Cybersecurity Essentials: Information Management, Culture, and Tools

22 August 2024, 2:00PM - 5:00PM

Colllege of Innovation Management, SSRU

MYSURACHET.COM

Surachet Suchaiya, PhD.
Director of
Cyber Innovation Promotion
Association of Technology (CIPAT)

College of Innovation Management
Suan Sunandha Rajabhat University

MYSURACHET.COM

Surachet Suchaiya, PhD.

Educational history, work history
Expertise, experience
Training certificates received
and research.

Cybersecurity Essentials : Information Management, Culture, and Tools

Agenda

1. Information Security
2. Creating a culture of security awareness
3. Cybersecurity Tools
4. Conclusion, Questions & Answer

innovation management
MYSURACHET.COM

Chapter 1
Information Security

1 Information Security

1.1 Information Management

1.2 Identity Management

1.3 Authentication

1.4 Access Control

1.5 Monitoring and Auditing

1.6 Platform Security

1 Information Security

4.1 Information Management

- Data Storage
- Data Protection
- Access Management
- Risk Management

1 Information Security

1.1 Information Management

1 Information Security

1.1 Information Management

- Data Storage
  - Data Encryption
  - Data Backup

1 Information Security

1.1 Information Management

- Data Protection
  - Access Control
  - Monitoring and Auditing

1 Information Security

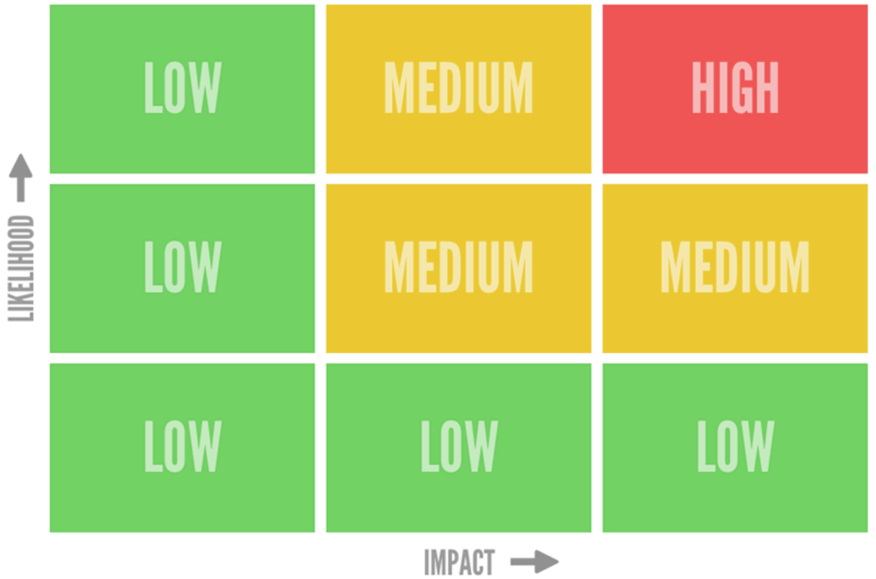
1.1 Information Management

- Access Management
  - Authentication
  - Authorization
  - Account

1 Information Security

1.1 Information Management

- Risk Management
  - Risk Assessment
  - Risk Mitigation



1 Information Security

1.2 Identity Management)

- Identity Identification
  - User Registration
  - Identity Data Storage

1 Information Security

1.3 Authentication

Something you
KNOW

Password or phrase
PIN

Something you
HAVE

Code from app or SMS
Push notification
USB token

Something you
ARE

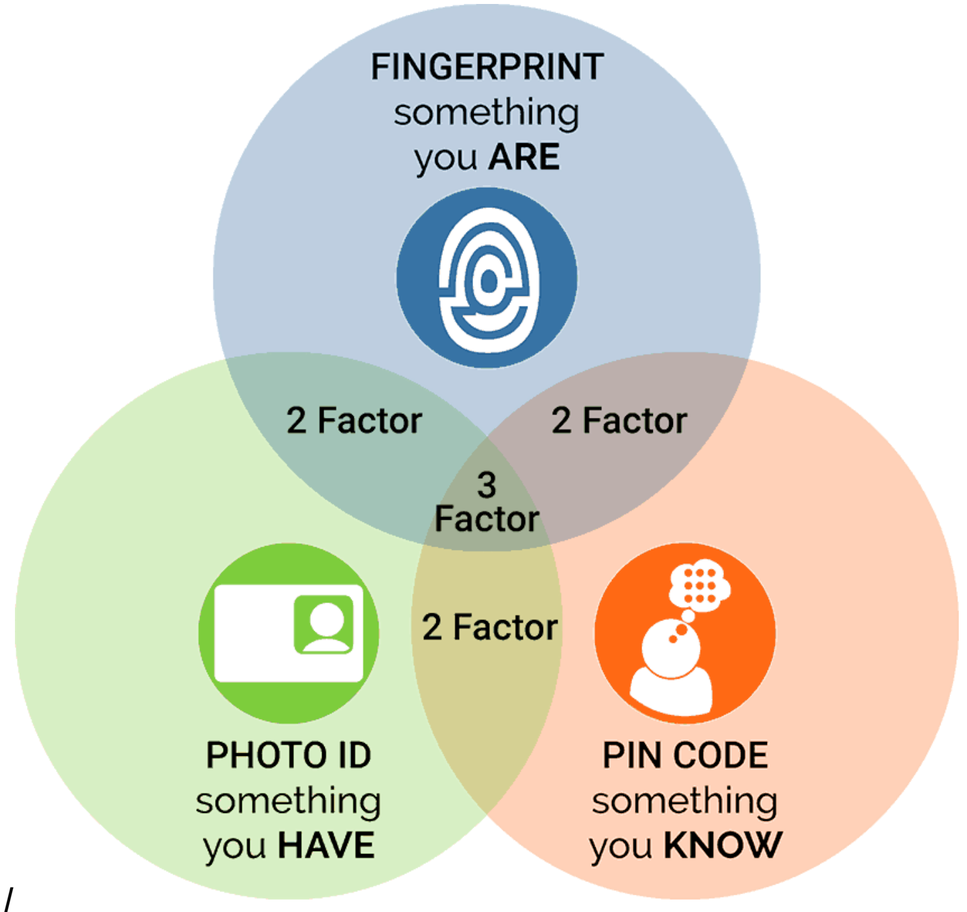
Finger or thumb print
Face scan
Iris scan

ข้อมูลจาก https://www.hsph.harvard.edu

1 Information Security

1.3 Authentication

- Multi-Factor Authentication - MFA
- Password Management



ข้อมูลจาก https://www.borer.co.uk/

1 Information Security

1.4 Access Control

- Role-Based Access Control - RBAC
- Attribute-Based Access Control - ABAC
- Mandatory Access Control - MAC

1 Information Security

1.4 Access Control

- Role-Based Access Control - RBAC
  - Access by employee role, such as manager, salesperson, administrator

1 Information Security

1.4 Access Control

- Attribute-Based Access Control - ABAC
  - Allow access to specific resources during working hours or from specific locations.

1 Information Security

1.4 Access Control

- Mandatory Access Control - MAC
  - It is a control of high-level security systems, such as the military or government agencies, where the level of confidentiality and access rights are determined according to the level of confidentiality according to the command position.

1 Information Security

1.5 Monitoring and Auditing

- Access Logging
- Analysis and Reporting

1 Information Security

1.6 Platform Security

- Operating System Security
- Software Security
- Hardware Security
- Monitoring and Auditing
- Risk Management

1 Information Security

1.6 Platform Security

- Operating System Security
  - System Updates and Patches
  - Secure Configuration

1 Information Security

1.6 Platform Security

- Software Security
  - Secure Software Development
  - Vulnerability Scanning

1 Information Security

1.6 Platform Security

- Hardware Security
  - Hardware Access Control
  - Security Technologies

1 Information Security

1.6 Platform Security

- Monitoring and Auditing
  - Event Logging
  - Event Monitoring

1 Information Security

1.6 Platform Security

- Risk Management
  - Risk Assessment
  - Risk Mitigation

1 Information Security

Summarize Lesson : Information Security

- Confidentiality
- Integrity
- Availability)
- Identity Management
- Authentication
- Access Control
- Platform Security

Chapter 2
Creating a culture of security awareness

2 Creating a culture of security awareness

2.1 Risky behaviors that may lead to security vulnerabilities in the organization

2.2 Impacts that may occur from information security breaches

2.3 Roles and responsibilities of personnel in various departments related to information security

2.4 Creating and promoting a security culture in the organization

2.5 The process of creating a cybersecurity culture within the organization

2 Creating a culture of security awareness

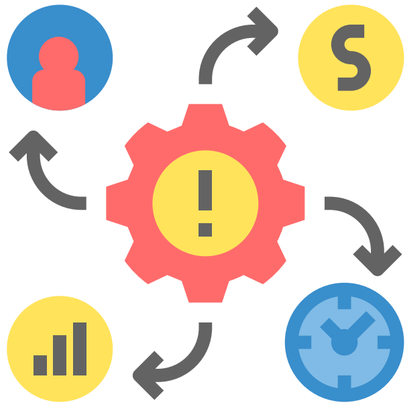
2.1 Risky behaviors that may lead to security vulnerabilities in the organization

- Using outdated software
- Using weak passwords
- Using public Wi-Fi
- Opening insecure attachments
- Neglecting training

2 Creating a culture of security awareness

2.2 Impacts that may occur from information security breaches

- Financial damage
- Damage to reputation
- Damage to operations
- Legal impact



2 Creating a culture of security awareness

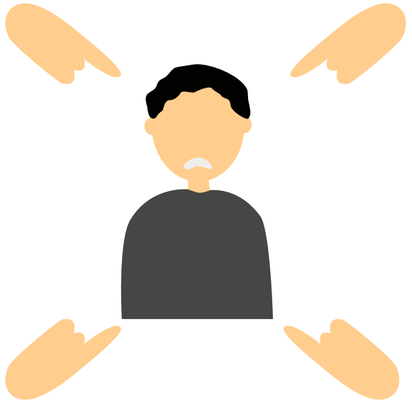
2.2 Impacts that may occur from information security breaches

- Financial damages
  - Fines and penalties
  - Remedial costs
  - Loss of income

2 Creating a culture of security awareness

2.2 Impacts that may occur from information security breaches

- Reputation damage
  - Loss of customer trust
  - Corporate image



2 Creating a culture of security awareness

2.2 Impacts that may occur from information security breaches

- Operational Damage
  - Business Interruption
  - Loss of Critical Data

2 Creating a culture of security awareness

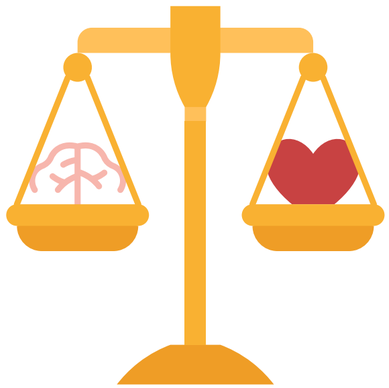
2.2 Impacts that may occur from information security breaches

- Legal Impact
  - Litigation
  - Non-compliance with laws and standards

2 Creating a culture of security awareness

2.2 Impacts that may occur from information security breaches

- Legal Implications
  - Case Study: High-profile Organization Data Security Breach
    - Yahoo Data Breach in 2013 and 2014
    - Case Study: Facebook Data Breach in 2018



2 Creating a culture of security awareness

2.3 Roles and responsibilities of personnel in various departments involved in maintaining information security

- Senior Management
- Information Security Officer
- System Administrator
- End Users
- Risk Manager
- Software Developer

2 Creating a culture of security awareness

2.3 Roles and responsibilities of personnel in various departments involved in maintaining information security

- Senior Management
  - Set policies and directions
  - Allocate resources
  - Promote a culture of security

2 Creating a culture of security awareness

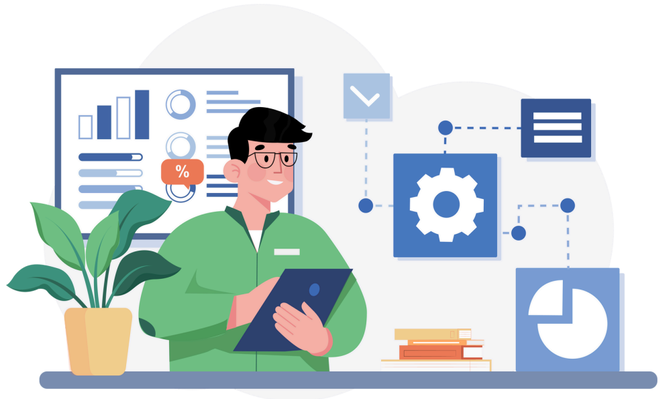
2.3 Roles and responsibilities of personnel in various departments involved in maintaining information security

- Information Security Officer
  - Plan and implement policies
  - Assess and monitor risks
  - Consult and train

2 Creating a culture of security awareness

2.3 Roles and responsibilities of personnel in various departments involved in maintaining information security

- System Administrator
  - Maintain systems and networks
  - Install and update software
  - Monitor and respond to incidents



2 Creating a culture of security awareness

2.3 Roles and responsibilities of personnel in various departments involved in maintaining information security

- End Users
  - Policy and Practice Compliance
  - Reporting Unusual Events
  - Training and Awareness

2 Creating a culture of security awareness

2.3 Roles and responsibilities of personnel in various departments involved in maintaining information security

- Risk Manager
  - Risk identification and assessment
  - Risk management planning
  - Monitoring and reporting

2 Creating a culture of security awareness

2.3 Roles and responsibilities of personnel in various departments involved in maintaining information security

- Software Developer
  - Writing secure code
  - Testing and auditing security
  - Updating and maintaining

2 Creating a culture of security awareness

2.4 Creating and promoting a culture of security in the organization

- Motivating employees to participate in security
- Organizing activities and programs that promote security awareness
- Organizing activities and games to promote security awareness
- Evaluating and measuring the success of security awareness programs

2 Creating a culture of security awareness

2.4 Creating and promoting a culture of security in the organization

- Motivating employees to participate in security
  - Rewarding and Recognition
  - Participation in decision-making

2 Creating a culture of security awareness

2.4 Creating and promoting a culture of security in the organization

- Organizing activities and programs that promote security awareness
  - Training and Workshops
  - Seminars and Lectures

2 Creating a culture of security awareness

2.4 Creating and promoting a culture of security in the organization

- Organizing activities and games to promote security awareness
  - Games and competitive activities
  - Using interactive media

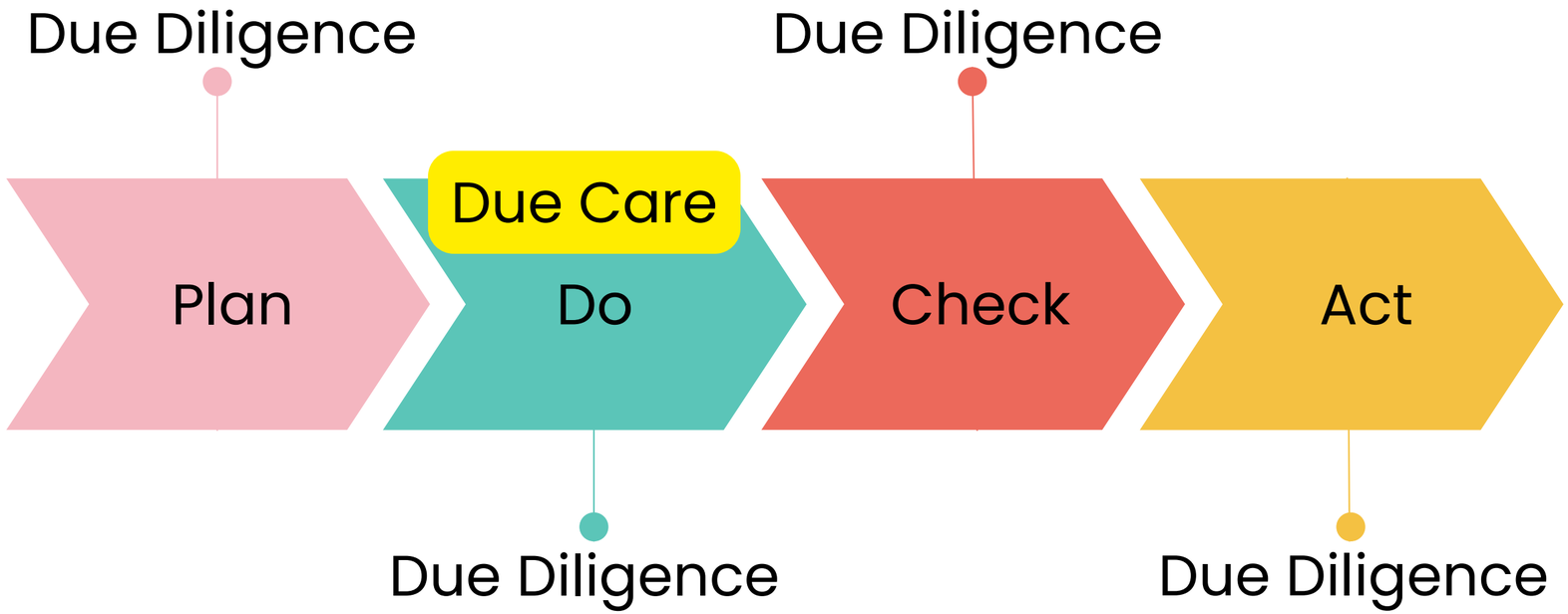
2 Creating a culture of security awareness

2.4 Creating and promoting a culture of security in the organization

- Evaluating and measuring the success of security awareness programs

Awareness Level

- Due Care
- Due Diligence



2 Creating a culture of security awareness

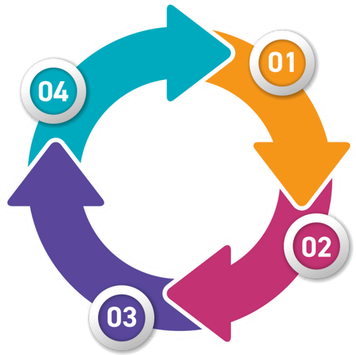
2.4 Creating and promoting a culture of security in the organization

- Evaluating and measuring the success of security awareness programs
  - Questionnaire and Evaluation
  - Analysis and Reporting

2 Creating a culture of security awareness

2.5 Process for creating a cybersecurity culture within the organization

- Assessing the Current State of the Organization's Cybersecurity
- Creating Senior Executive Accountability for Building an Organizational Cybersecurity Culture
- Case Study: Building an Organizational Cybersecurity Culture: Yahoo



2 Creating a culture of security awareness

Summarize Lesson : Creating a culture of security awareness

- Using outdated software
- Using weak passwords
- Using public Wi-Fi
- Social Engineering
- Creating a culture of awareness in the organization
- Creating and promoting a culture of security in the organization

Chapter 3
Cybersecurity Tools

3 Cybersecurity Tools

3.1 Firewalls

3.2 Intrusion Detection and Prevention Systems, IDS/IPS

3.3 Security information and event management (SIEM)

3.4 Security Orchestration, Automation, and Response (SOAR)

3.5 Endpoint Detection Response (EDR)

3.6 Network Detection Response (NDR)

3.7 Security Operation Center (SOC)

3 Cybersecurity Tools

3.1 Firewall

Hardware Firewalls , Intrusion Detection and Prevention Systems, IDS/IPS

3 Cybersecurity Tools

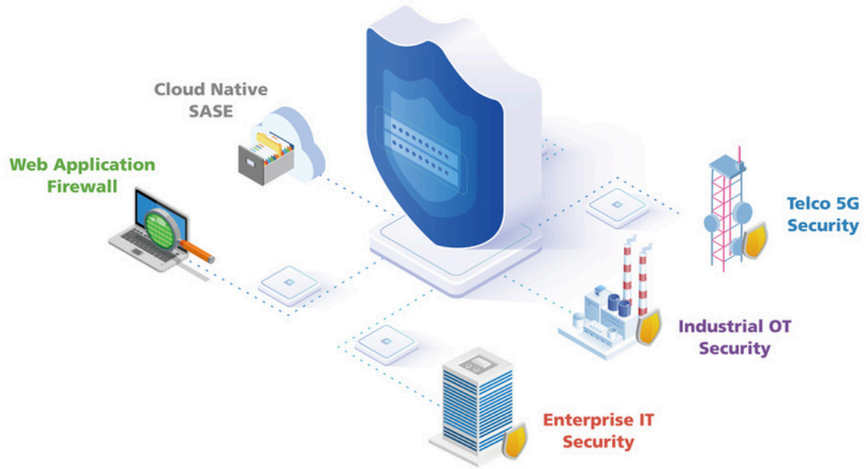
3.1 Firewall

- Network Firewall : Installed at the connection point between two computer networks, such as between an internal network and the Internet.
- Host Firewall : firewalls that are installed on each computer device.

3 Cybersecurity Tools

3.1 Firewall

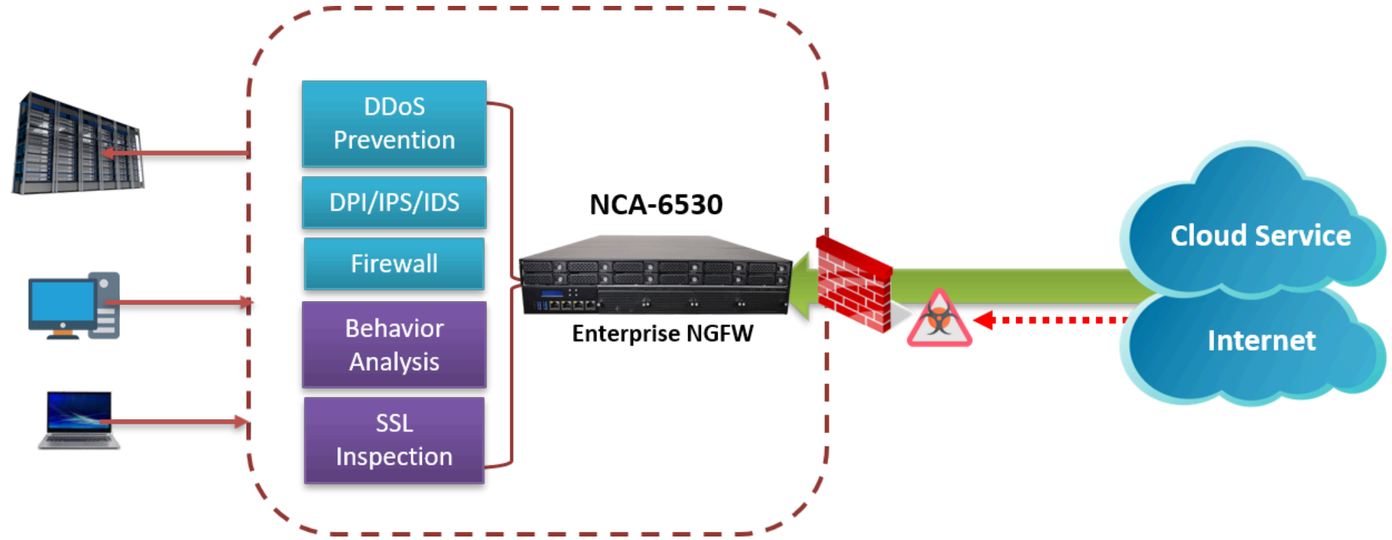
- Firewall's primary functions
  - Proxy to internet
  - Rules : Stateful inscpection packet data, Packet Filtering
  - Policy
  - Monitoring and Review



3 Cybersecurity Tools

3.2 Intrusion Detection and Prevention Systems, IDS/IPS

- Benefits
  - Protects computer systems from cybersecurity threats
  - Helps respond quickly to cybersecurity incidents
  - Helps improve the efficiency of cybersecurity management processes



3

Cybersecurity Tools

3.3 Security information and event management (SIEM)

3

Cybersecurity Tools

3.3 Security information and event management (SIEM)

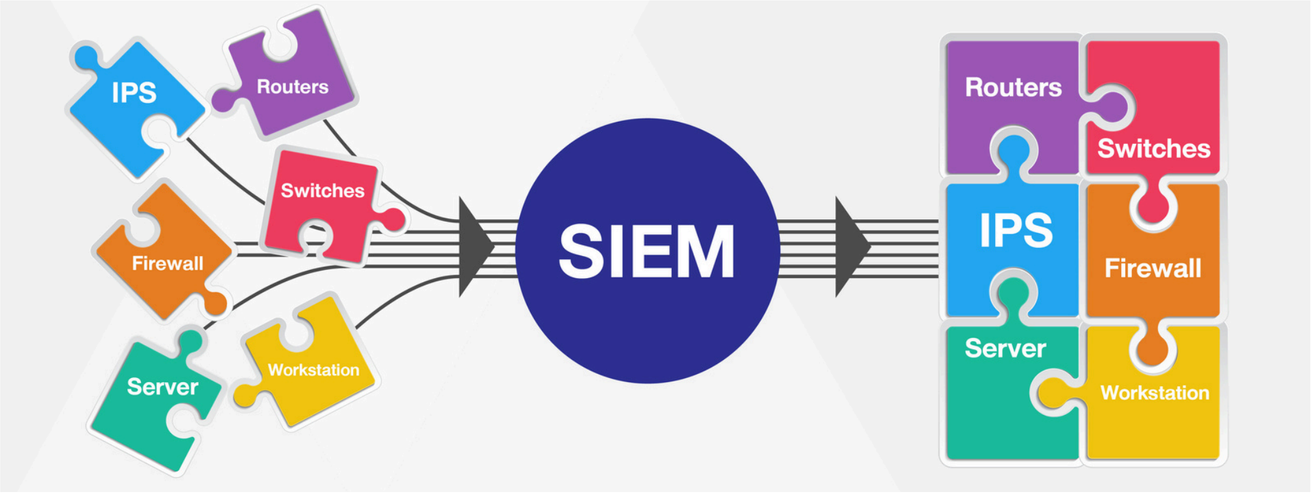
3 Cybersecurity Tools

3.3 Security information and event management (SIEM)

3 Cybersecurity Tools

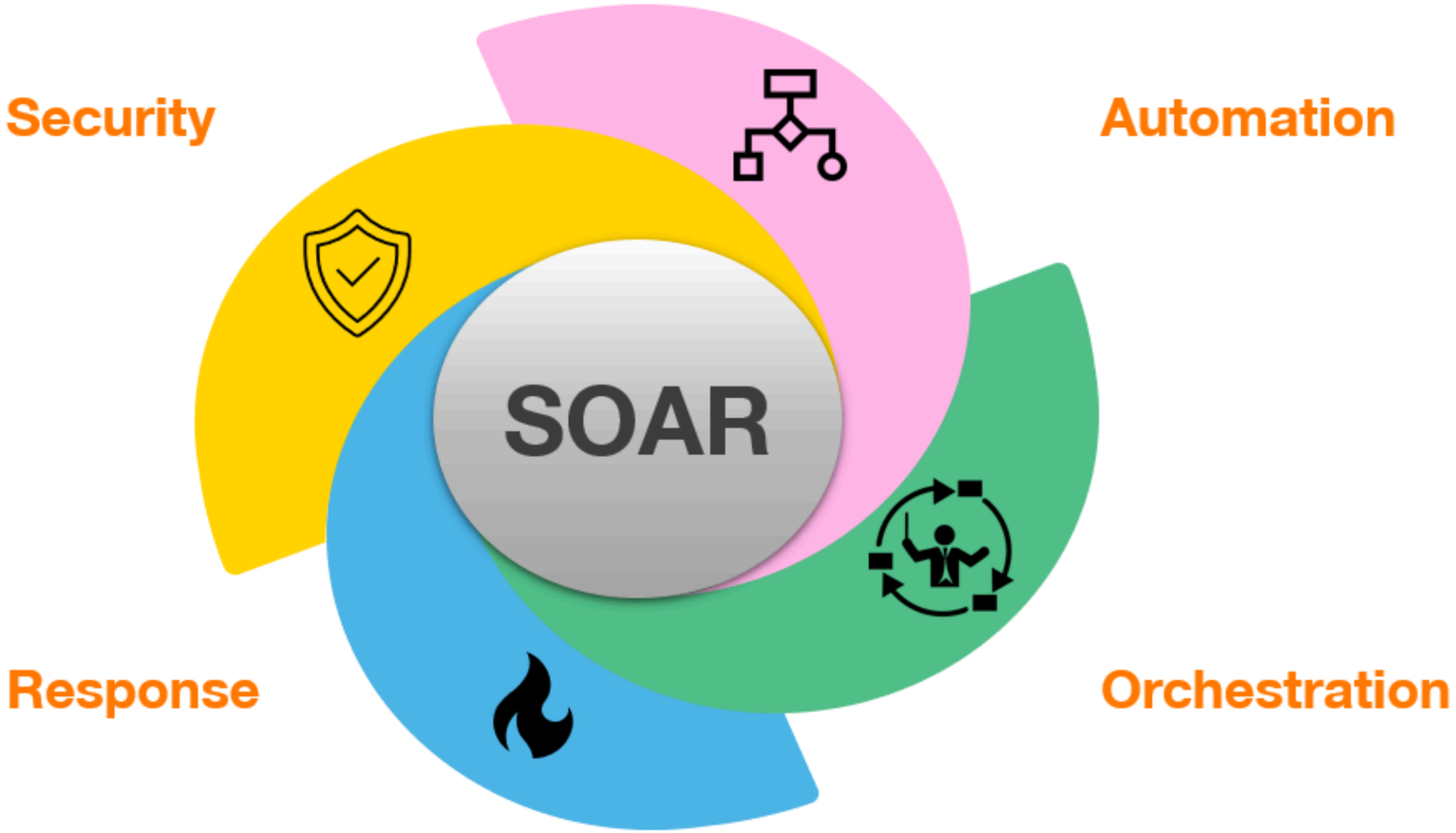
3.3 Security information and event management (SIEM)

- Benefits of using a SIEM system
  - Increase visibility into security incidents
  - Identify threats quickly and efficiently
  - Reduce potential damage from threats
  - Reduce security costs



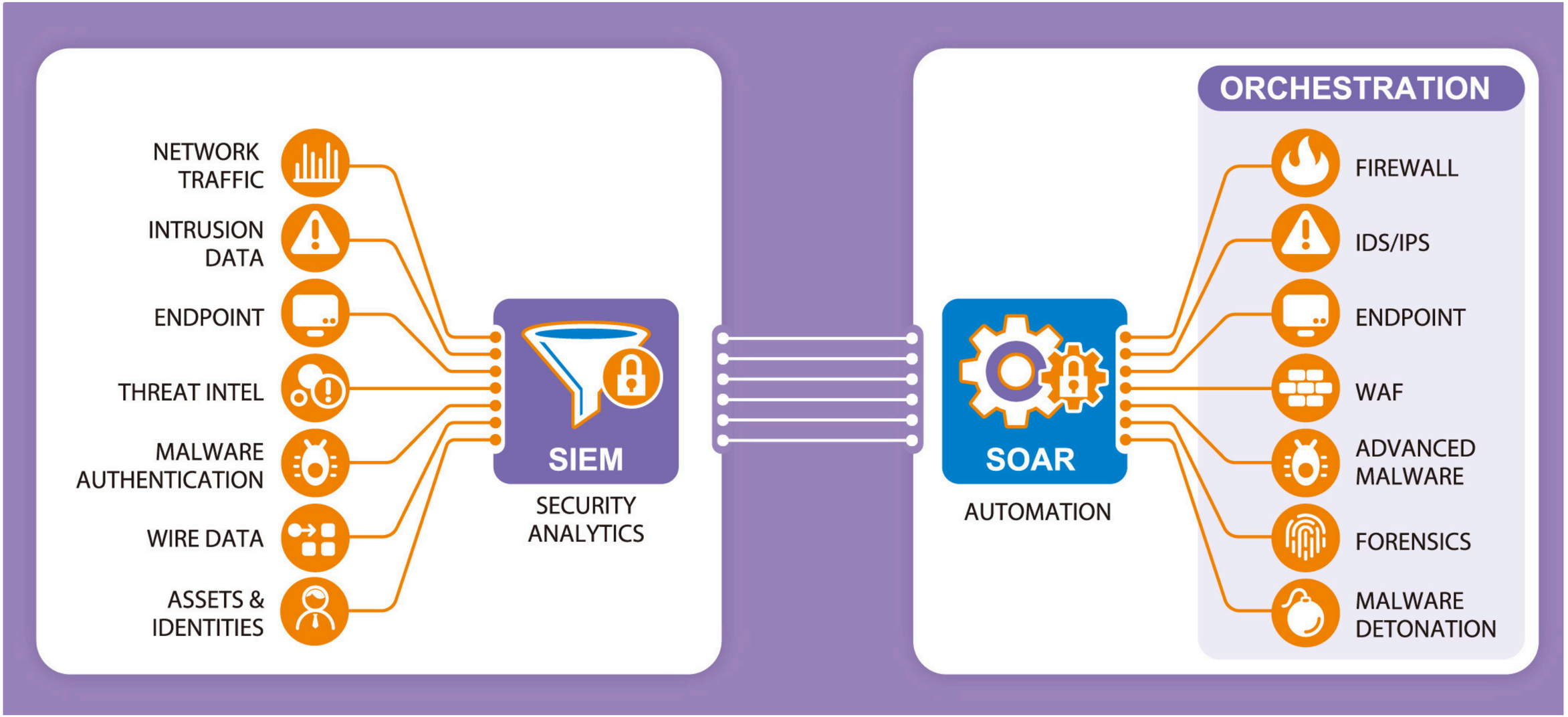
3 Cybersecurity Tools

3.4 Security Orchestration, Automation, and Response (SOAR)



3 Cybersecurity Tools

3.4 Security Orchestration, Automation, and Response (SOAR)



3 Cybersecurity Tools

3.4 Security Orchestration, Automation, and Response (SOAR)

- Security Orchestration, Automation and Response (SOAR) is a system that coordinates, automates, and responds to security events. SOAR collects event data from various devices on the network.
- SOAR coordinates with various security tools to automate tasks according to specified procedures, such as blocking access, deleting malicious files, etc.
- SOAR automatically responds to security events, such as alerting security personnel, issuing commands for security tools, etc.

3 Cybersecurity Tools

3.4 Security Orchestration, Automation, and Response (SOAR)

- Benefits of using SOAR systems
  - Increase the speed and efficiency of response to security incidents
  - Reduce the workload of security officers
  - Reduce the risk of damage from security incidents

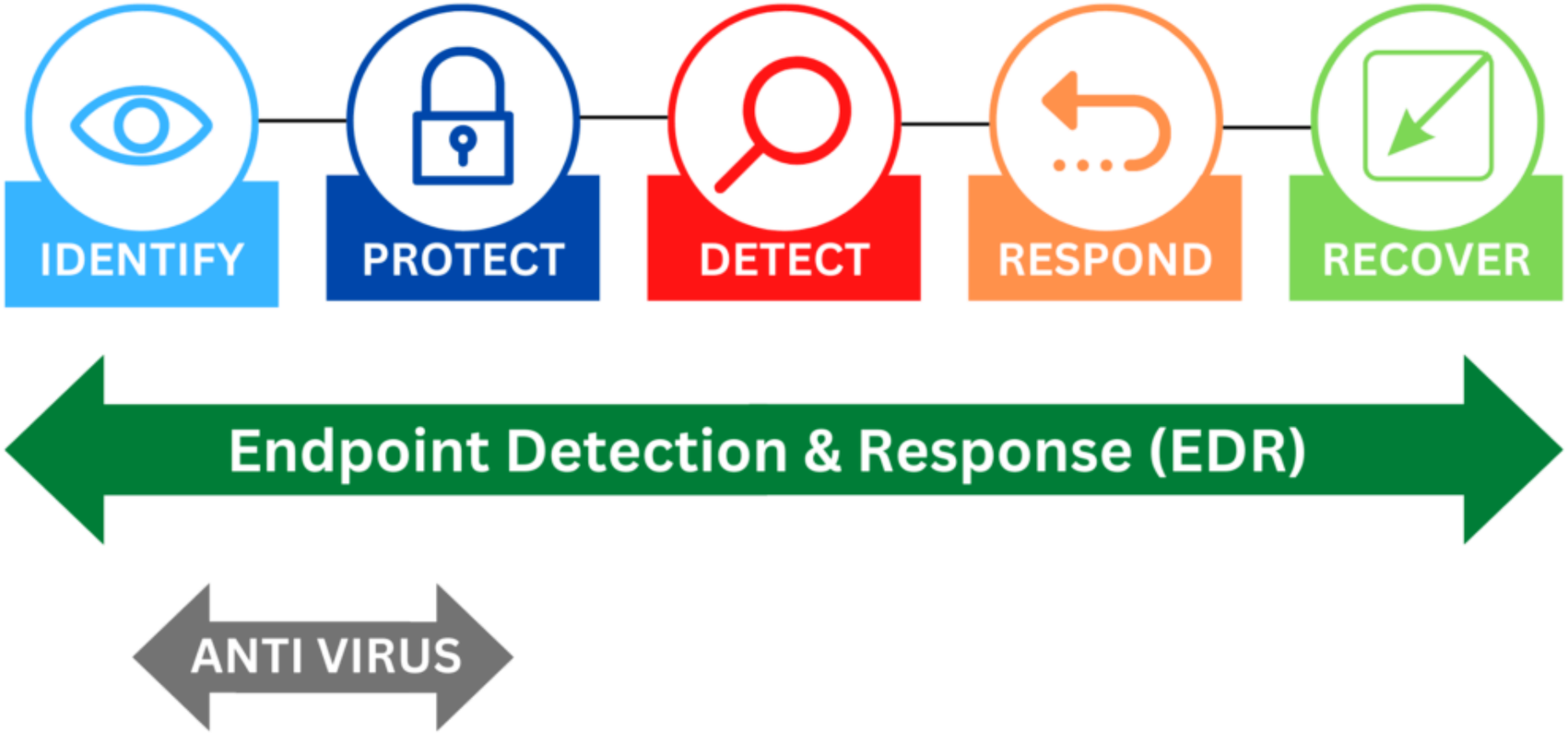
3 Cybersecurity Tools

3.4 Security Orchestration, Automation, and Response (SOAR)

- Differences between SIEM and SOAR systems
  - SOAR systems are more capable of automating tasks than SIEM systems. SOAR systems can automate many of the tasks that security officers perform, such as gathering event data, alerting, and responding to security incidents.

3 Cybersecurity Tools

3.5 Endpoint Detection Response (EDR)



3

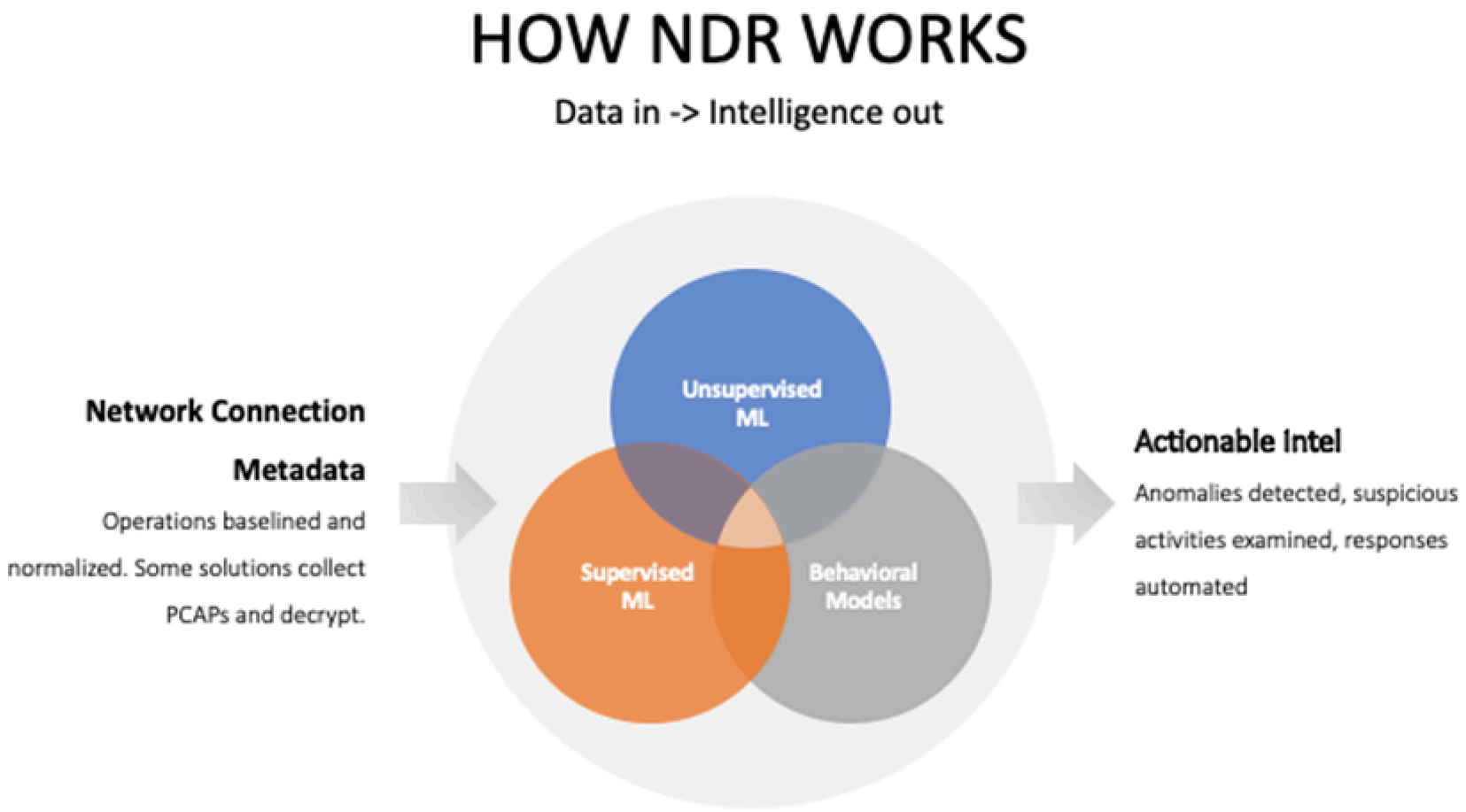
Cybersecurity Tools

3.6 Network Detection Response (NDR)

3

Cybersecurity Tools

3.6 Network Detection Response (NDR)



3

Cybersecurity Tools

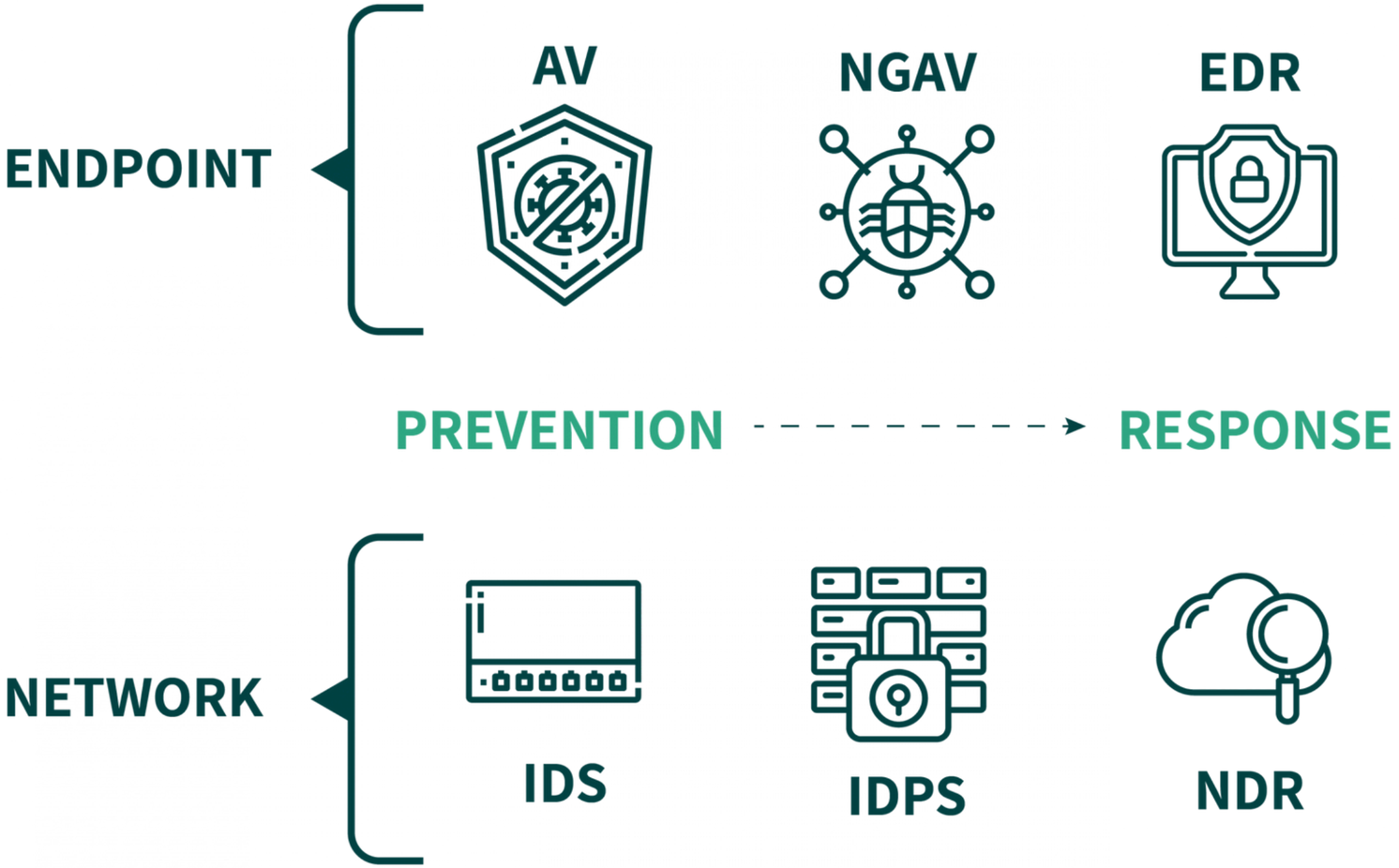
3.6 Network Detection Response (NDR)

3

Cybersecurity Tools

3.6 Network Detection Response (NDR)

Difference between EDR and NDR



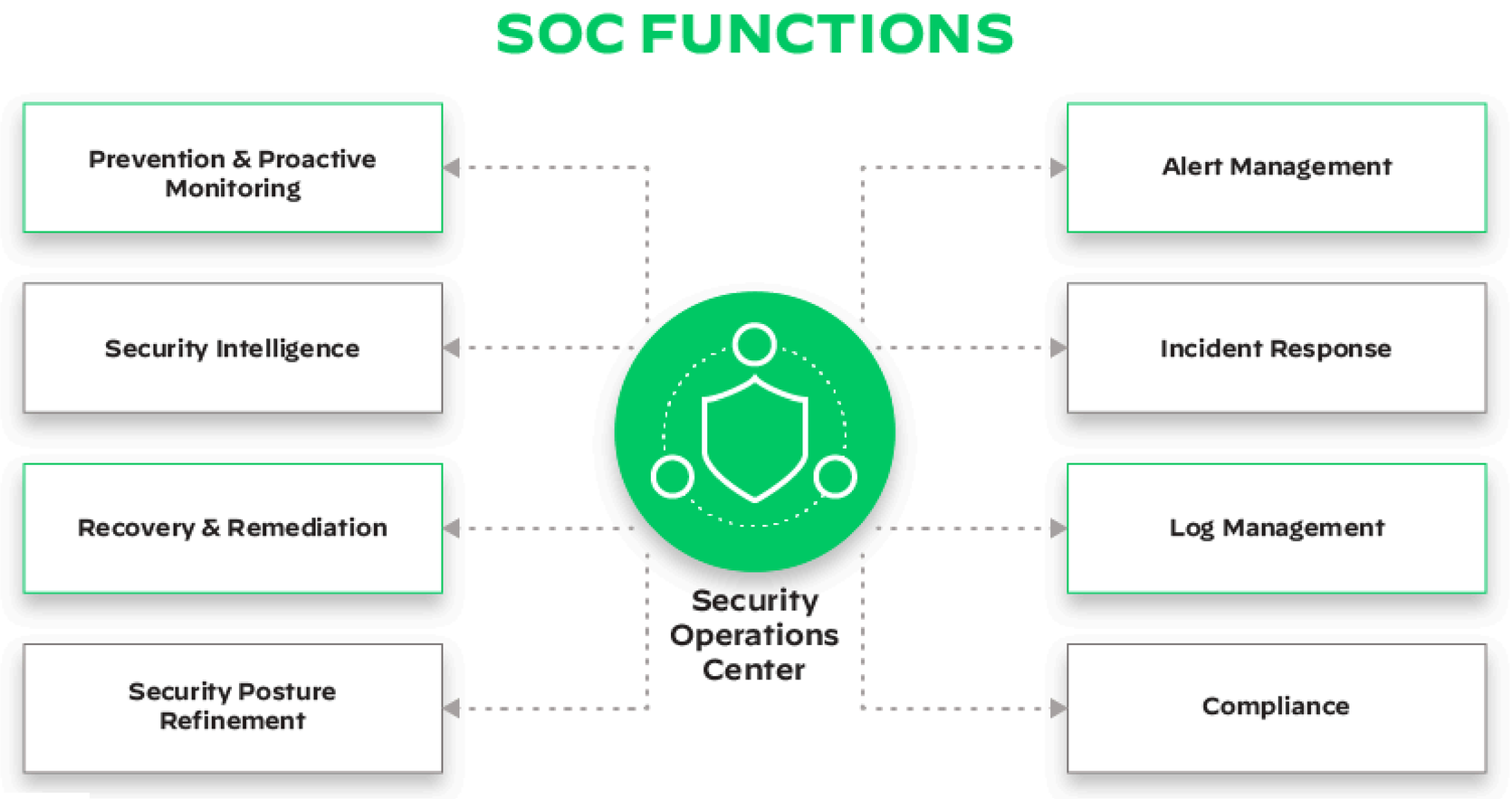
3

Cybersecurity Tools

3.7 Security Operation Center (SOC)

3 Cybersecurity Tools

3.7 Security Operation Center (SOC)



3

Cybersecurity Tools

3.7 Security Operation Center (SOC)

SECURITY OPERATION CENTER ROLES

SOC Manager

The **leaders of their organization**, top-level responsibilities fall to them and they report directly to the CISO.

Compliance Auditor

Plays a **key role in the standardization of processes,** they ensure protocols and compliance are being followed.

Incident Responder

They **react quickly to alerts** and when necessary they react to alerts as soon as possible.

SOC Analyst

They are responsible for reviewing past incidents and **determining the root cause** behind them.

Threat Hunter

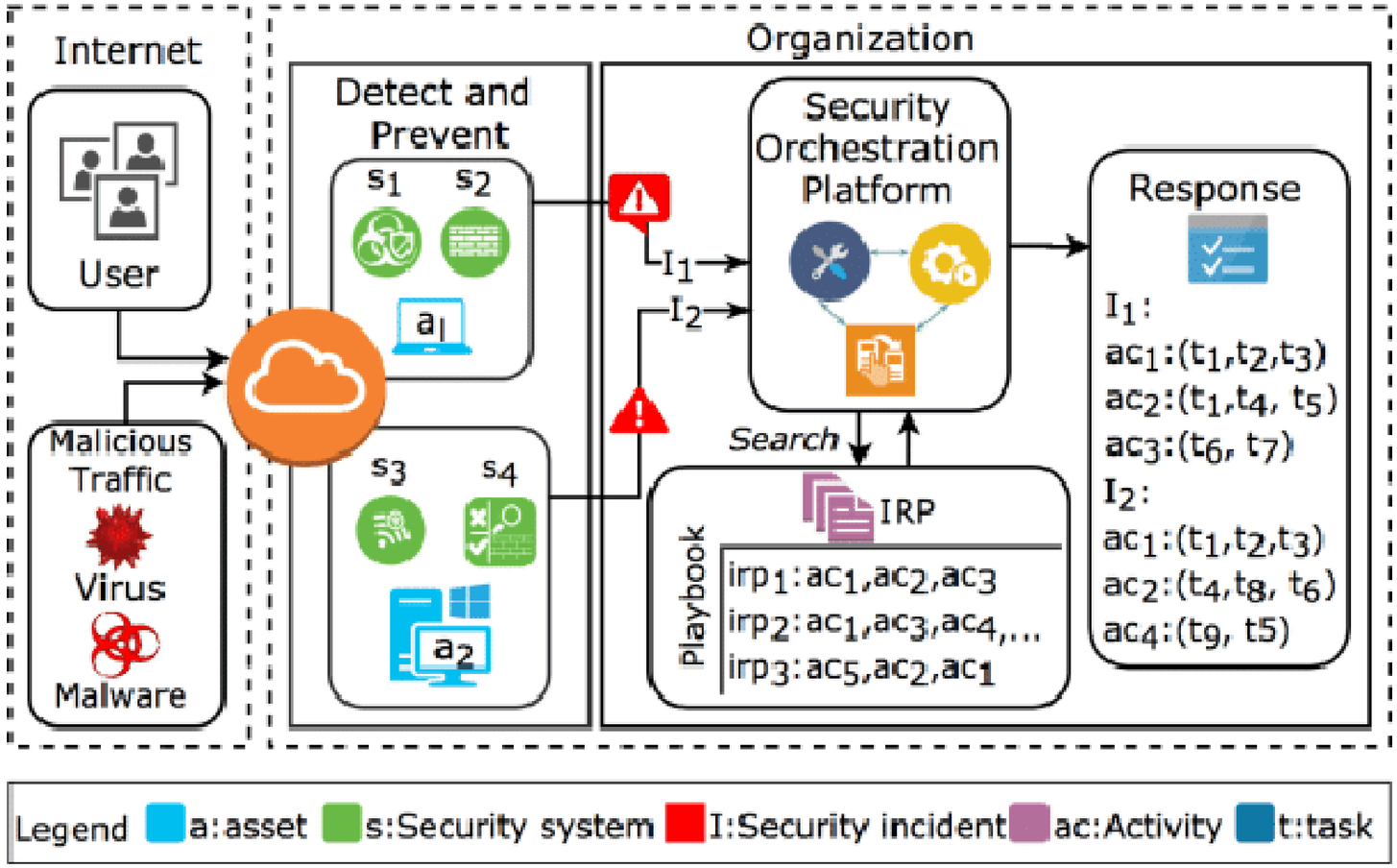
Run tests across a network to **identify weaknesses** before they can be exploited.

3

Cybersecurity Tools

3.7 Security Operation Center (SOC)

Example : Incident response process in a security orchestration platform

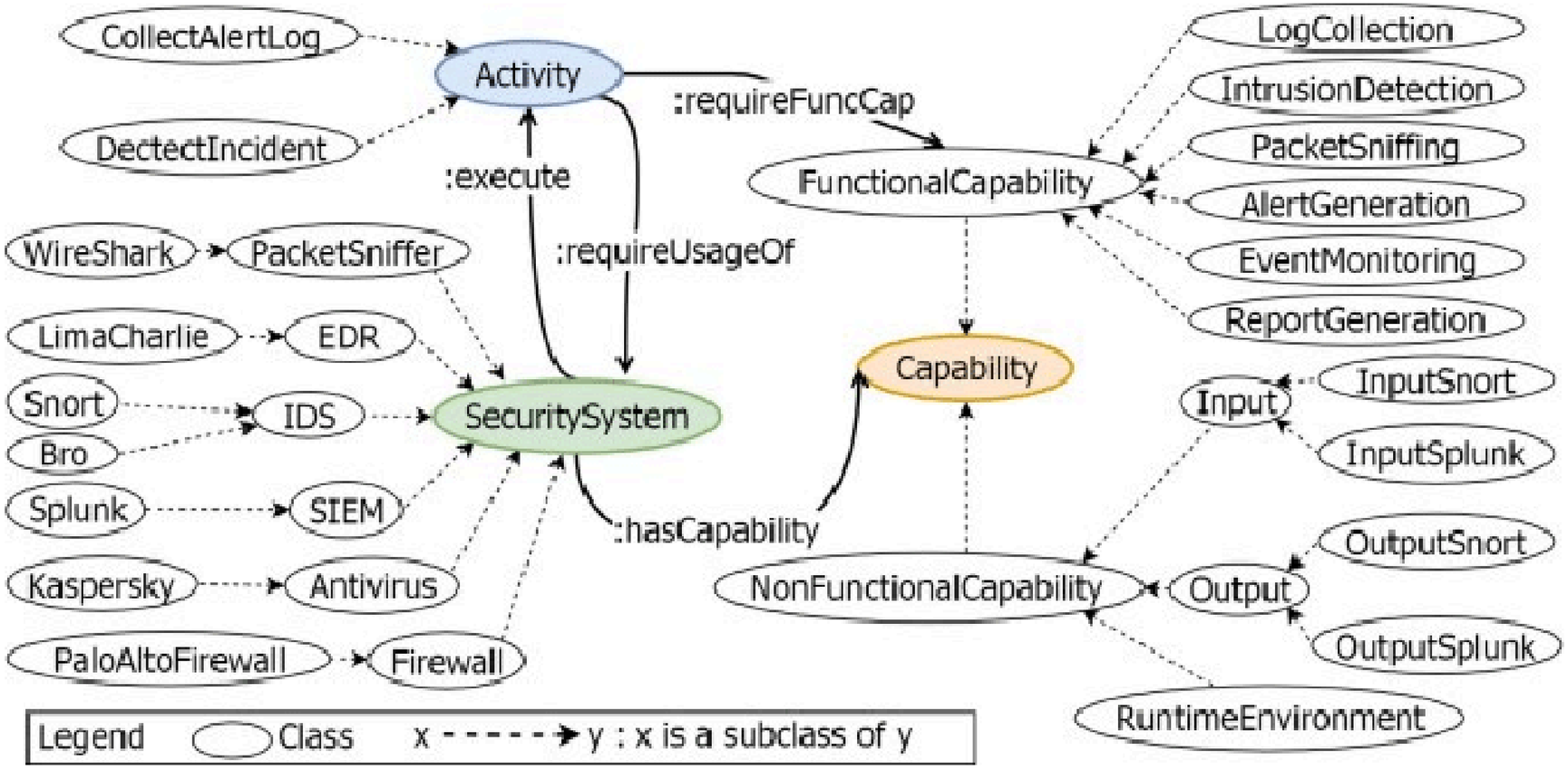


3

Cybersecurity Tools

3.7 Security Operation Center (SOC)

An Ontology-driven Approach to Automate the Integration Process of Security Software Systems



Chapter 4
Cybersecurity Tools

4 Conclusion, Questions & Answer

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

MYSURACHET.COM

Questions & Answer

ขอบคุณครับที

www.MySurachet.com

085 636 2551

surachet@catinfonet.com

Thank you

LINE

LINE