Defensive Security

Cybersecurity Bootcamp 2024

Disclaimer

This learning material is addressed and used only for Cybersecurity Bootcamp 2024 and should not be used or relied upon for any other purposes. Our learning material is not to be disseminated to or used by any third party in whole or in part without prior consent and permission from Kasikorn Technology Group Secretariat Company Limited (KBTGSec). Accordingly, we will not accept or take any responsibility or liability for any party or any person, whether or not such material is shown, disseminated, obtained, or possessed to such party or person since such material is only for educational purposes. We reserve all of our rights, including but not limited to intellectual property rights in our learning material, such as presentations, spreadsheets, system techniques, ideas, concepts, information, forms, electronic tools, forming parts of the materials, etc. © 2024 KASIKORN Business-Technology Group (KBTG) All rights reserved."

Topic overview

1. Protec, Detect, and Respond
2. Security Monitoring Technology
3. Threat Intelligence
4. Incident Response and Forensic
5. Threat Hunting

14

CHAPTERs

Key objective

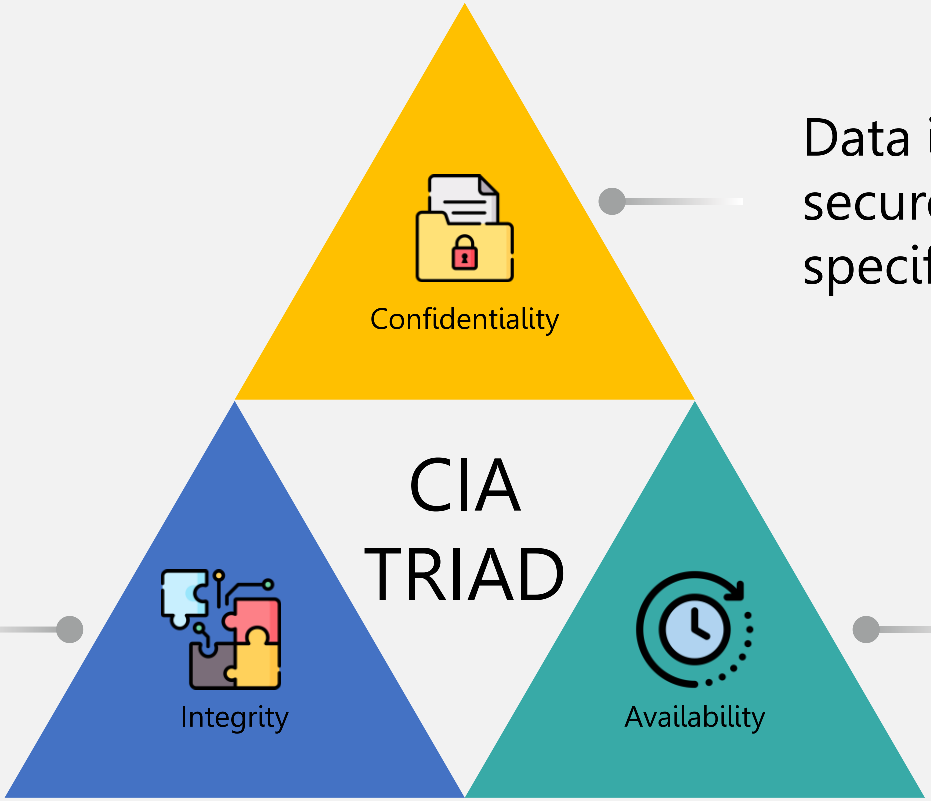
1. What is defensive security?
2. How to defensive security works?
3. How to create a secure environment?
4. Defensive security technology

01 Overview

01 Overview

- CIA Triad
- People Process Technology – Cybersecurity
- Offensive Security VS Defensive Security

CIA Triad

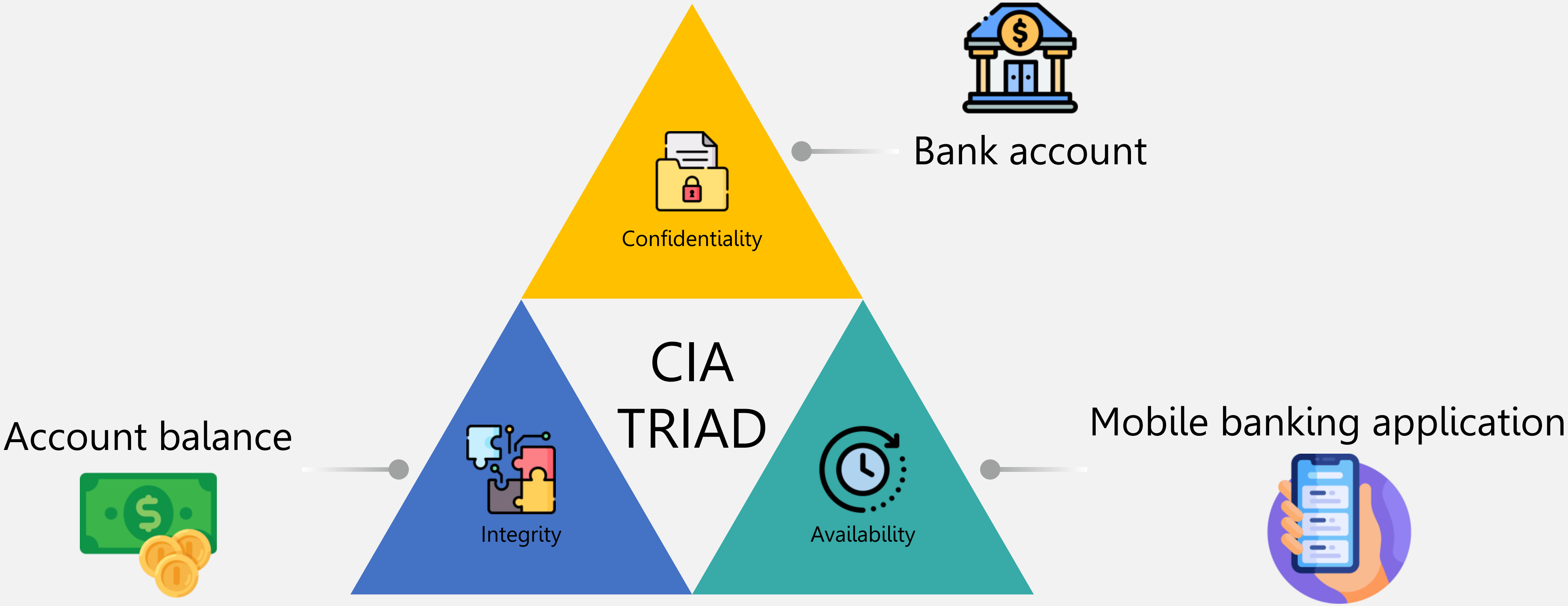


Data is kept private, secret and secure only to be accessed by specific parties

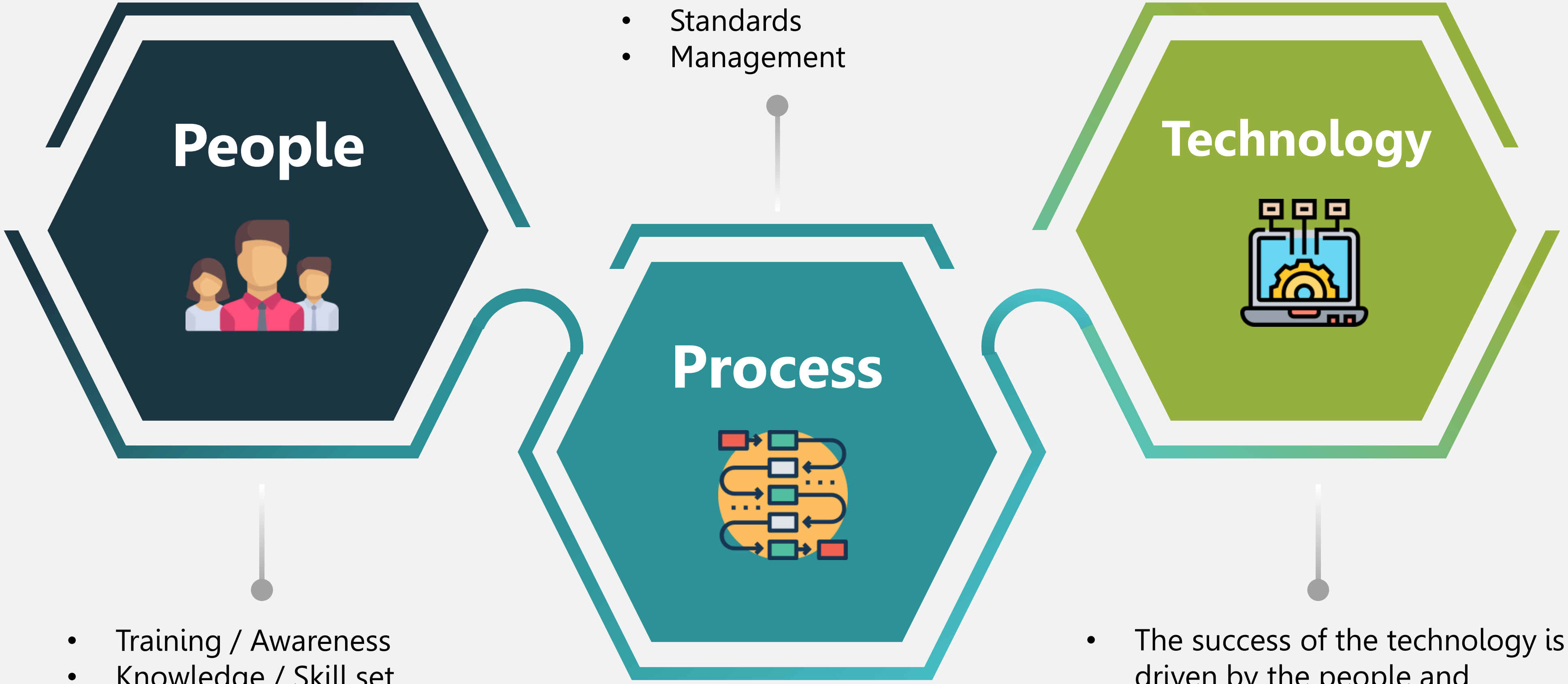
Data and the security around it is consistent, accurate and reliable

Systems and applications remain available unless compromised in an attack

Example : CIA Triad



People Process Technology (PPT) - Cybersecurity



- Strategic planning
- Frameworks
- Standards
- Management

- Training / Awareness
- Knowledge / Skill set
- Company culture

- The success of the technology is driven by the people and processes of the organization

Defensive Security VS Offensive Security

Defensive Security

Defensive Security, on the other hand, refers to protecting computer systems and networks from attack by identifying and mitigating vulnerabilities and implementing measures to prevent or detect unauthorized access or activity.

Offensive Security

Offensive Security refers to the practice of actively attacking and exploiting computer systems and networks to test their defenses and identify vulnerabilities.

Key Takeaways

- CIA Triad
- People Process Technology
- Offensive Security VS Defensive Security

02

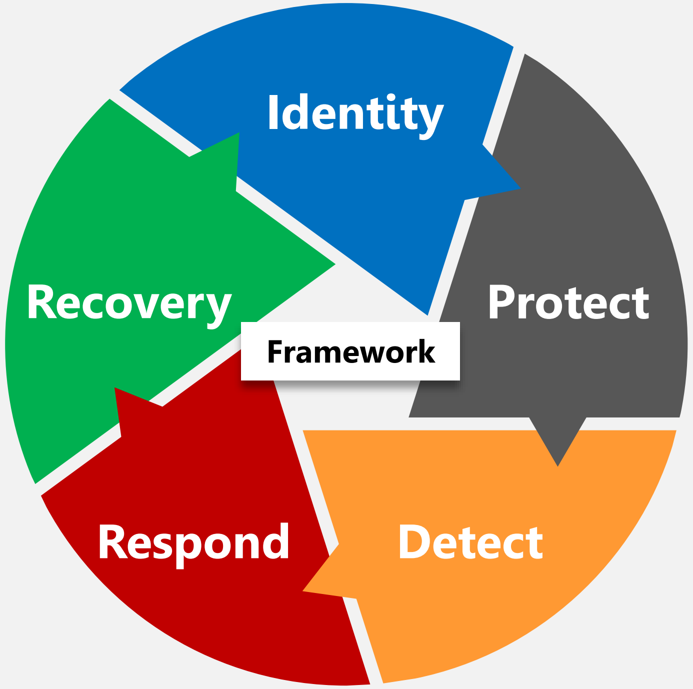
Protect, Detect, and Respond

KBTG KASIKORN BUSINESS-TECHNOLOGY GROUP

NIST Cybersecurity Framework

The **NIST Cybersecurity Framework (CSF)** provides guidance on how to manage and reduce IT infrastructure security risk.

The CSF is made up of standards, guidelines and practices that can be used to protect, detect and respond to cyberattacks.



NIST Cybersecurity Framework

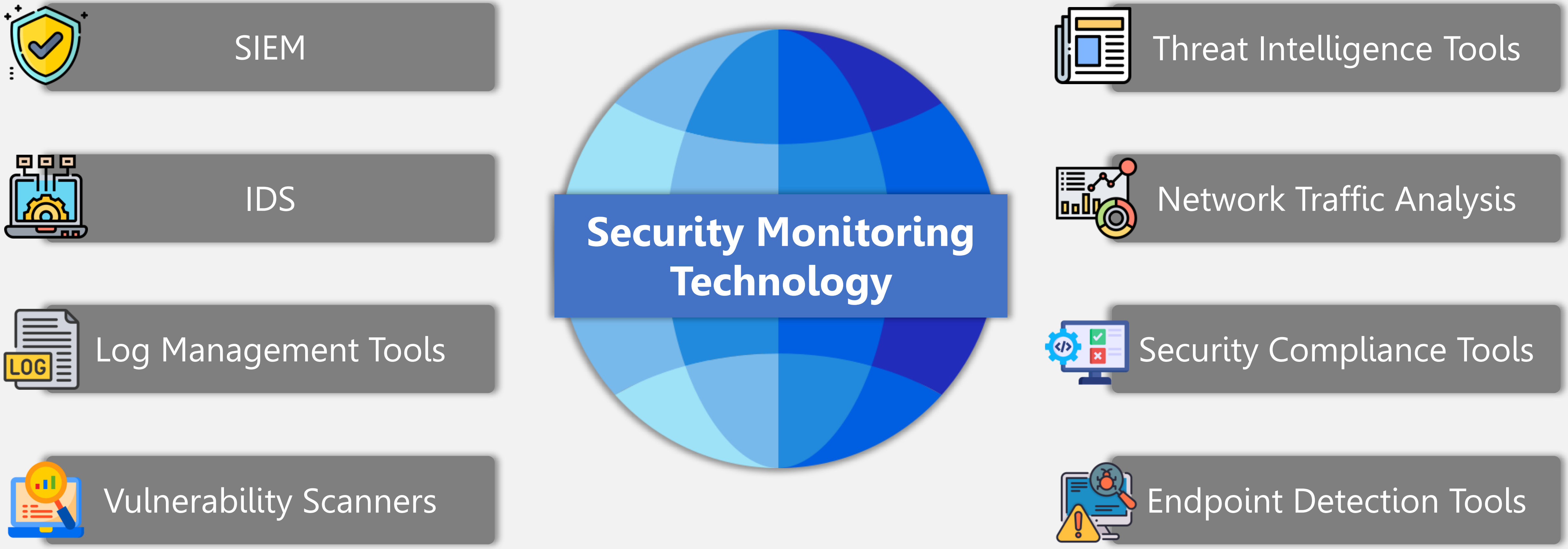
Identity	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recover Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communication	Improvements
Governance	Data Security	Detection Processes	Analysis	Communication
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Key Takeaways

- NIST Cybersecurity Framework (CSF)

03 Security Monitoring Technology

03 Security Monitoring Technology



Security Monitoring Technology

- SIEM
- IDS
- Log Management Tools
- Vulnerability Scanners
- Threat Intelligence Tools
- Network Traffic Analysis
- Security Compliance Tools
- Endpoint Detection Tools

Security information and event management (SIEM)

Security information and event management tools help maintain a unified repository of security-logs in real-time. By gathering data from multiple sources, these tools enable event correlation and raise context-rich suspicious activity alerts.

Intrusion detection systems (IDS)

Intrusion detection systems serve as an early warning system for any unauthorized access, abnormal network behavior, malware infections etc. Network traffic is compared to baseline normal activities to identify any indicators of compromise and flag suspicious behavior.

Log Management Tools

Log Management Tools used to monitor and analyze log data in order to identify potential issues, track performance, and gain insights into the behavior of an organization's systems and devices.

Vulnerability scanners

Vulnerability scanners scan networks and systems to identify weaknesses or vulnerable points that can be exploited by hackers. These vulnerabilities include misconfigurations, weak passwords, suspicious applications and more.

Threat Intelligence Tools

Threat intelligence tools read raw data on existing and emerging threats and threat actors from multiple sources. The data is analyzed and filtered to develop intelligence feeds and reports that can be used by automated security solutions.

Network Traffic Analysis (NTA)

Network traffic analysis (NTA) is a method of monitoring network availability and activity to identify anomalies, including security and operational issues.

Security Compliance Tools

Security and compliance tools are inherently connected and so compliance automation solutions facilitate efficient cybersecurity monitoring. These tools give real-time visibility on security posture, evaluate effectiveness of security controls, escalate deviations while enforcing security policies.

Endpoint Detection Tools

Endpoint Detection Tools software dedicated to tracking, monitor, and managing the myriad of endpoint devices used by the organization.

Key Takeaways

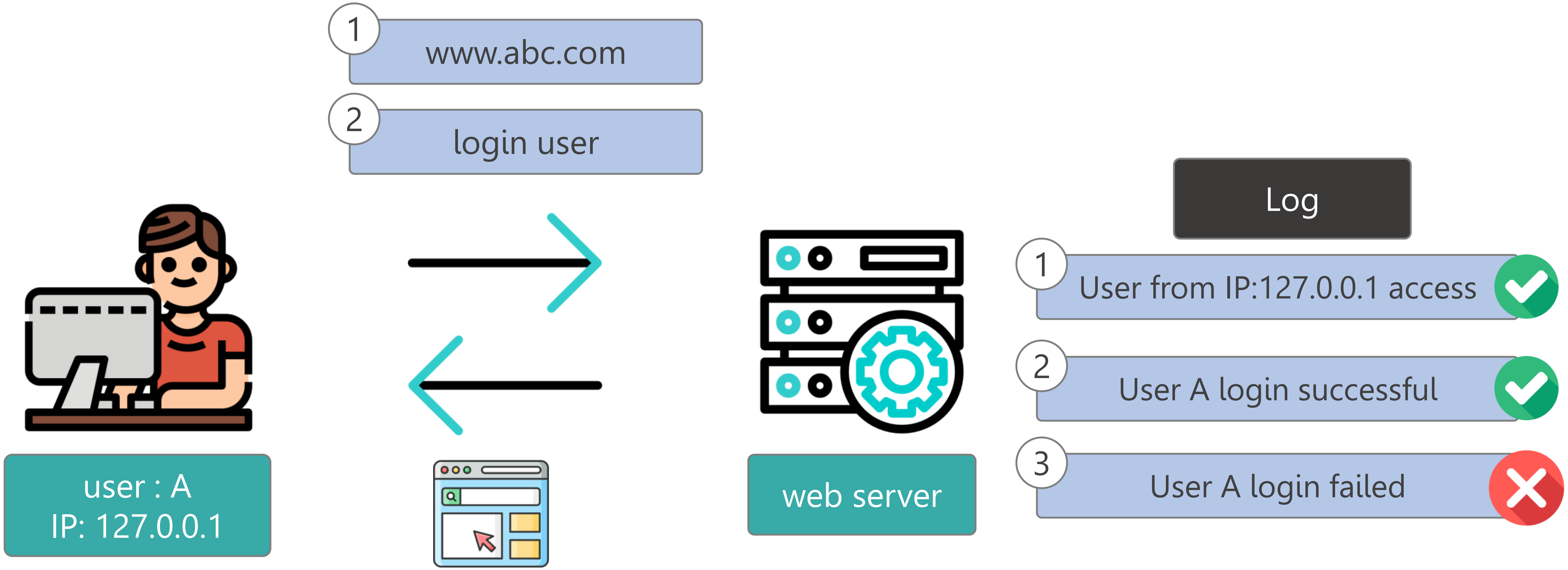
- What is Security Monitoring Technology?
- Security Monitoring Technology
  - SIEM
  - IDS
  - Log Management Tools
  - Vulnerability Scanners
  - Threat Intelligence Tools
  - Network Traffic Analysis
  - Security Compliance Tools
  - Endpoint Detection Tools

04

Security information and event management (SIEM)

04 Security information and event management (SIEM)

Introduction



1 www.abc.com

2 login user

user : A
IP: 127.0.0.1

web server

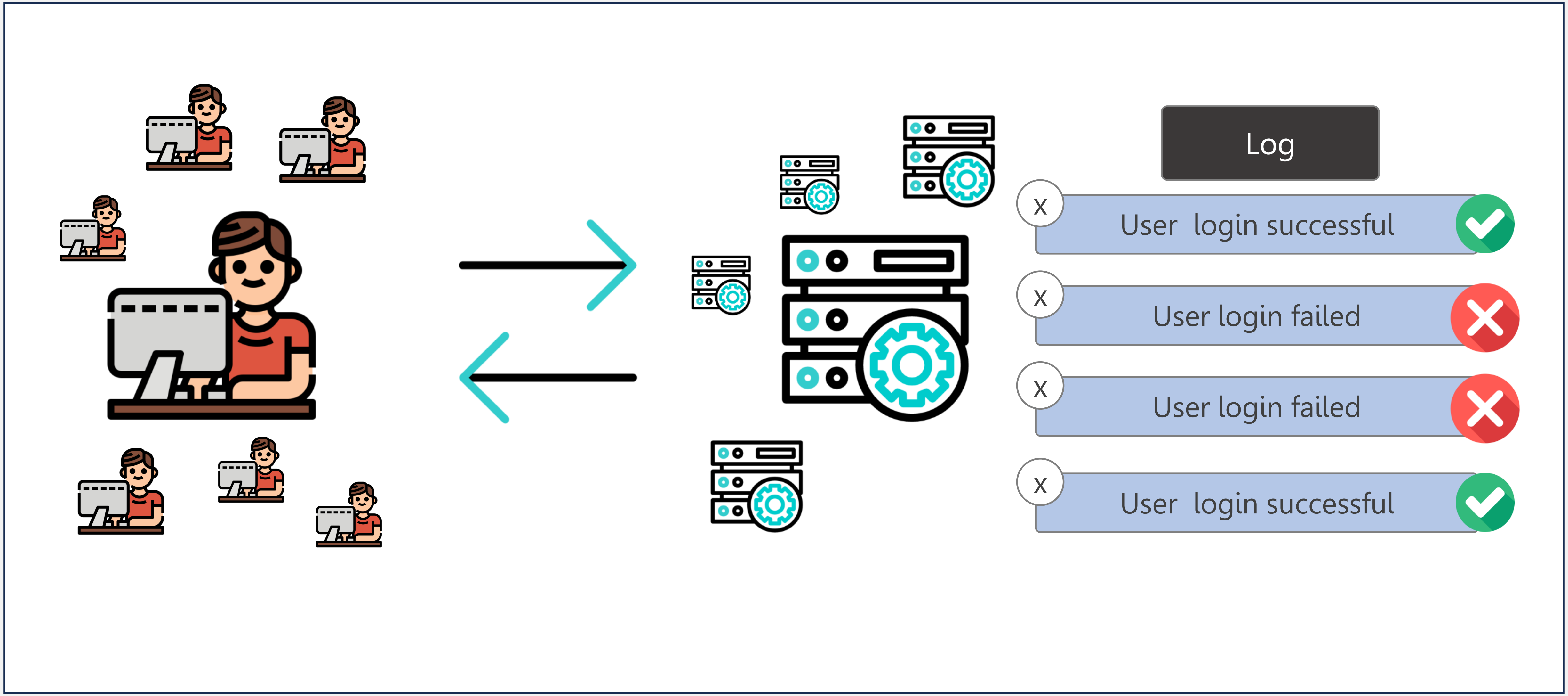
Log

1 User from IP:127.0.0.1 access ✓

2 User A login successful ✓

3 User A login failed ✗

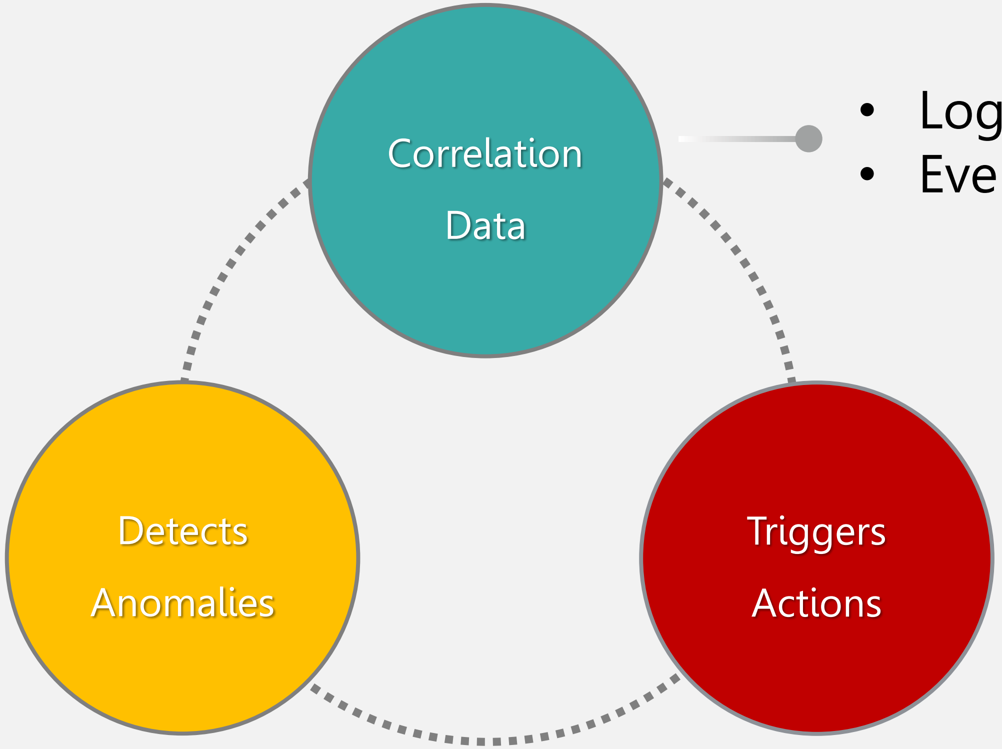
Introduction



What is SIEM?

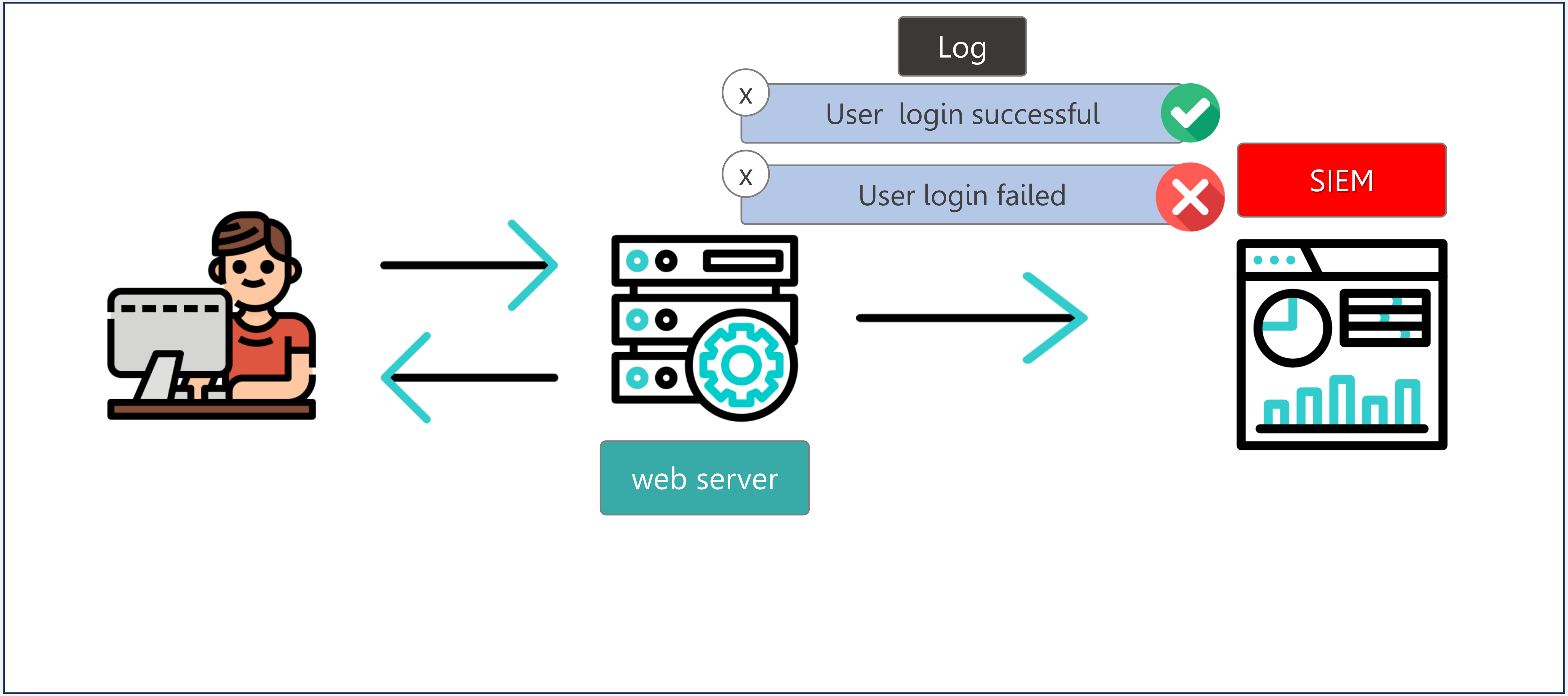
Security Information and Event Management (SIEM)

Security Information Management (SIM) + Security Event Management (SEM)



- Log
- Event

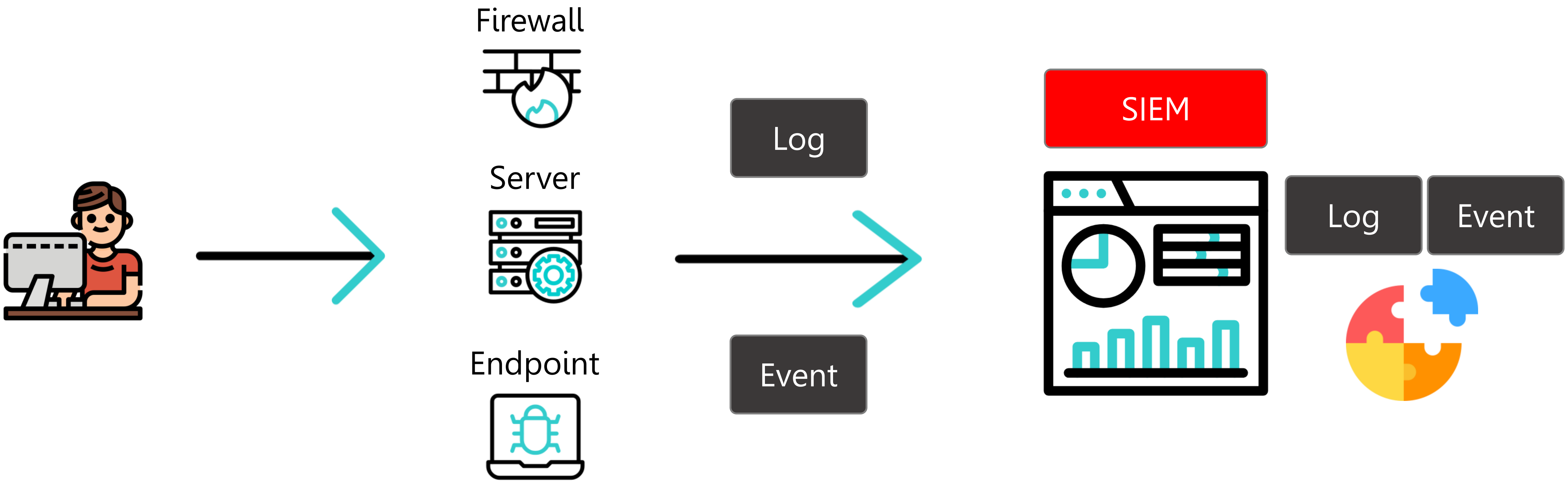
What is SIEM?


Log
x User login successful ✓
x User login failed ✗
SIEM
web server

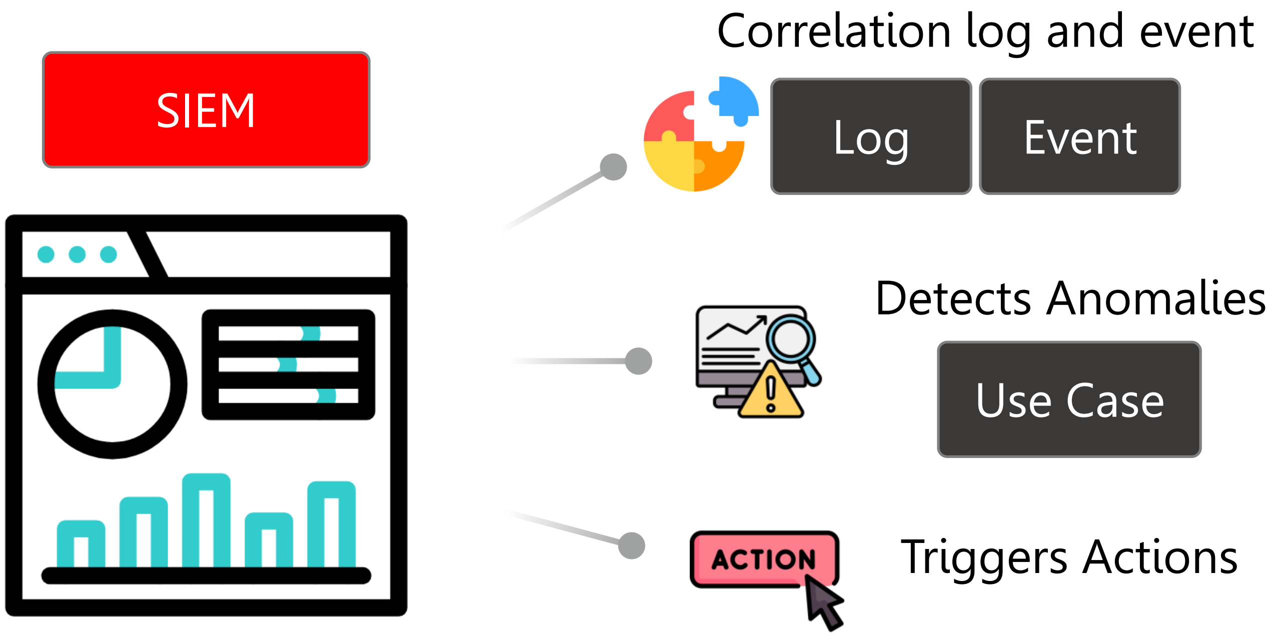
SIEM collected with log type

- Operating System (OS)
  - Microsoft Windows, Linux, MacOS
- Endpoint
- Firewall
- Network

How does SIEM work?



How does SIEM work?



SIEM

Correlation log and event

Log

Event

Detects Anomalies

Use Case

Triggers Actions

Correlation log and event

- Server
  - 01/01/24 - 09:00 User A access server IP: 192.168.1.1 from IP: 127.0.0.1
- Firewall
  - 01/01/24 - 09:00 IP: 192.168.1.1 Port 80 allow from IP: 127.0.0.1

Result

- 01/01/24 - 09:00
  - **User A** access server **IP: 192.168.1.1 Port 80** from **IP: 127.0.0.1** and firewall action **allow**

Use Case

Use Case is set to identify a specific threat scenario from correlation data

Component of Use Case

- Rules : which detect and trigger alerts based on targeted events
- Logic : which defines how events or rules will be considered
- Action : which determines what action is required if logic or conditions are met

Use Case

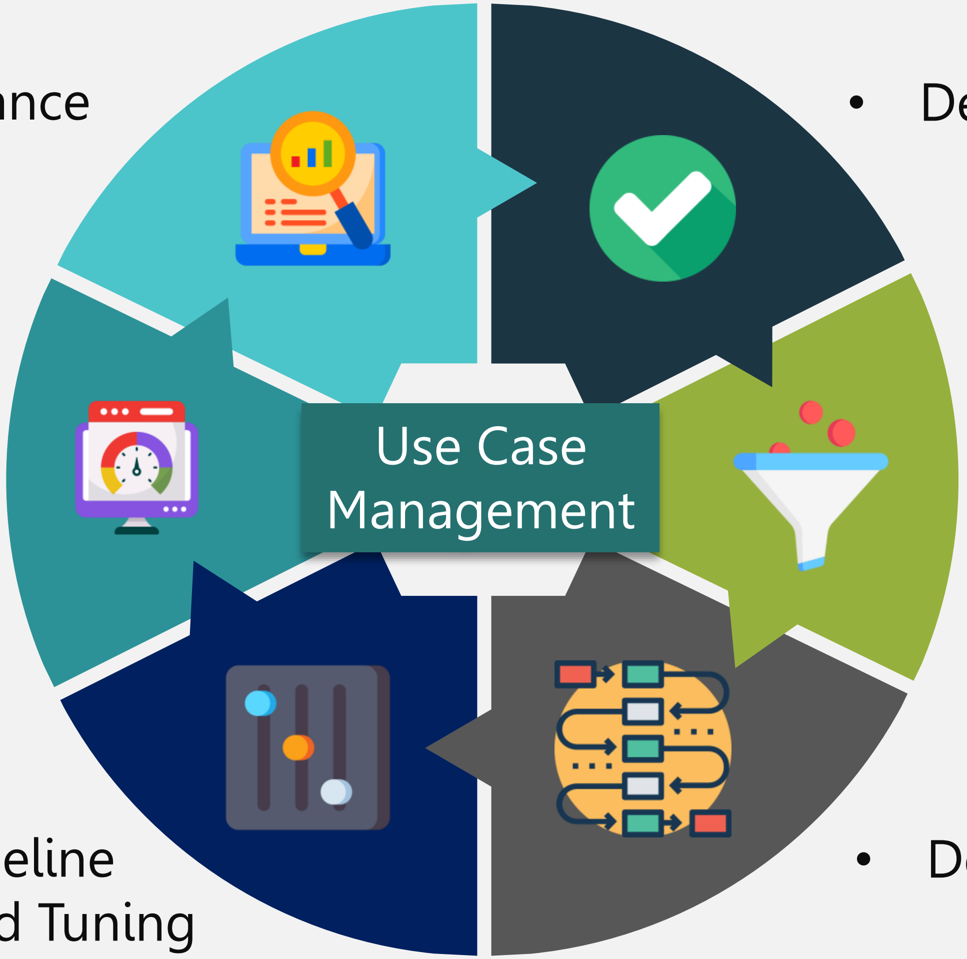
Correlation Data

- 01/01/24 - 09:00
  - **User A** access server **IP: 192.168.1.1 Port 80** from **IP: 127.0.0.1** and firewall action **allow**

Example Use Case

- Rule : firewall action deny
- Logic : deny 10 times in 10 seconds
- Action : disable account / block source IP

Use Case Management



- Monitoring Performance
- Define/Review Requirements
- Optimize Based on Outcome
- Identify Data Source
- On-/Off-board Data Source
- Define Baseline
- Testing and Tuning
- Design/Review Logic

SIEM features and capabilities

- Correlation data
- Dashboard
- Alerting
- Automation

The benefits of SIEM

- Real-time threat recognition
- AI-driven automation
- Improved organizational efficiency
- Detecting advanced and unknown threats
- Monitoring users and applications

SIEM implementation

- Set understandable goals
- Apply data correlation rules
- Asset list
- Record incident response plans and workflows

Key Takeaways

- What is SIEM?
- How does SIEM work?
- SIEM features and capabilities
- The benefits of SIEM
- SIEM implementation

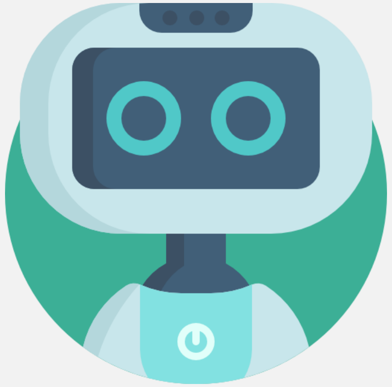
05

Security orchestration automation and response (SOAR)

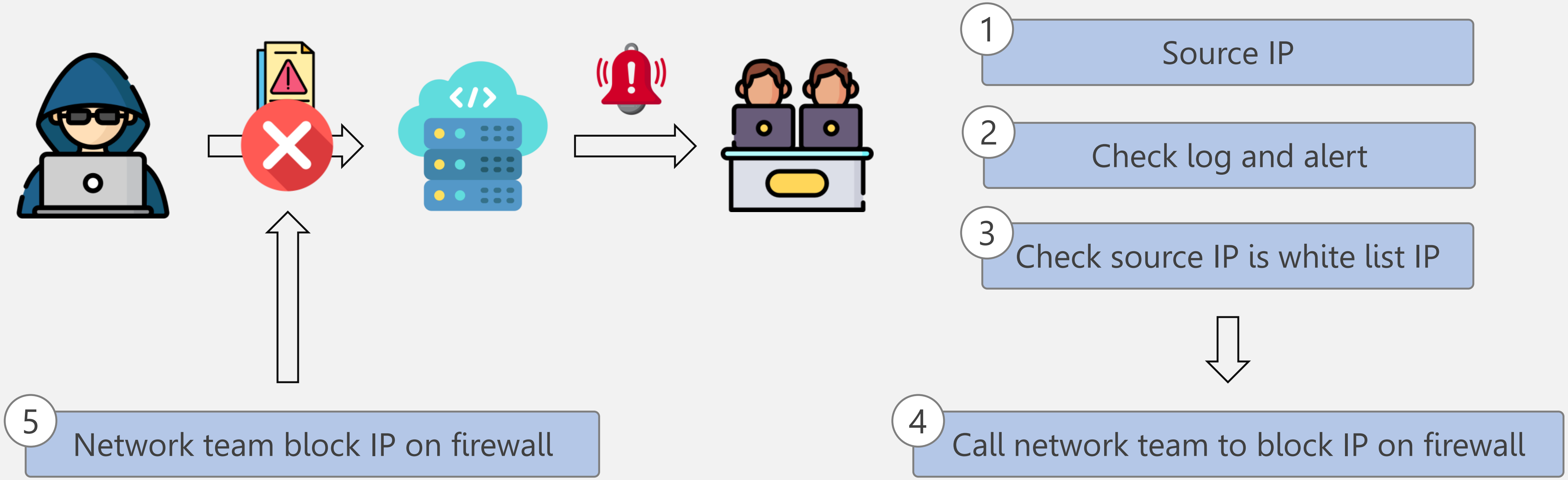
What is SOAR?

Security **O**rchestration **A**utomation and **R**esponse (SOAR) is a software solution that enables security teams to integrate and coordinate separate tools into streamlined threat response workflows.

- Security orchestration
- Security automation
- Incident response

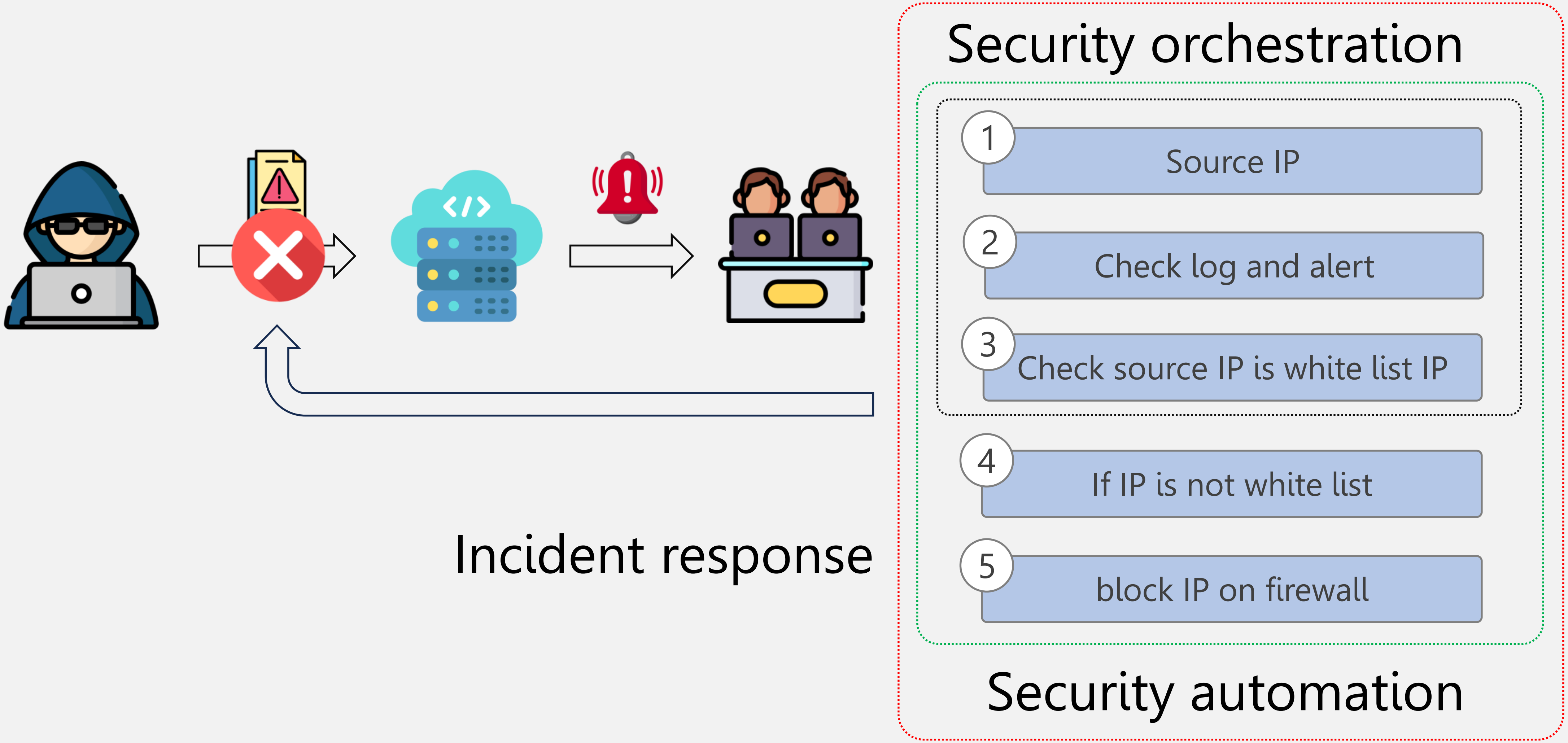


05 Security orchestration automation and response (SOAR)



1. Source IP
2. Check log and alert
3. Check source IP is white list IP
4. Call network team to block IP on firewall
5. Network team block IP on firewall

Security orchestration automation and response (SOAR)



Security orchestration

1. Source IP
2. Check log and alert
3. Check source IP is white list IP
4. If IP is not white list
5. block IP on firewall

Security automation

Incident response

How does SOAR work?

- Playbook
- Integration technology

Playbook is a collection of workflows or tasks and action with step in collection

Integration technology

- Security Device
  - Firewall
  - WAF
- Network
- Identity Management
- ITSM

SOAR features and capabilities

- Automated Incident Response
- Improved Threat Hunting
- Technology and Tools Integration

The benefits of SOAR

- Processing more alerts in less time
- More consistent incident response plans
- Enhanced SOC decision-making
- Improved SOC collaboration

SOAR implementation

- Set understandable goals
- Set incident response
- Define logic for playbook

Key Takeaways

- What is SOAR?
- How does SOAR work?
- SOAR features and capabilities
- The benefits of SOAR
- SOAR implementation

06

User and Entity Behavior Analytics (UEBA)

What is UEBA?

User and entity behavior analytics (UEBA) is a type of security software that uses behavioral analytics, machine learning algorithms and automation to identify abnormal and potentially dangerous user and device behavior

Why UEBA?

User and entity behavior analytics (UEBA) is a cybersecurity solution that uses algorithms and machine learning to detect anomalies in the behavior of not only the users in a corporate network but also the routers, servers, and endpoints in that network

Source type for UEBA

- Network equipment and network access solutions
- Security tools and solutions, such as anti-malware, EDR, intrusion detection and prevention systems
- Authentication databases, such as Active Directory
- Threat intelligence feeds

How does UEBA work?

User behavior analytics collects information from system logs on the normal behavior of users across an organization.

Using machine learning, UBA then analyzes the data, establishes a baseline of user behavior patterns, and detects any irregularities.

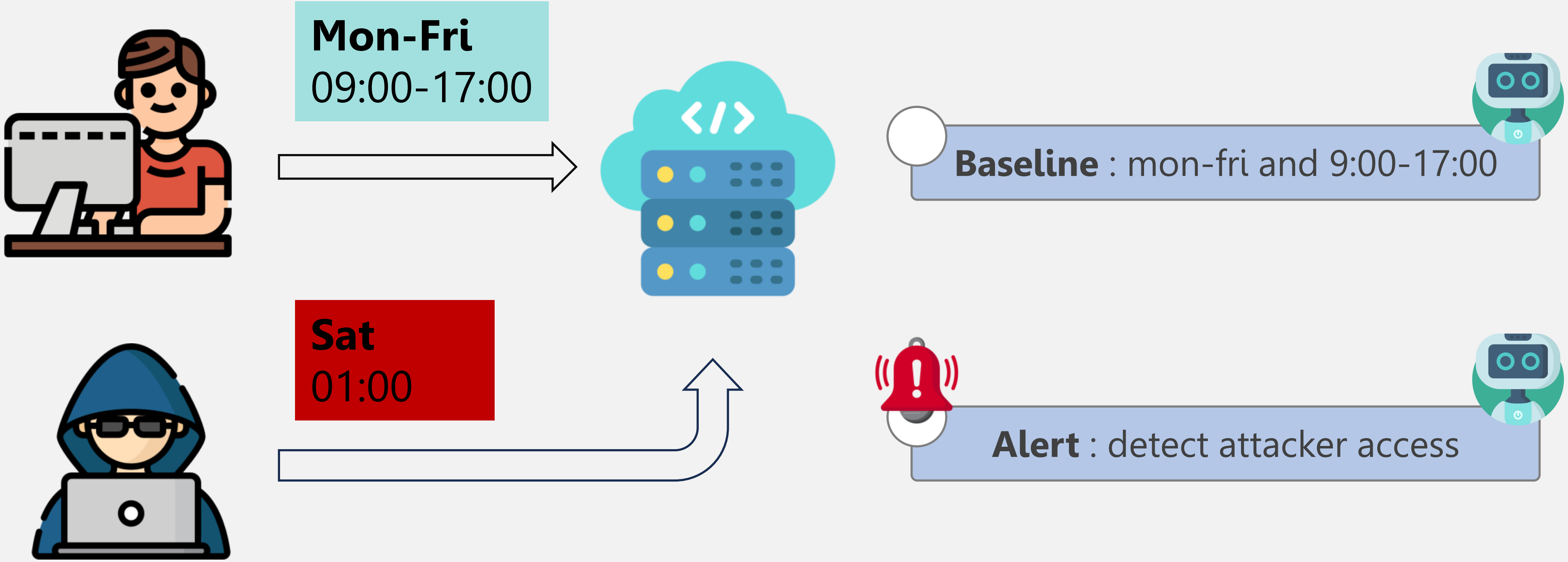
How does UEBA work?

Three pillars of UEBA

- Use cases
- Data sources
- Analytics

06 User and Entity Behavior Analytics (UEBA)

How does UEBA work?



Mon-Fri
09:00-17:00

Sat
01:00

Baseline : mon-fri and 9:00-17:00

Alert : detect attacker access

UEBA Use Case

- Detecting Suspicious User Accounts
- Detecting Suspicious User-Like Entities
- Detecting Insider Threats
- Detecting Suspicious Account Creation Attempts

UEBA features and capabilities

- Machine learning
- Dynamic baseline
- Behavior Analytic

The benefits of UEBA

- Detect breach of protected data
- Detect insider threats
- Reduce false positives

UEBA implementation

- Set understandable goals
- Consider data sources
- Define use case

Key Takeaways

- What is UEBA?
- Why UEBA?
- How does UEBA work?
- UEBA Use Case
- UEBA features and capabilities
- The benefits of UEBA
- UEBA implementation

07

Threat Intelligence

What is Threat Intelligence?

Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor’s motives, targets, and attack behaviors. Threat intelligence enables to make faster and more informed.

How does Threat Intelligence work?

Threat intelligence feed is a stream of data about potential attacks

- Tactics, techniques, and procedures (TTP)
- Malware signatures
- Indicators of compromise (IoC)
- Suspicious IP addresses and domains

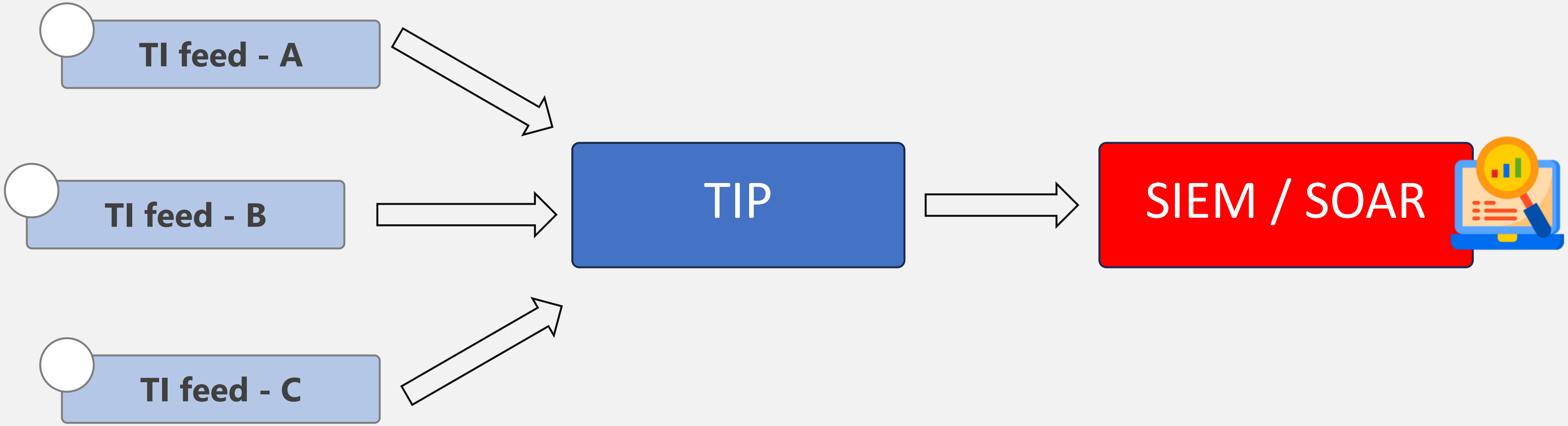
What is Threat Intelligence Platform?

Threat intelligence platform (TIP) is software or a set of tools you can use to collect, analyze and manage data about potential cyber threats.

How does Threat Intelligence Platform work?

Threat intelligence feeds are a common source of information for most threat intelligence platforms

How does Threat Intelligence Platform work?



Stages Of Threat Intelligence

- Collection
- Processing
- Analysis
- Dissemination
- Use

07 Threat Intelligence Platform (TIP)

TIP features and capabilities

- A user interface
- Tools for collecting and processing data
- Feeds and application programming interfaces (APIs)
- Reporting tools
- The possibility of integration with other security tools
- Tools for scoring the threat risks

The benefits of TIP

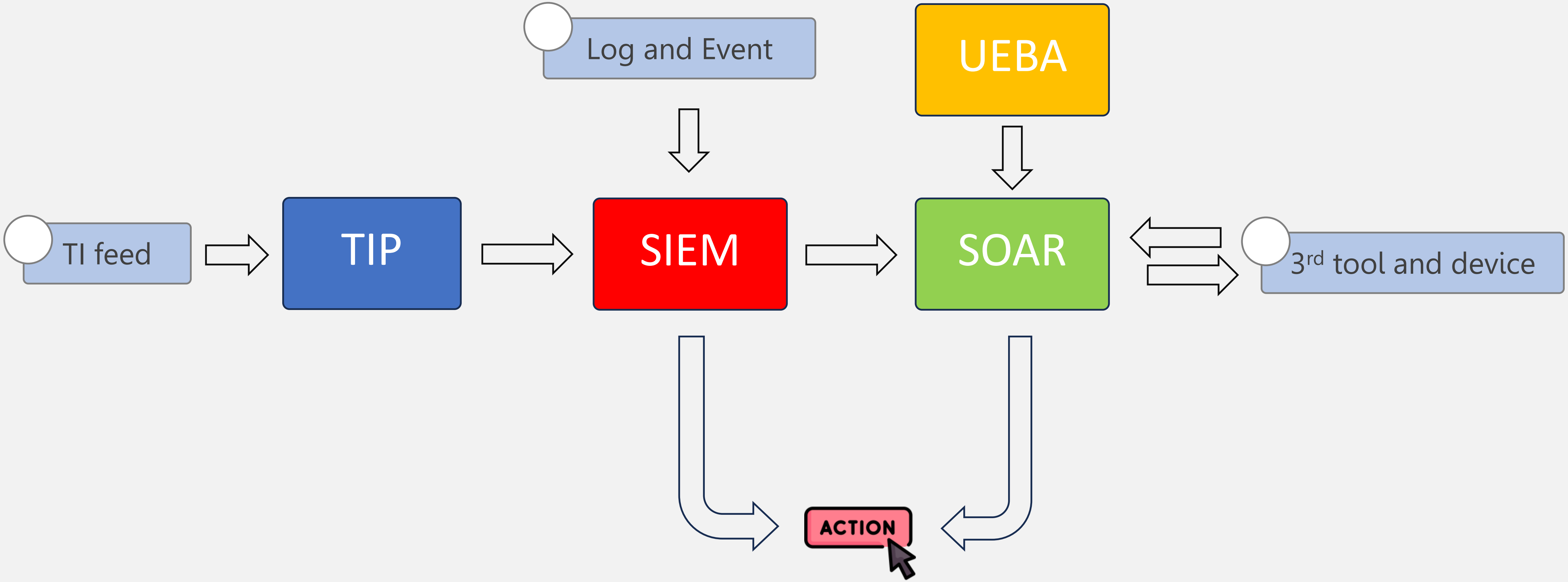
- Improved protection
- Streamlined security operations
- Increased awareness about cyber threats

Key Takeaways

- What is Threat Intelligence?
- How does Threat Intelligence work?
- What is Threat Intelligence Platform?
- How does Threat Intelligence Platform work?
- TIP features and capabilities
- The benefits of TIP

08 Technology Integrations

Technology Integrations



Key Takeaways

- How to implement technology integrations

09

Incident Response

Security Incident Response

Event

- A measurable change in state

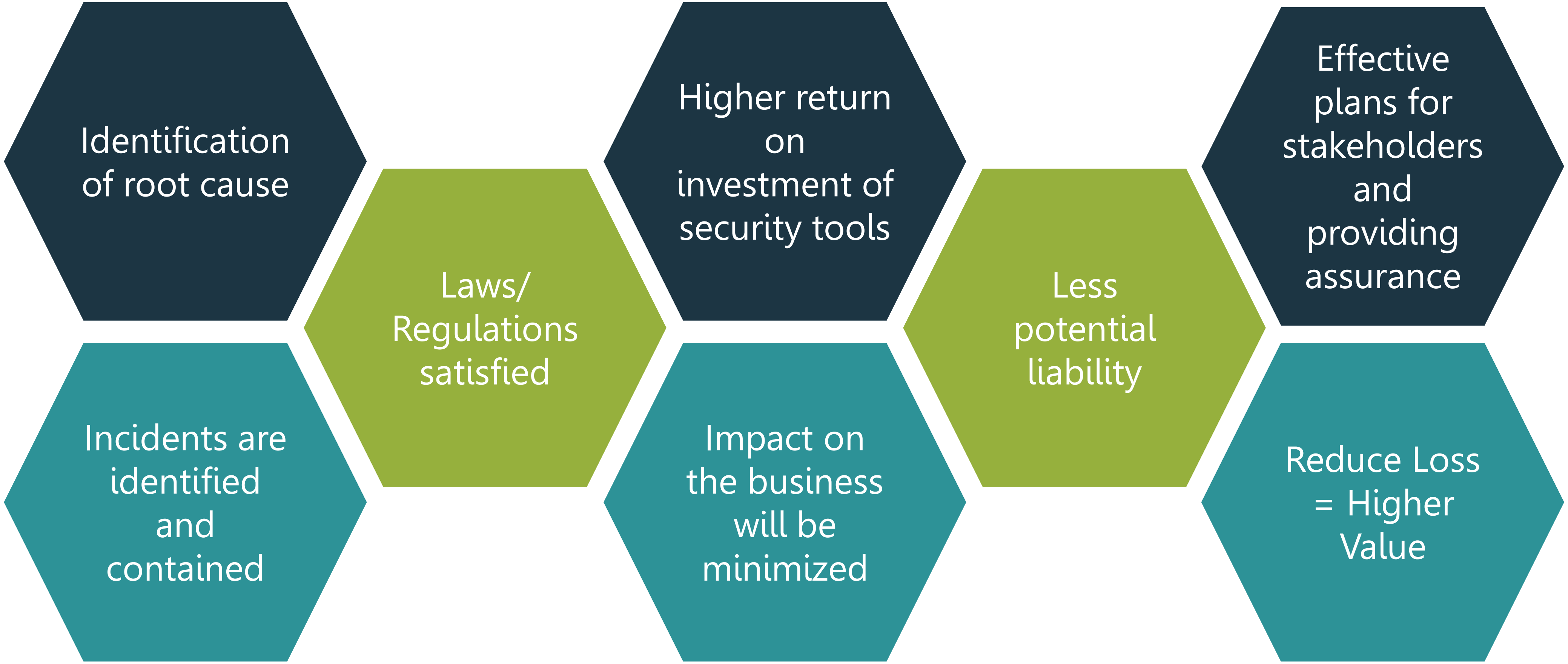
Incident

- Event that has a negative impact on the company
- Incident response focuses on containing the damage of an attack and restoring normal operations

Incident Response

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

Value to the Business



Identification of root cause

Incidents are identified and contained

Laws/ Regulations satisfied

Higher return on investment of security tools

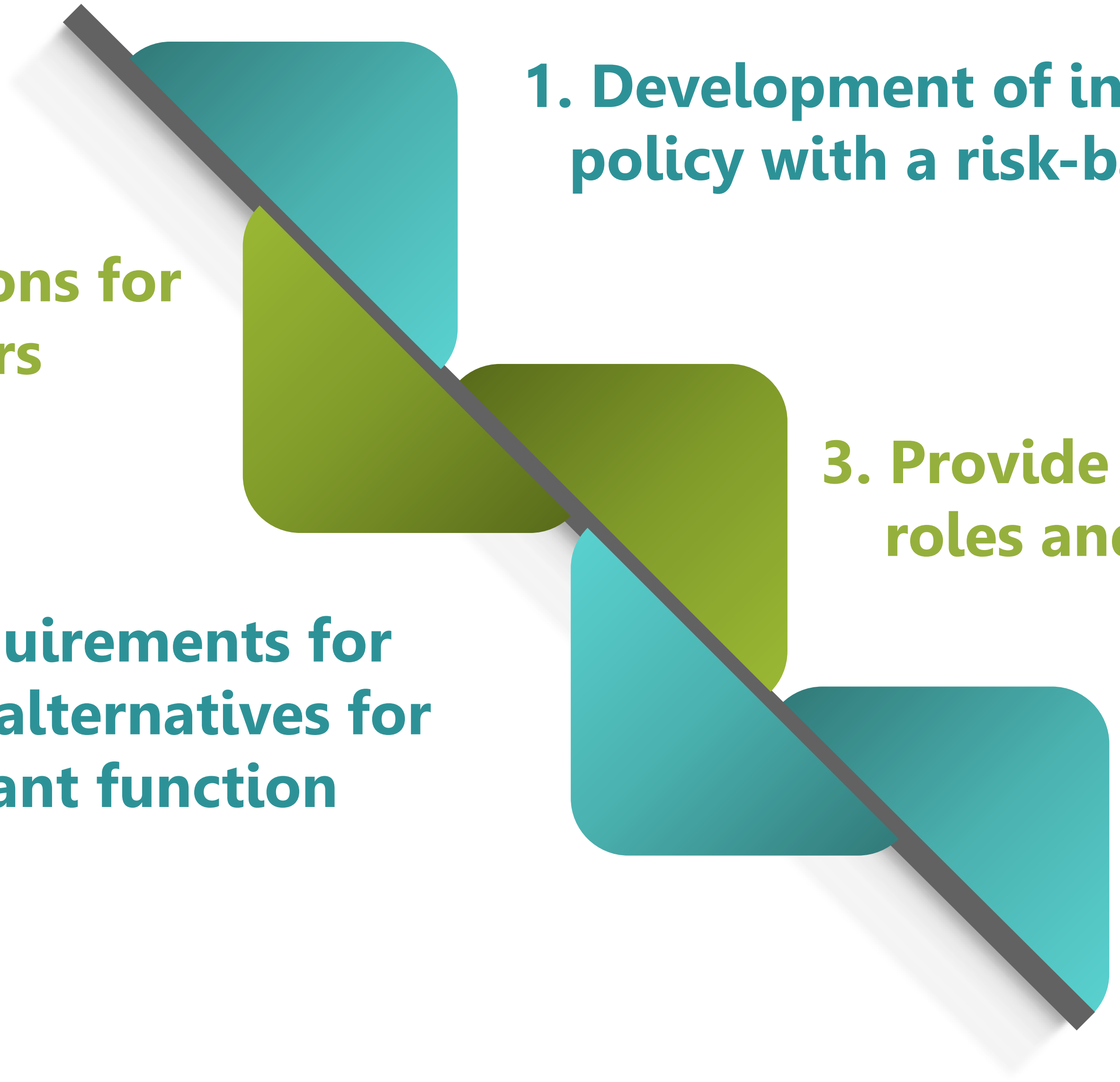
Impact on the business will be minimized

Less potential liability

Effective plans for stakeholders and providing assurance

Reduce Loss = Higher Value

How to build Incident Response (1/2)



1. Development of incident management policy with a risk-based methodology

2. Set expectations for stakeholders

3. Provide documentation for roles and responsibilities

4. Set requirements for identified alternatives for important function

5. Development of incident management and response plans

How to build Incident Response (2/2)

6. Handling and coordinating incident response activity

7. Maintain the consistency and reliability of service

8. Verifying, validating and reporting of countermeasures

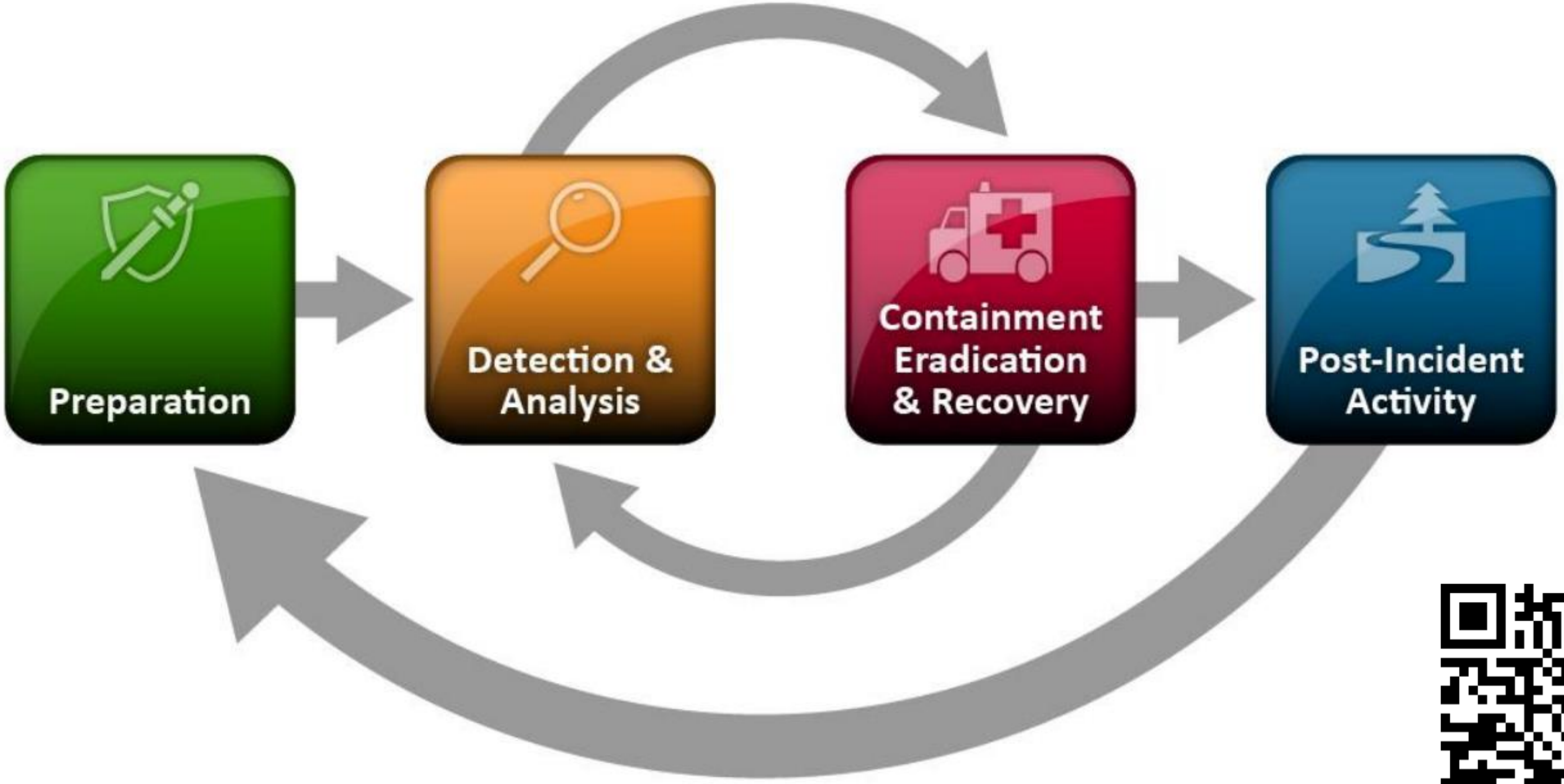
9. Planning, budgeting and program development for all matters related to incident management

10. Regular review and update incident response align new threat

Incident Response Plan

Incident Response Life Cycle

KBTG
KASIKORN
BUSINESS-TECHNOLOGY GROUP



https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Preparation

Preparation phase involves various activities aimed at ensuring the organization is adequately prepared to effectively respond to and manage security incidents

1. Establishment of Incident Response Team
2. Define Roles and Responsibilities
3. Development of Incident Response Plan (IRP)
4. Identification of Critical Assets and Data
5. Risk Assessment and Threat Intelligence
6. Implementation of Security Controls
7. Establishment of Communication Channels
8. Training and Awareness
9. Testing and Exercises
10. Documentation and Documentation

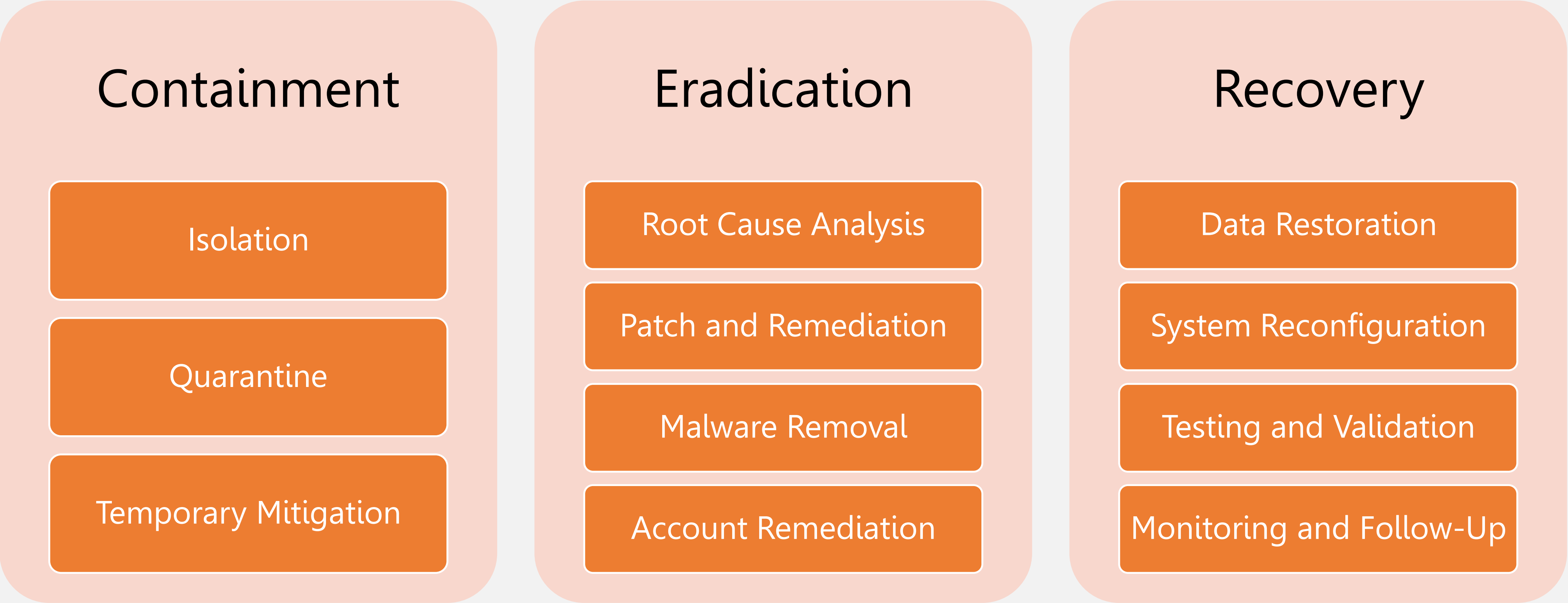
Detection and Analysis

Detection and Analysis phase involves the identification, investigation, and assessment of potential security incidents. This phase is crucial for promptly recognizing unauthorized access, malicious activities, or anomalies in the organization's IT infrastructure

1. Event Monitoring
2. Alert Triage
3. Incident Identification
4. Incident Classification
5. Root Cause Analysis
6. Evidence Collection
7. Impact Assessment
8. Reporting

Containment, Eradication, and Recovery

the phase of **Containment, Eradication, and Recovery** focuses on mitigating the impact of the incident, eliminating the root cause, and restoring affected systems and data to normal operation. This phase involves a series of coordinated actions to contain the incident, eradicate any malicious presence, and recover affected assets



Containment

- Isolation
- Quarantine
- Temporary Mitigation

Eradication

- Root Cause Analysis
- Patch and Remediation
- Malware Removal
- Account Remediation

Recovery

- Data Restoration
- System Reconfiguration
- Testing and Validation
- Monitoring and Follow-Up

Post Incident Activities

Post-Incident Activities phase involves activities and processes conducted after the resolution of a security incident. These activities are critical for learning from the incident, improving the organization's security posture, and minimizing the likelihood of similar incidents in the future

- Incident Debriefing
- Post-Mortem Analysis
- Documentation and Reporting
- Communication and Notification
- Continuous Improvement
- Training and Awareness

Key Takeaways

1. Definition of Event and Incident are different
2. 4 Steps of Incident Response Plan (NIST SP800-61r2)
    1. Preparation
    2. Detection and Analysis
    3. Containment, Eradication, and Recovery
    4. Post-incident Activities

10

Security Operation Center (SOC)

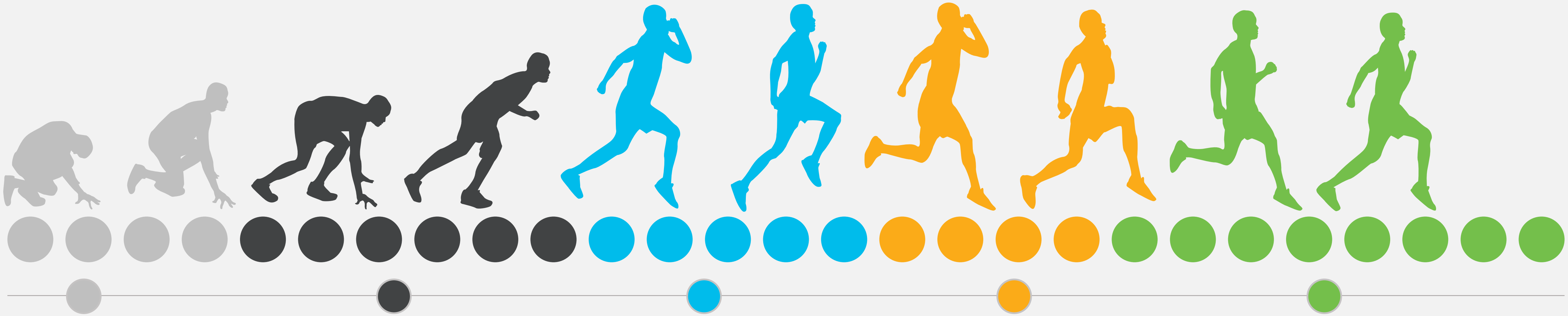
Security Operation Center

A Security Operations Center (SOC) is a centralized facility or team responsible for monitoring, detecting, analyzing, and responding to cybersecurity threats and incidents within an organization. The primary goal of a SOC is to protect the organization's systems, networks, data, and assets from security breaches and unauthorized access.

Key function

- Monitoring and Detection
- Incident Response
- Threat Intelligence and Analysis
- Vulnerability Management
- Security Incident Management
- Forensic Analysis
- Continuous Monitoring and Improvement

Security Operation Center Journey



PLAN

A solid model for the SOC with clear services and maturity roadmaps to drive successful execution.

BUILD

Successful build an integrated SOC and migrate from the previous limited deployment.

OPERATE

Achieve Go-Live requirements and start operating the SOC services with continuous improvement in mind.

EXPAND

Successfully onboarded the tenants into SOC. Good response from them about the service and the experience.

EXCEL

Safeguards the organization from cyber threats but also contributes to regulatory compliance, customer trust, and overall business resilience.

11

Forensic Investigation

KBTG
KASIKORN BUSINESS-TECHNOLOGY GROUP

Forensic Investigation

The process of collecting, analyzing, and interpreting digital evidence to reconstruct past events or activities related to computer systems, networks, and electronic devices. The primary goal of forensic investigation is to uncover evidence that can be used in legal proceedings, such as criminal investigations, civil litigation, or internal disciplinary actions.

EVIDENCE COLLECTION

ANALYSIS AND EXAMINATION

TIMELINE RECONSTRUCTION

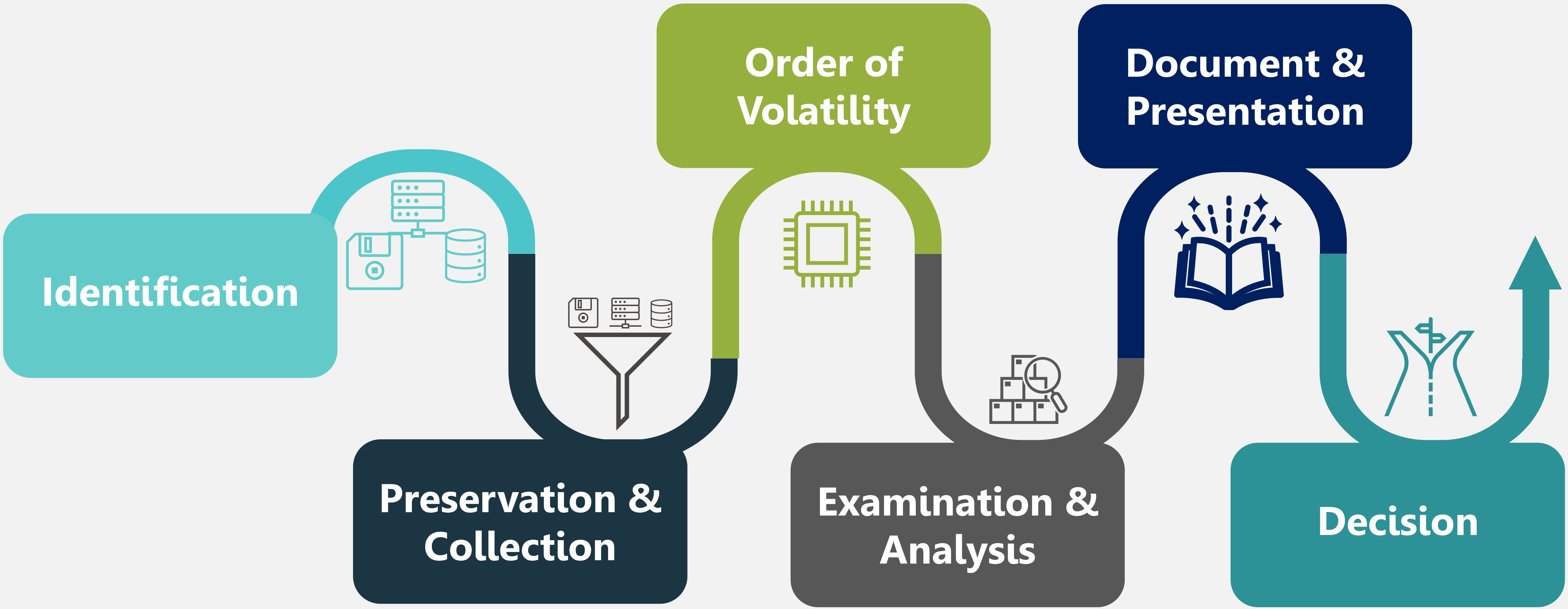
ARTIFACT ANALYSIS

MALWARE ANALYSIS

REPORTING AND DOCUMENTATION

EXPERT TESTIMONY

Forensics Investigation Process



Identification

Preservation & Collection

Order of Volatility

Examination & Analysis

Document & Presentation

Decision

Chain of Custody

Key Takeaways

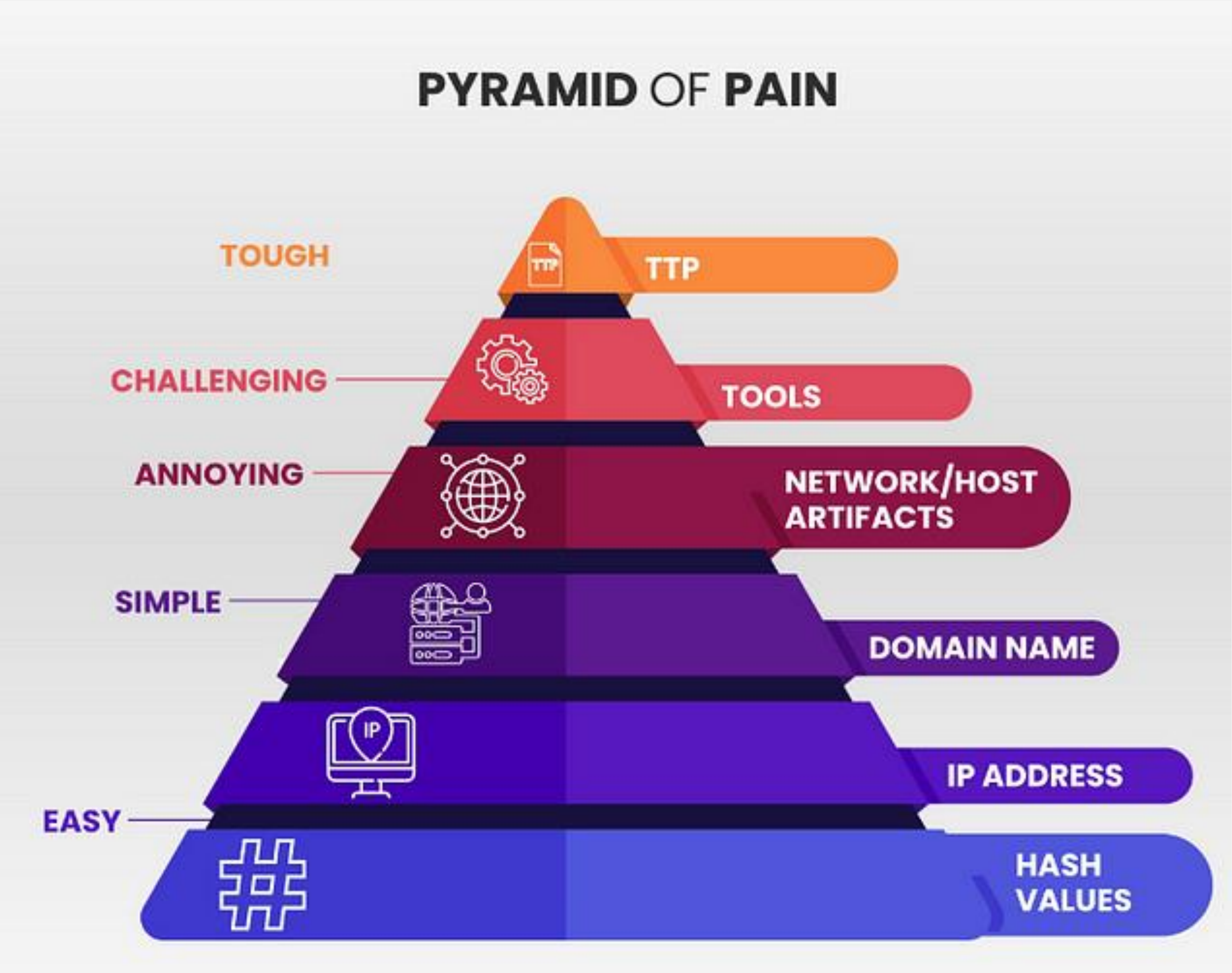
1. Forensic Investigation is a process
2. There are 6 steps
   - Identification
   - Preservation and Collection
   - Order of Volatility
   - Examination & Analysis
   - Document & Presentation
   - Decision
3. Chain of Custody

12

MITRE ATT&CK

IOC* and Pyramid of Pain

"This simple diagram shows the relationship between the types of indicators you might use to detect an adversary's activities and how much pain it will cause them when you are able to deny those indicators to them."



David Bianco, a **cybersecurity** and threat hunting expert, created the **Pyramid of Pain** in 2013

*IOC = Indicator of Compromise

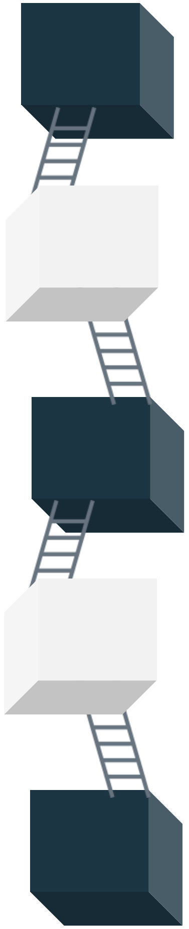
MITRE ATT&CK

Adversarial Tactics, Techniques, and Common Knowledge,

is a globally accessible knowledge base maintained by the MITRE Corporation. It is a comprehensive framework that provides a curated list of tactics, techniques, and procedures (TTPs) used by adversaries during cyber attacks.

MITRE ATT&CK

Key Components



01 Tactics

High-level categories representing the goals or objectives of an attacker. These tactics are derived from the Cyber Kill Chain

02 Techniques

Specific methods or procedures that adversaries use to achieve their tactical objectives

03 Sub-techniques

Sub-techniques represent specific variations or implementations of a technique and help capture the diversity of attacker behavior within each tactic

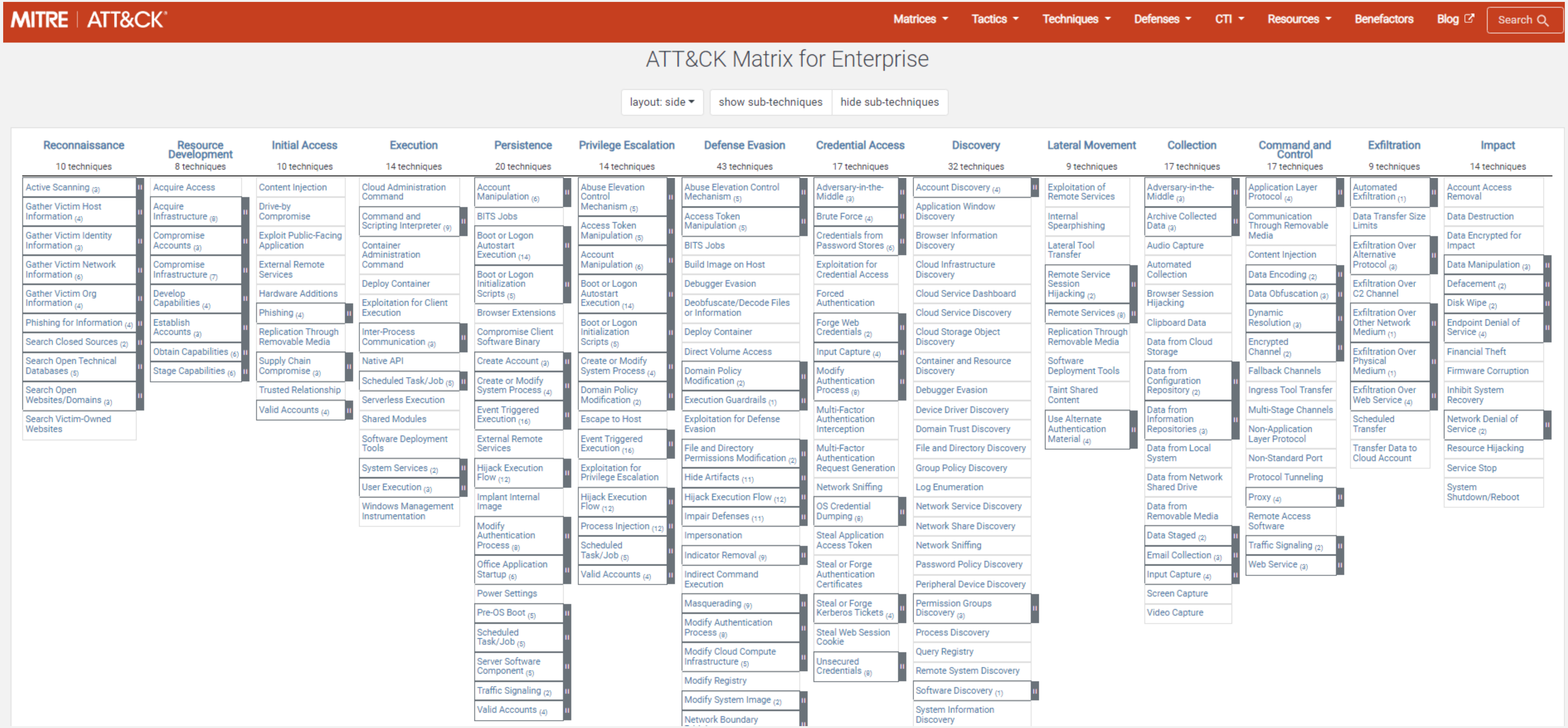
04 Mitigations

Countermeasures and defensive strategies that organizations can implement to defend against specific techniques and tactics

05 Groups and Software

Profiles of threat actor groups and specific malware or tools associated with observed adversary behavior

MITRE ATT&CK



ATT&CK Matrix for Enterprise

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Escape to Host	Direct Volume Access	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Ingress Tool Transfer	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Multi-Stage Channels		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service (2)
			System Services (2)	Implant Internal Image	Process Injection (12)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Standard Port		Resource Hijacking
			User Execution (3)	Modify Authentication Process (8)	Scheduled Task/Job (5)	Hide Artifacts (11)	Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Office Application Startup (6)	Valid Accounts (4)	Hijack Execution Flow (12)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (3)	Proxy (4)		System Shutdown/Reboot
				Power Settings		Impair Defenses (11)	Steal or Forge Kerberos Tickets (4)	Network Service Discovery		Input Capture (4)	Remote Access Software		
				Pre-OS Boot (5)		Impersonation	Steal Web Session Cookie	Network Share Discovery		Screen Capture	Traffic Signaling (2)		
				Scheduled Task/Job (5)		Indicator Removal (9)	Unsecured Credentials (8)	Network Sniffing		Video Capture	Web Service (3)		
				Server Software Component (5)		Indirect Command Execution		Password Policy Discovery					
				Traffic Signaling (2)		Masquerading (9)		Peripheral Device Discovery					
				Valid Accounts (4)		Modify Authentication Process (8)		Permission Groups Discovery (3)					
						Modify Cloud Compute Infrastructure (5)		Process Discovery					
						Modify Registry		Query Registry					
						Modify System Image (2)		Remote System Discovery					
						Network Boundary		Software Discovery (1)					
								System Information Discovery					

Pros and Cons

Pros

- Comprehensive understanding of adversarial behavior
- Common language for communication
- Guidance for threat detection and response
- Community collaboration and knowledge sharing
- Baseline and integration with security tools and solutions

Cons

- Complexity tactic, technique, and sub-technique requires time, effort, and expertise, which may present a steep learning curve for some users
- It's essential to approach the framework with a clear understanding of its limitations and context
- Limited budgets or staffing may struggle to fully leverage the framework's benefits

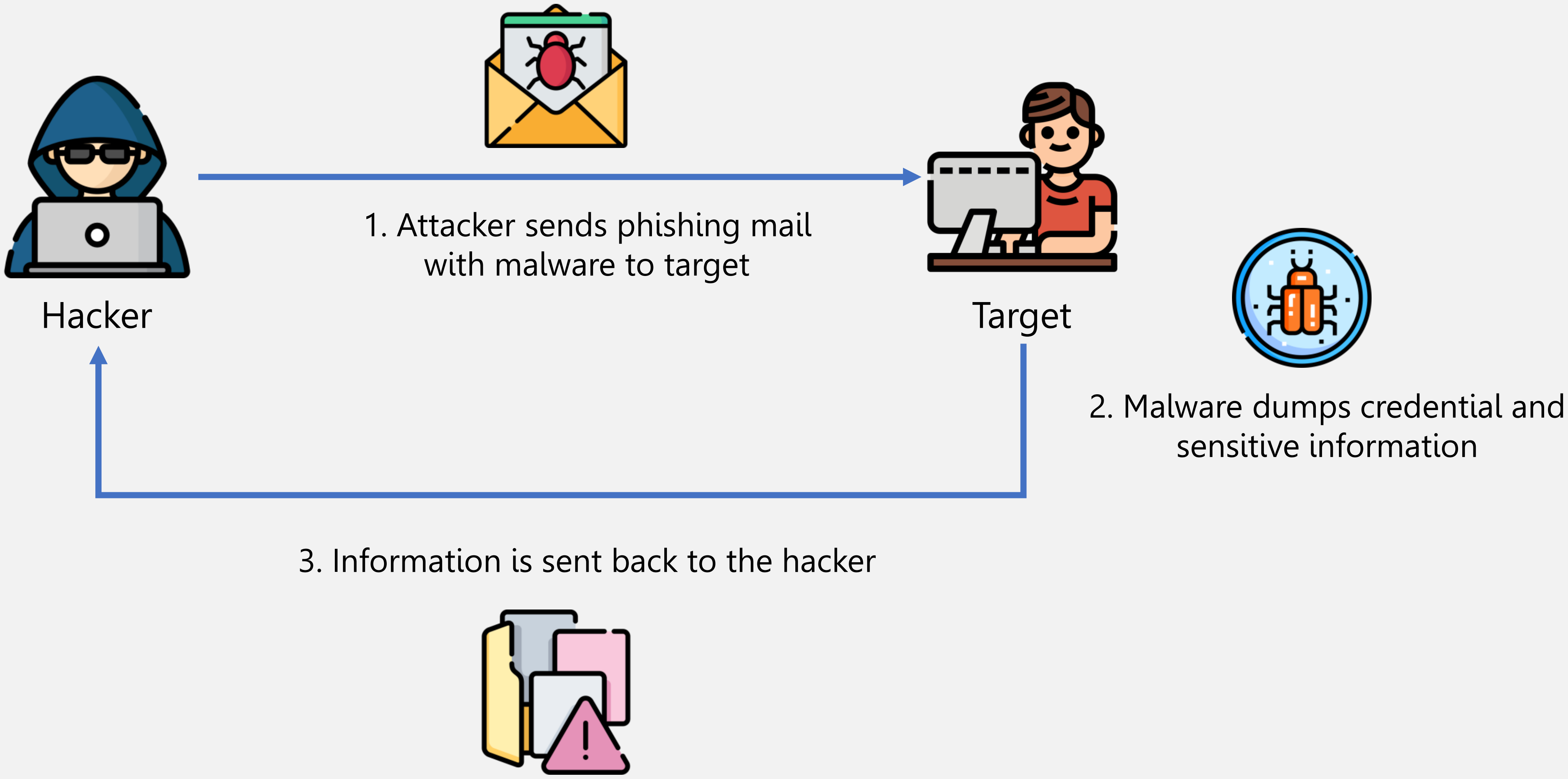
Key Takeaways

1. ATT&CK is the framework for understanding TTP
2. Pyramid of Pain and IOC

13

Case Study

Case study example



Hacker

Target

1. Attacker sends phishing mail with malware to target

2. Malware dumps credential and sensitive information

3. Information is sent back to the hacker

Incident Response Plan

Preparation

- Policy and Procedure
- Monitoring Tools
- Contact point

Detection and Analysis

- Alert from EDR or Anti-malware
- Triage and Classify incident
- Impact analysis from malware and data stolen incident
- Root cause analysis

Containment, Eradication, and Recovery

- Disconnect from network
- Scan by using EDR
- Remover or Re-install OS
- Block all traffic to hacker
- Restore all data

Post-Incident Activity

- Find the actual root cause and gap of protection (PPT)
- Awareness training
- Improve phishing detection mechanism

Forensic Investigation

Identification

- Identify what the attacker takes and leaves
- Identify the responsible party

Preservation and Collection

- Chain of Custody (documented and use Hashing Algo.)
- Minimize handling of evidence
- Keep activity logs
- Capture an image of the system
- Work Fast

Order of Volatility

- CPU Registers
- Cache
- RAM
- Virtual Memory
- Hard drive
- Paper Records

Examination & Analysis

- Signature of malware
- Review all logs
- Any hidden data left
- NOT working on the original image
- Find the root cause, what malicious files installed, what data stolen, and communication channel

Document & Presentation

- Interpreting the result
- Documentation
- Expert Testimony

Decision

- The investigation result
- Suspect
- Corrective Action

MITRE ATT&CK

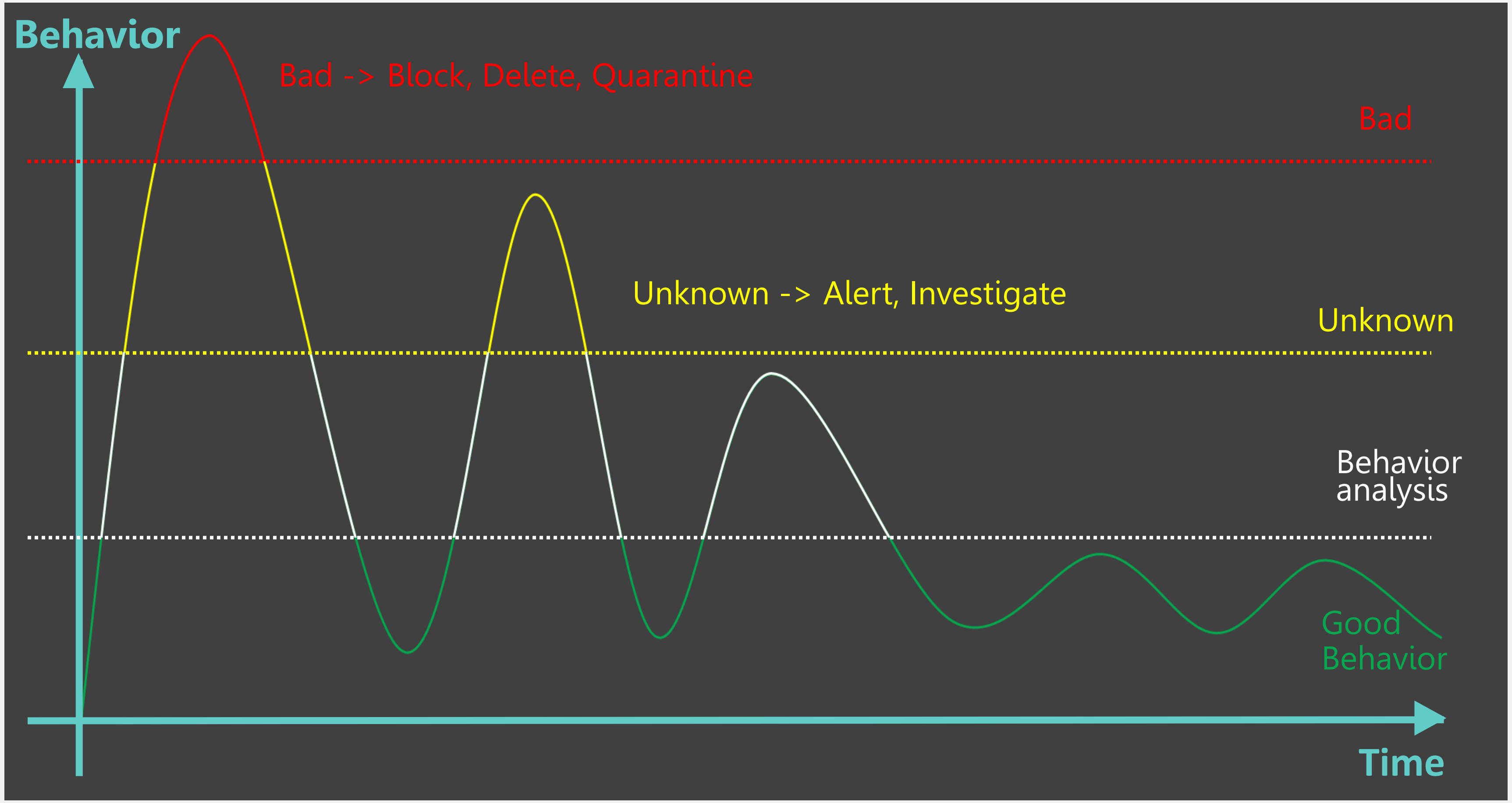
Tactic	Technique	Mitigations
Initial Access (ID: TA0001)	Spearphishing Attachment (ID: T1566.001)	• Antivirus/Antimalware (M1049) • Network Intrusion Prevention (M1031) • Restrict Web-Based Content (M1021) • Software Configuration (M1054) • User Training (M1017)
Execution (ID: TA0002)	User Execution Malicious File (ID: T1204.002)	• Behavior Prevention on Endpoint (M1040) • Execution Prevention (M1038) • User Training (M1017)
Exfiltration (ID: TA0010)	Exfiltration Over Web Service (ID: T1567.003)	• Restrict Web-Based Content (M1021)

14

Threat Hunting

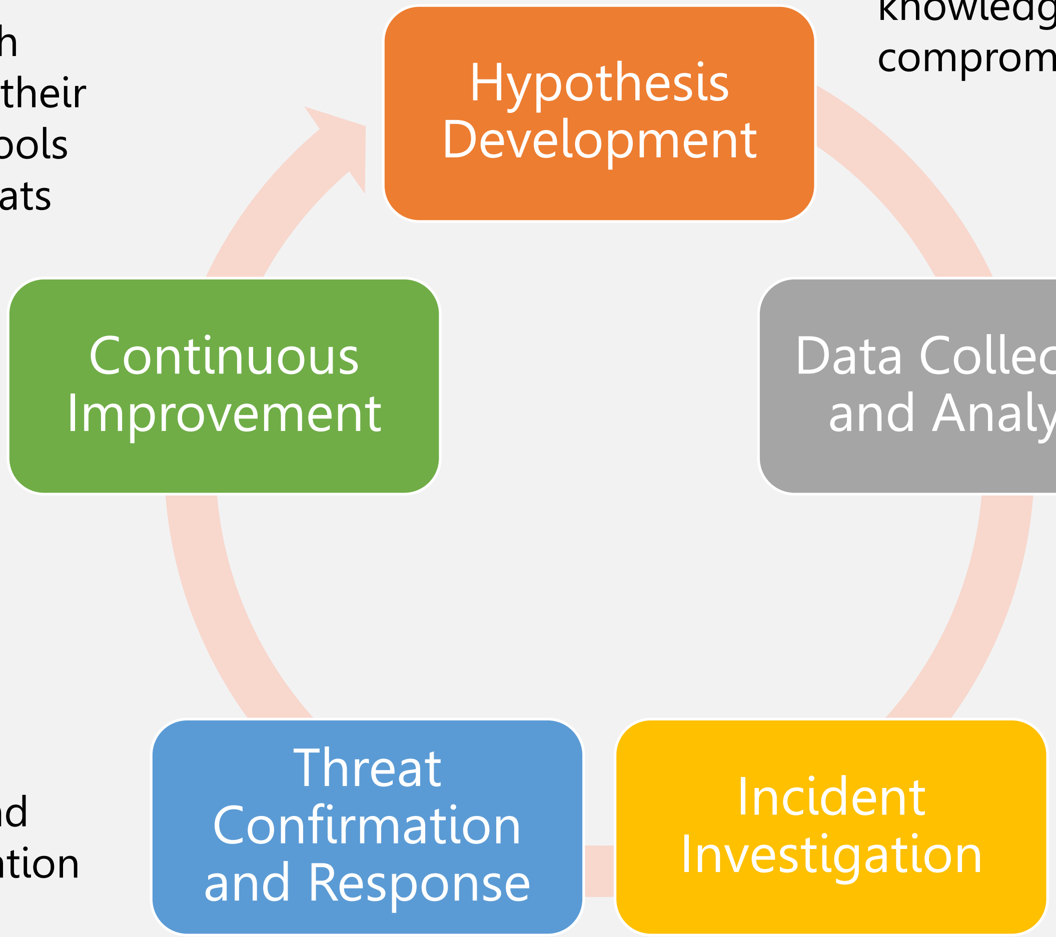
Threat Hunting

Threat hunting is a proactive cybersecurity practice that involves actively searching for and identifying security threats or anomalies within an organization's networks, systems, and endpoints. Threat hunting involves actively seeking out potential threats before they manifest into security incidents or breaches.


Behavior
Bad -> Block, Delete, Quarantine
Bad
Unknown -> Alert, Investigate
Unknown
Behavior analysis
Good Behavior
Time

Increase understanding of the system environment and baseline knowledge of "good" behavior to make detection of anomalies

Threat Hunting Steps



Hypothesis Development

Threat hunters formulate hypotheses based on their knowledge of potential threats, indicators of compromise (IOCs), and attack patterns.

Data Collection and Analysis

Analyze this data using a combination of manual techniques and automated tools to search for anomalies, patterns, or indicators of malicious activity.

Incident Investigation

Conducting forensic analysis and tracing the attacker's movements within the network.

Threat Confirmation and Response

If a threat is confirmed, threat hunters work with incident response teams to develop and implement appropriate mitigation measures.

Continuous Improvement

Threat hunters learn from each hunting expedition, updating their knowledge, techniques, and tools to stay ahead of evolving threats and adversary tactics.

5 Types of Threat Hunting

Hypothesis-Driven Threat Hunting

Tactical Threat Hunting

Strategic Threat Hunting

Adversary-Centric Threat Hunting

Continuous Threat Hunting

Pros and Cons

Pros

- Early detection of threats and proactive defense
- Enhanced visibility and situational awareness
- Customized detection
- Continuous improvement

Cons

- Threat hunting requires a high cost and level of expertise in cybersecurity, threat intelligence, network forensics, and attack techniques
- Threat hunting activities may raise legal and ethical concerns, particularly when it involves accessing and analyzing sensitive data or monitoring employee activities

Key Takeaways

1. Threat hunting is the proactive action to seek the potential threats
2. There are 5 types of Threat hunting

Journey of Incident

THREATS

Assets

- Devices
- Users
- Mailboxes
- Apps

DATA

- Events
- User activity

DETECTIONS

- Sensors
- SIEM
- SOAR

ALERT

- Usecase
- Automated playbooks
- Auto remediation

INCIDENT

- Impacted assets
- Evidence
- Remediation status
- Response actions
- Prevention
- Post incident

Topics key takeaways

Understand the defensive security technology

The Incident Response Plan, Monitoring process, Forensic Investigation, and Threat Hunting

✓ Defensive Security should combine People, Process, and Technology