignoring employees buying online. This is a time-consuming technique but has a very low false positive rate.

- **Exact file matching:** This technique involves computing the **hash value of a file** and monitoring for any files that match the exact fingerprint. It is easy to implement and checks whether a file has been accidentally **stored or transmitted in an unauthorized manner**. However, unless a more time-consuming cryptographic hash function is used, this is trivial for an attacker to evade.

- **Partial document matching:** This technique involves looking for a partial match on a protected document. It involves the use of **multiple hashes on portions of the document**, such that if a portion of the document is extracted and filed elsewhere or pasted into an email, it can be detected. This technique is useful for protecting sensitive documents.

Data States

Key to effective DLP **is to develop an understanding of the places and times at which data are vulnerable.**

A useful way of managing DLP is to categorize data into **three states**: data in motion, data at rest, and data in use.

Corresponding to these three states are three key DLP objectives:

- **Data at rest:** Locate and catalog sensitive information stored throughout the enterprise.
- **Data in motion (or transit):** Monitor and control the movement of sensitive information across enterprise networks.
- **Data in use:** Monitor and control the movement of sensitive information on end-user systems.

DLP for Data at Rest

Data at rest presents significant risk for enterprises.

A large enterprise may have millions of files and database records on drives and removable media.

A particular set of data files or **records may have a "home" location**, but **portions of that data may also migrate to other storage** locations, and this situation, if not monitored and controlled, quickly becomes unmanageable.

One example of how data is replicated and proliferated is **file sharing**. With networked computer systems, file sharing for collaborative projects is common, but this may mean that the owner or creator of a file has no idea of what happened to the file after sharing it.

The same risk exists with the many **web-based collaboration** and document management platforms in common use.

The **fundamental task of DLP for data at rest is to identify and log where specific types of information are stored** throughout the enterprise. The DLP unit uses some sort of data discovery agent that performs actions

DLP for Data in Motion

The term **data in motion refers to data transmitted over enterprise networks** and between the enterprise networks and external network links

Data-in-motion solutions operate in one of two modes:

Passive monitoring

- Observes a copy of data packets as they move across a network link
- This is done by a port mirror on a switch or a network line tap
- Packets or sequences of packets containing information of interest are logged, and security violations trigger an alert

Active monitoring

- Interposes a relay or gateway type of device on a network line to analyze and forward data packets
- The active monitor logs and issues alerts but can also be configured to block data flows that violate a security policy

DLP for Data in Use

✓ **Data-in-use solutions generally involve installing DLP agent software on endpoint systems**

The agent monitors, reports, blocks, or quarantines the use of particular kinds of data files and/or the contents of a file

The agent also **maintains an inventory of files on the hard drives** and removable media that is **plugged** in to the endpoint

The **agent either allows or disallows certain types of removable media**, such as requiring that the removable device support encryption

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Simone **Soderi**

✉ simone.soderi@unipd.it

M3.3 - Cybersecurity Operations and Management

Thanks for your attention!