Strategi dan Kebijakan Manajemen Insiden Siber Pada Organisasi

Jakarta, 30 Oktober 2025

Digit Oktavianto
@digitoktav
https://blueteam.id

Who Am I

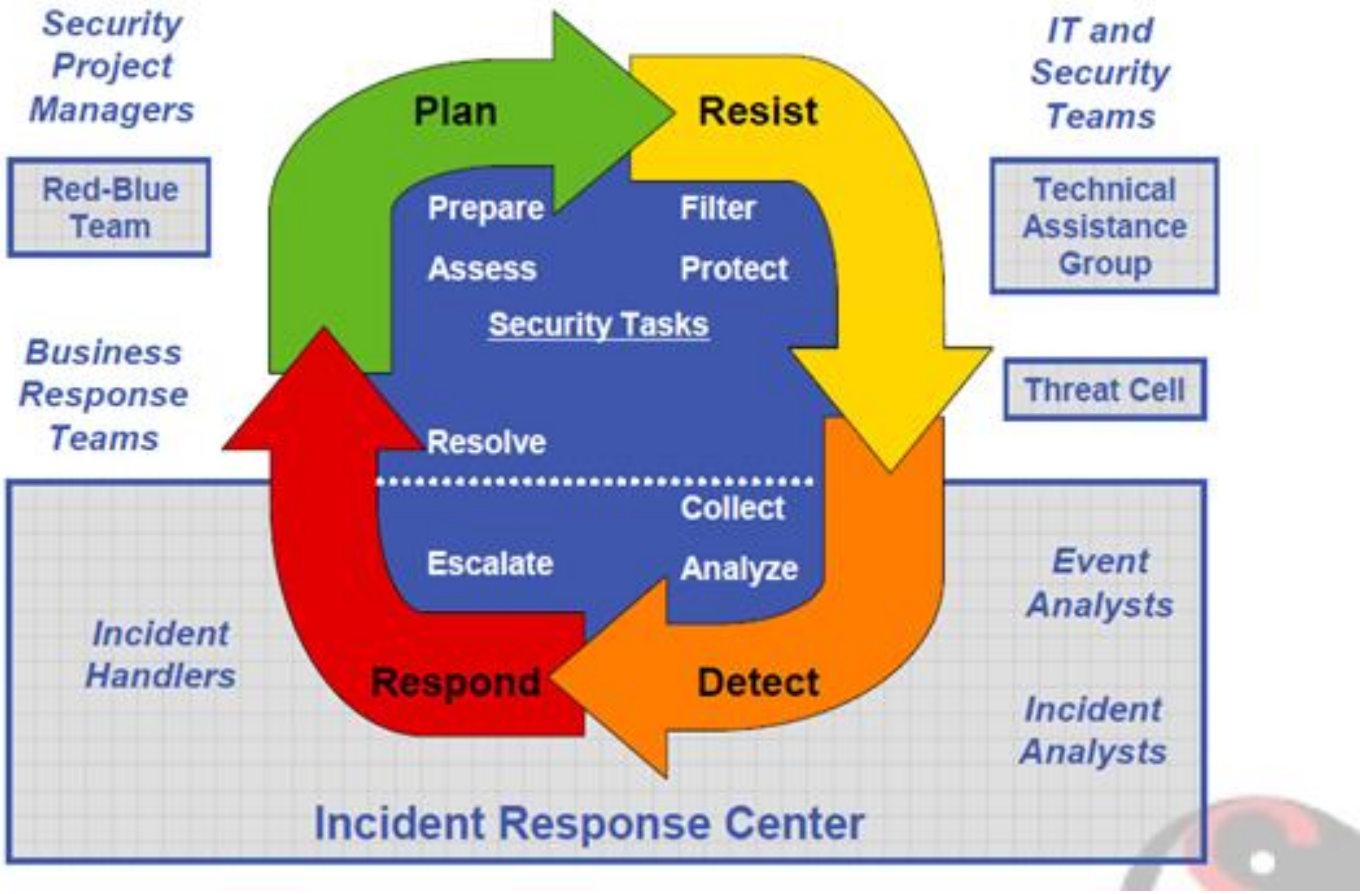
- Division Manager Cyber Security Consulting – FPT Metrodata Indonesia
- Co-Founder BlueTeam.ID (https://blueteam.id)
- Community Lead @ Cyber Defense Community Indonesia (https://cdef.id)
- Cyber Security Training Instructor
- Member of Indonesia Honeynet Project Community
- R&D Division at Asosiasi Forensik Digital Indonesia (AFDI)
- Member of High Tech Crime Investigation Association (HTCIA) APAC
- Opreker and Researcher

Problem Statement of IR

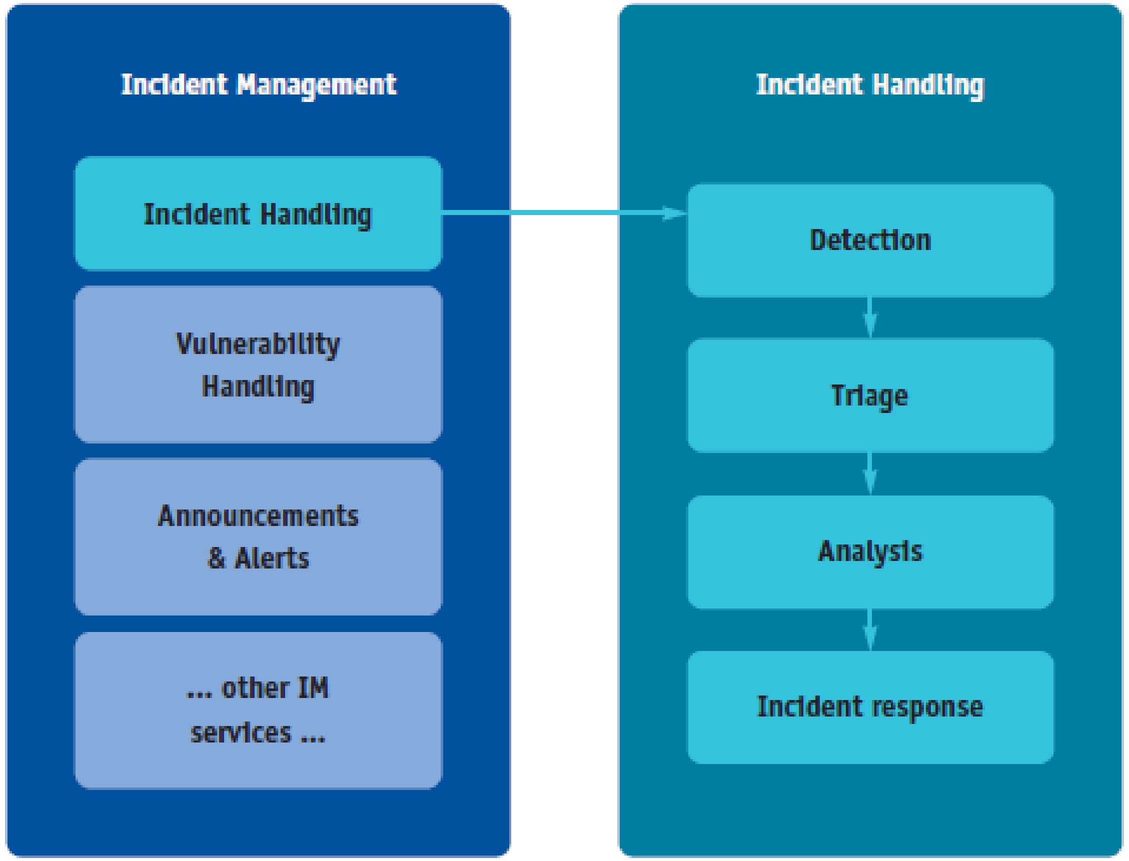
IR memiliki sejumlah tantangan dan juga kendala, di antaranya sebagai berikut :

- Jumlah kejadian / insiden cyber security semakin bertambah dari segi volume
- Security Threats semakin kompleks dan semakin sulit untuk di analisis
- Proses analisis pada saat melakukan IR dan investigasi dari berbagai macam data sources yang “scattered” membutuhkan effort dan waktu yang sangat banyak
- Proses containment dan mitigasi vulnerability semakin sulit seiring dengan semakin banyaknya kerentanan pada produk / aplikasi
- Adanya skill gaps di antara personil IR Team

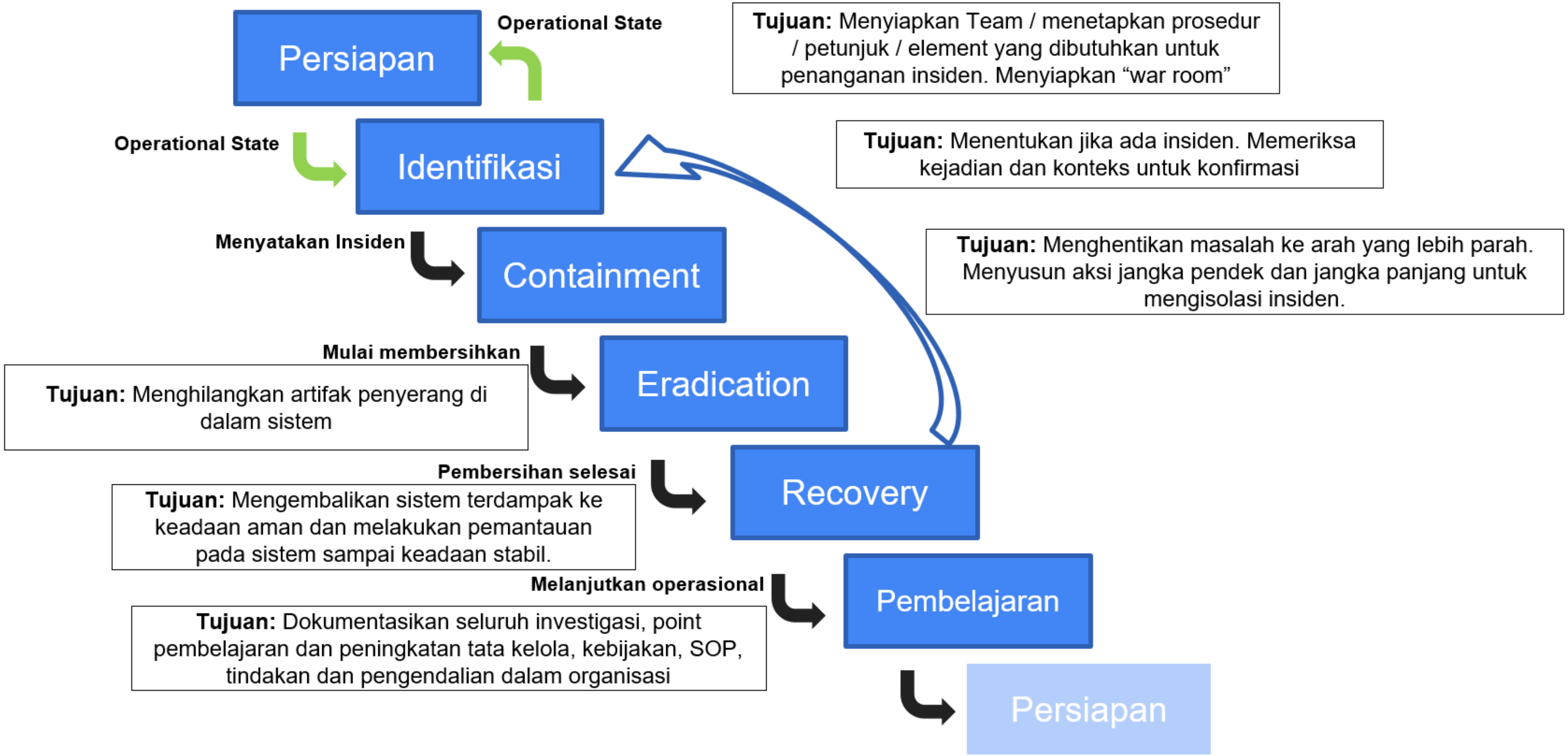
Security Incident Life Cycle



Incident Management dan Incident Handling



Incident Response Life Cycle



Persiapan

Operational State

Tujuan: Menyiapkan Team / menetapkan prosedur / petunjuk / element yang dibutuhkan untuk penanganan insiden. Menyiapkan “war room”

Operational State

Identifikasi

Tujuan: Menentukan jika ada insiden. Memeriksa kejadian dan konteks untuk konfirmasi

Menyatakan Insiden

Containment

Tujuan: Menghentikan masalah ke arah yang lebih parah. Menyusun aksi jangka pendek dan jangka panjang untuk mengisolasi insiden.

Mulai membersihkan

Eradication

Tujuan: Menghilangkan artifak penyerang di dalam sistem

Pembersihan selesai

Recovery

Tujuan: Mengembalikan sistem terdampak ke keadaan aman dan melakukan pemantauan pada sistem sampai keadaan stabil.

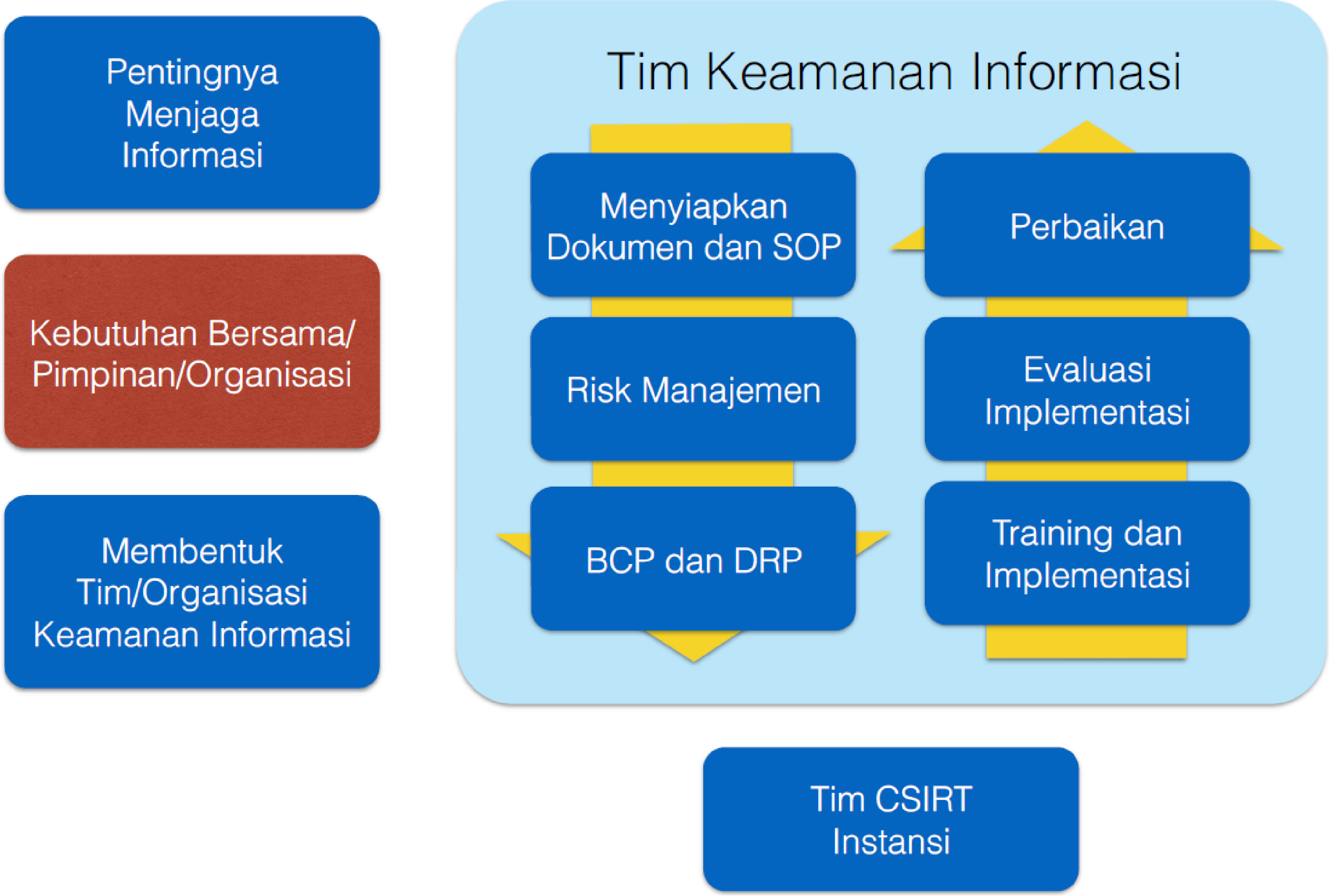
Melanjutkan operasional

Pembelajaran

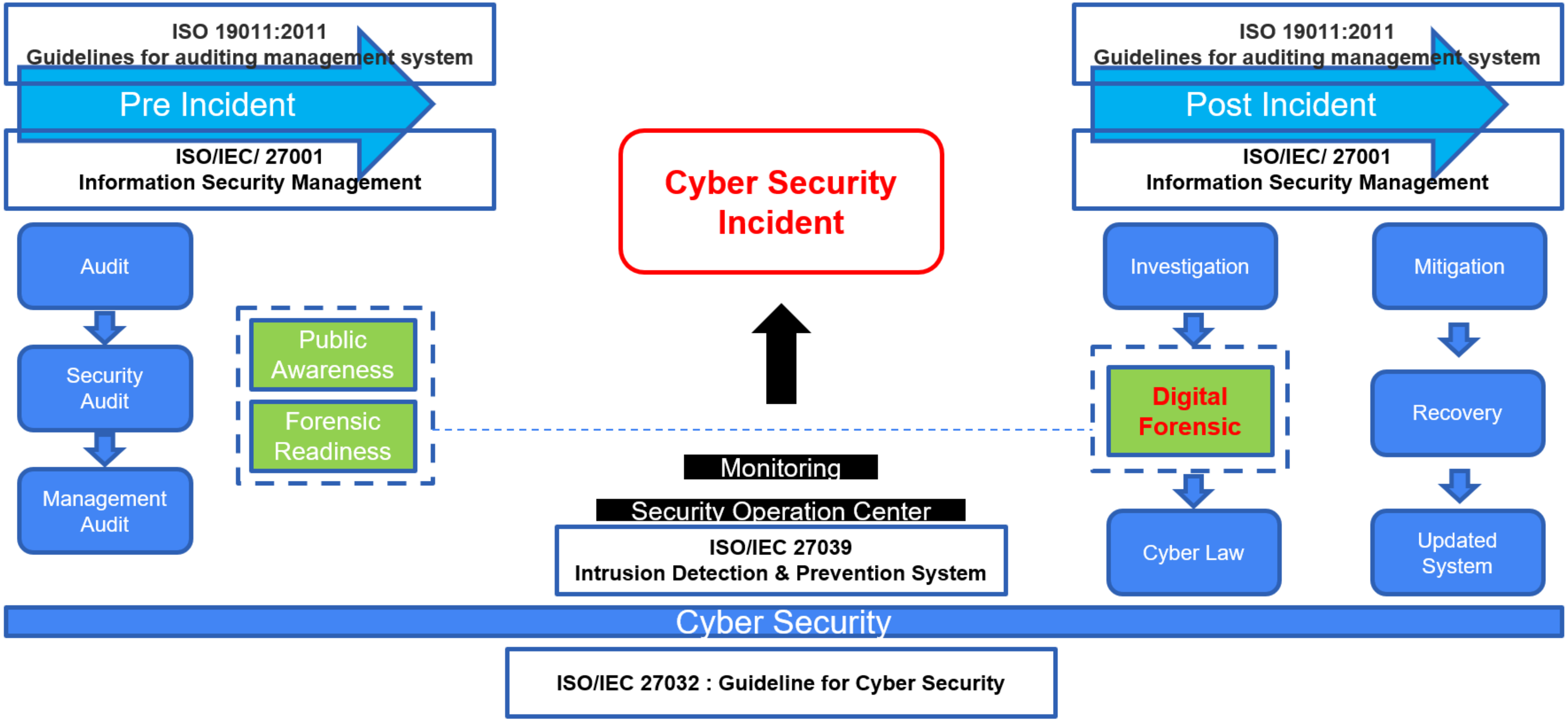
Tujuan: Dokumentasikan seluruh investigasi, point pembelajaran dan peningkatan tata kelola, kebijakan, SOP, tindakan dan pengendalian dalam organisasi

Persiapan

Kultur CSIRT di Organisasi


Pentingnya Menjaga Informasi
Kebutuhan Bersama/ Pimpinan/Organisasi
Membentuk Tim/Organisasi Keamanan Informasi
Tim Keamanan Informasi
Menyiapkan Dokumen dan SOP
Risk Manajemen
BCP dan DRP
Perbaikan
Evaluasi Implementasi
Training dan Implementasi
Tim CSIRT Instansi

Cyber Security Incident Management



ISO 19011:2011
Guidelines for auditing management system

ISO/IEC/ 27001
Information Security Management

ISO/IEC 27039
Intrusion Detection & Prevention System

ISO 19011:2011
Guidelines for auditing management system

ISO/IEC/ 27001
Information Security Management

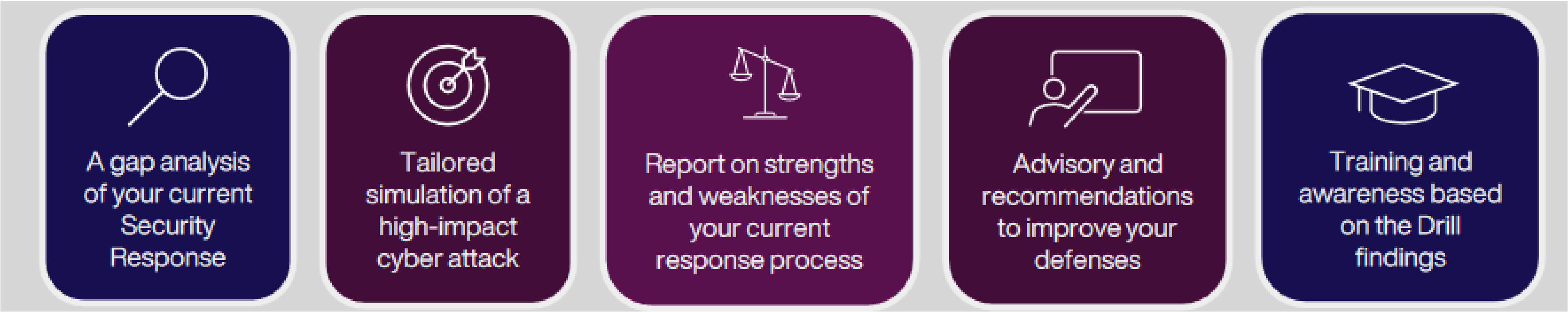
ISO/IEC 27032 : Guideline for Cyber Security

Cyber Security Incident Phase

- **Before Incident :**
  - Penguatan ketahanan Sistem
  - Melakukan Security Monitoring
  - **Persiapan / Readiness** System sebelum incident terjadi (**Cyber Drill**, DFIR Readiness Assessment, VAPT, Persiapan SOP, Tools IR, Team IR, dll)
- **During Incident :**
  - Analisis terhadap Anomali pada System
  - Deteksi terhadap aktivitas yang terjadi pada saat incident berlangsung
- **After Incident :**
  - Investigasi system terdampak
  - Analisis penyebab dari incident / root cause berdasarkan informasi yang di dapat pada “During Incident”
  - Threat Attribution / Profiling threat actor

Incident Response Team Preparedness

- Gap analysis terhadap kemampuan IR team saat ini **(Aspek People)**
- Mempersiapkan readiness di dalam organisasi dengan melakukan ***simulated attack*** **(Aspek people, process, dan technology)**
- Melakukan verifikasi terhadap terhadap tools dan teknologi yang saat ini digunakan dalam organisasi untuk penanganan insiden **(Aspek Technology)**
- Melakukan validasi dan verifikasi terhadap IR Policy dan Procedure yang dimiliki saat ini di dalam organisasi **(Aspek Process)**



A gap analysis of your current Security Response

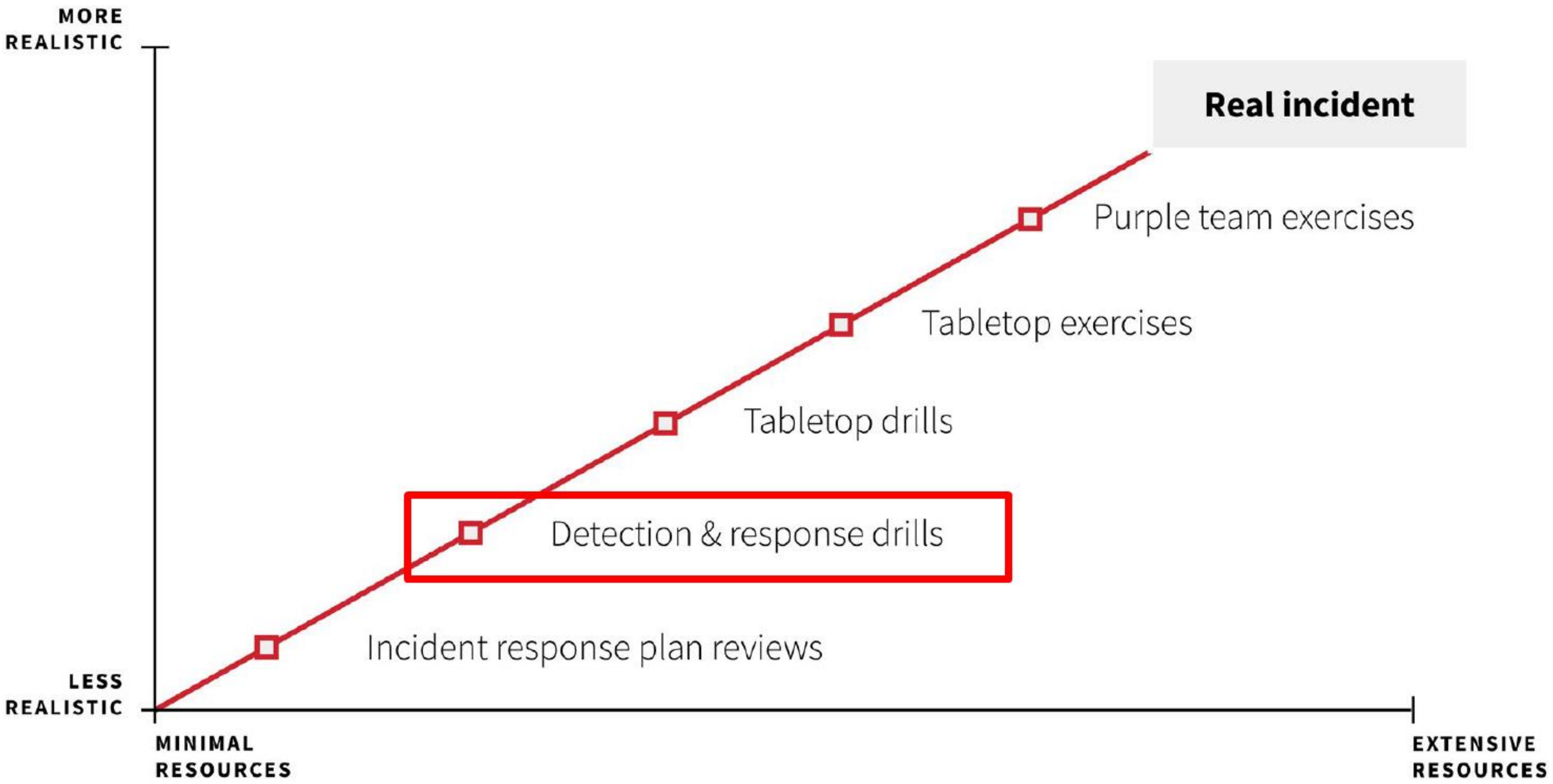
Tailored simulation of a high-impact cyber attack

Report on strengths and weaknesses of your current response process

Advisory and recommendations to improve your defenses

Training and awareness based on the Drill findings

Incident Response Readiness Program Example



Red Canary Incident Response and Readiness Guide

Are you ready – DFIR Readiness checklist

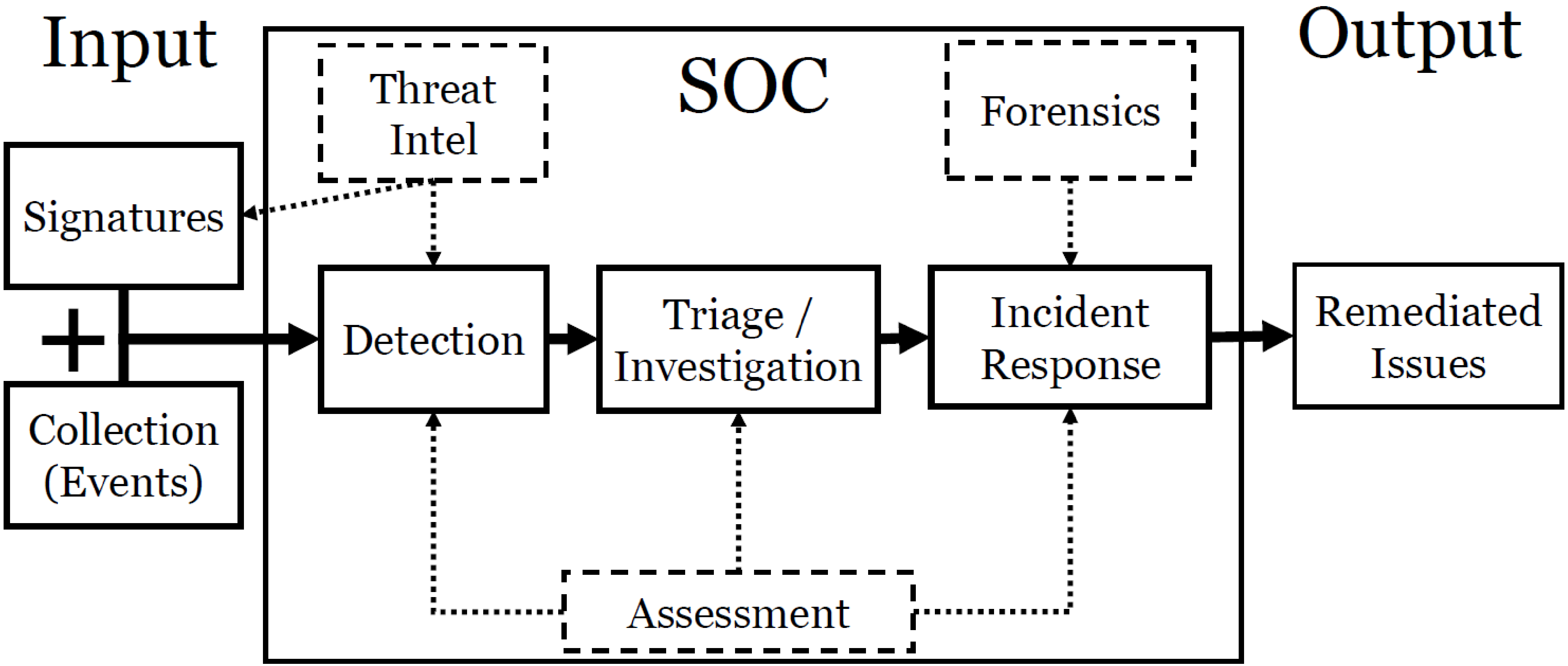
- ✓Identify the business scenarios and various threats both external and internals.
- ✓Identify potential sources and types of data – devices, applications, data bases
- ✓Map the sources of data with threat.
- ✓Identify the collection and retention requirement – Legal, Regulatory compliance
- ✓Awareness of SOC and IR team capability
- ✓Test and improve the forensic preservation, collection and chain of custody capability
- ✓Document evidence-based cases, describing the incident and its impact.
- ✓Ensure legal review to facilitate appropriate action in response to an incident
- ✓Test the sufficiency at regular intervals.

What is Missing?

- What logs from each device, application, database, etc, will generate?
- What type of logs are required to be captured for the type of attack?
- What type of logs are required to investigate a security incident?
- What type of logs are to be fed into SIEM for threat alert/modeling?
- What format they should be collected?
- How to preserve the logs(data)?
- How long they should be retained?
- What is the Legal & Regulatory requirements?

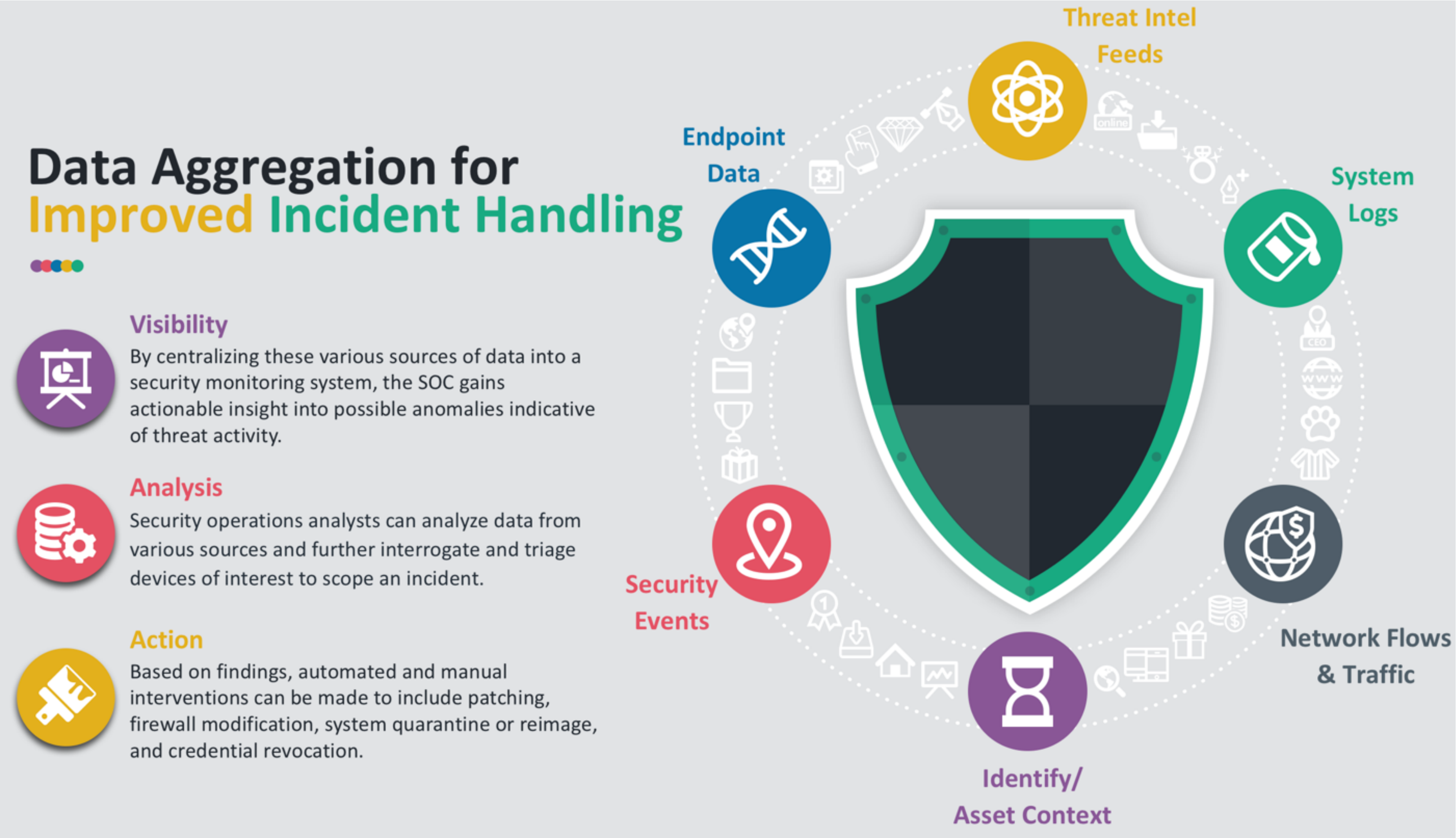
Our Disaster Recovery Plan Goes Something Like This...
HELP!
HELP!

Holistic SOC Process in a Flow



SANS Institute Blue Team Operation Tools

Data Aggregation for Improved Incident Handling



Data Aggregation for Improved Incident Handling

Visibility

By centralizing these various sources of data into a security monitoring system, the SOC gains actionable insight into possible anomalies indicative of threat activity.

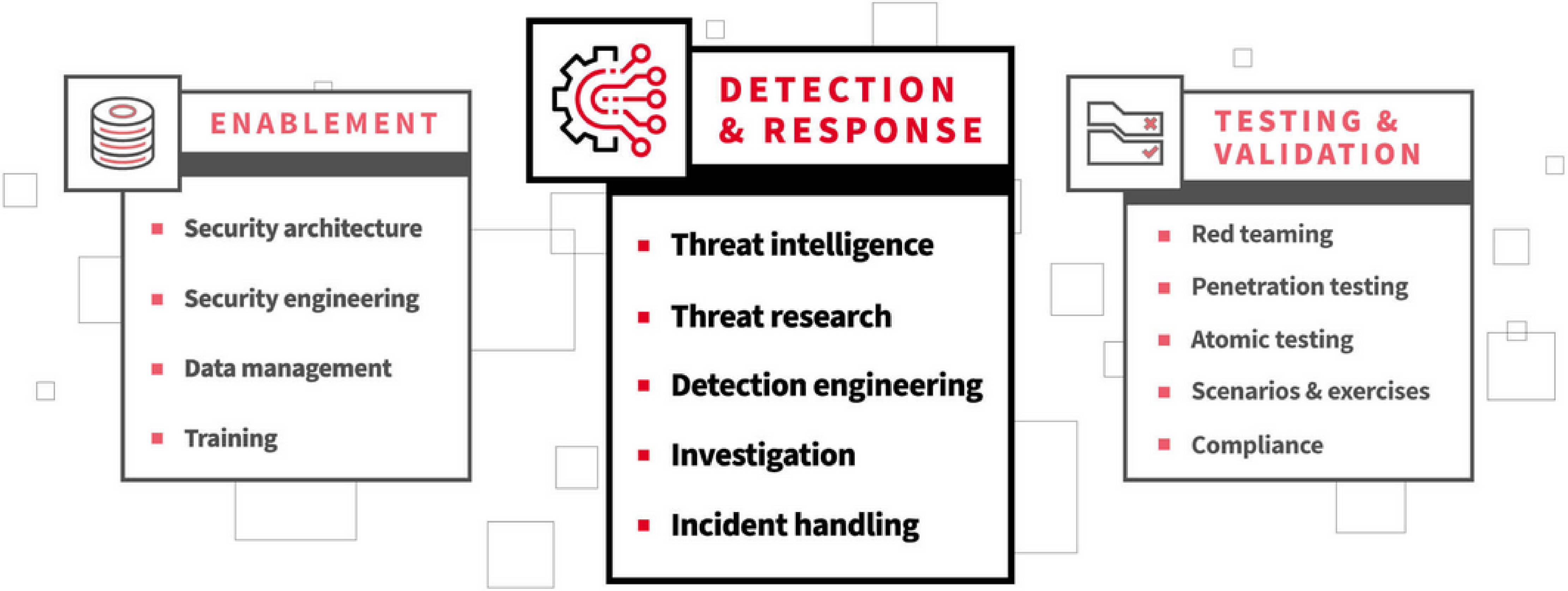
Analysis

Security operations analysts can analyze data from various sources and further interrogate and triage devices of interest to scope an incident.

Action

Based on findings, automated and manual interventions can be made to include patching, firewall modification, system quarantine or reimage, and credential revocation.

Modern Threat Analysis, Detection, and Response



ENABLEMENT

- Security architecture
- Security engineering
- Data management
- Training

DETECTION & RESPONSE

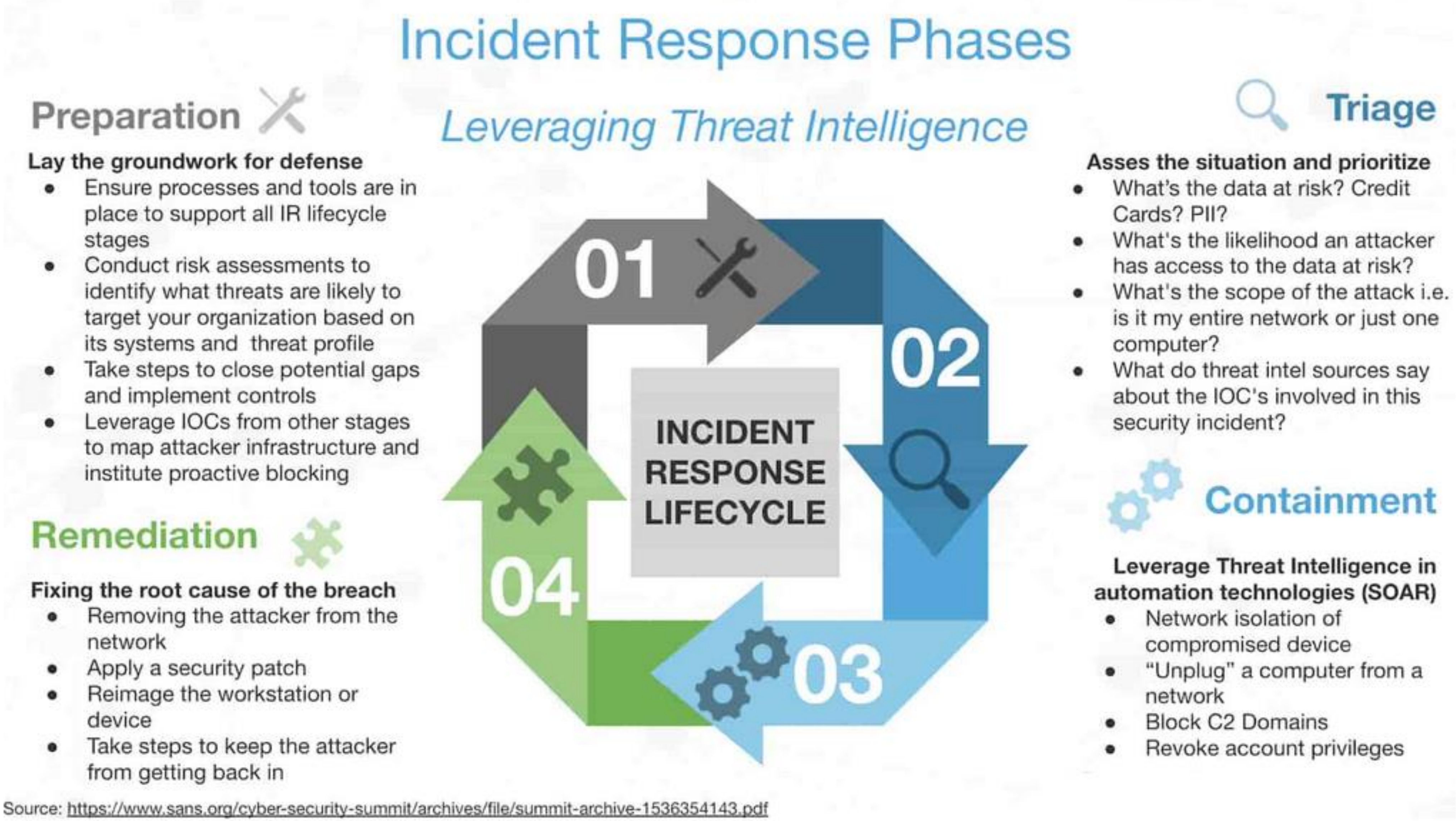
- Threat intelligence
- Threat research
- Detection engineering
- Investigation
- Incident handling

TESTING & VALIDATION

- Red teaming
- Penetration testing
- Atomic testing
- Scenarios & exercises
- Compliance

https://redcanary.com/blog/modern-security-operations-center/

Leveraging Threat Intelligence for Incident Response



Incident Response Phases

Leveraging Threat Intelligence

Preparation

Lay the groundwork for defense

- Ensure processes and tools are in place to support all IR lifecycle stages
- Conduct risk assessments to identify what threats are likely to target your organization based on its systems and threat profile
- Take steps to close potential gaps and implement controls
- Leverage IOCs from other stages to map attacker infrastructure and institute proactive blocking

Triage

Asses the situation and prioritize

- What's the data at risk? Credit Cards? PII?
- What's the likelihood an attacker has access to the data at risk?
- What's the scope of the attack i.e. is it my entire network or just one computer?
- What do threat intel sources say about the IOC's involved in this security incident?

Containment

Leverage Threat Intelligence in automation technologies (SOAR)

- Network isolation of compromised device
- "Unplug" a computer from a network
- Block C2 Domains
- Revoke account privileges

Remediation

Fixing the root cause of the breach

- Removing the attacker from the network
- Apply a security patch
- Reimage the workstation or device
- Take steps to keep the attacker from getting back in

Source: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1536354143.pdf

How does CTI Helps IR?

- **Faster Incident Response**

Using CTI, incident response teams can quickly and more effectively respond to a threat based on insightful information about adversaries and their attack methods.

- **In-Depth Threat Analysis**

Threat intelligence provides incident response teams with an in-depth analysis of every threat, helping them analyze the different techniques that adversaries can use. This improves the overall security of organizations and protects their network from new vulnerabilities.

- **Improved Efficiency**

Threat intelligence helps security teams to streamline incident triage, investigation, and actioning within an automated response workflow. This improves response speed , allowing for more time to focus on actual threats.

How does CTI Helps IR?

- **Threat Intelligence Enables Preparation and Prioritization**

Working under all of these constraints, incident response teams almost have no choice but to be reactive when potential threats materialize. In a typical incident response process, once alerts are flagged, they must be triaged, remediated, and followed up with as quickly as possible to minimize impact.

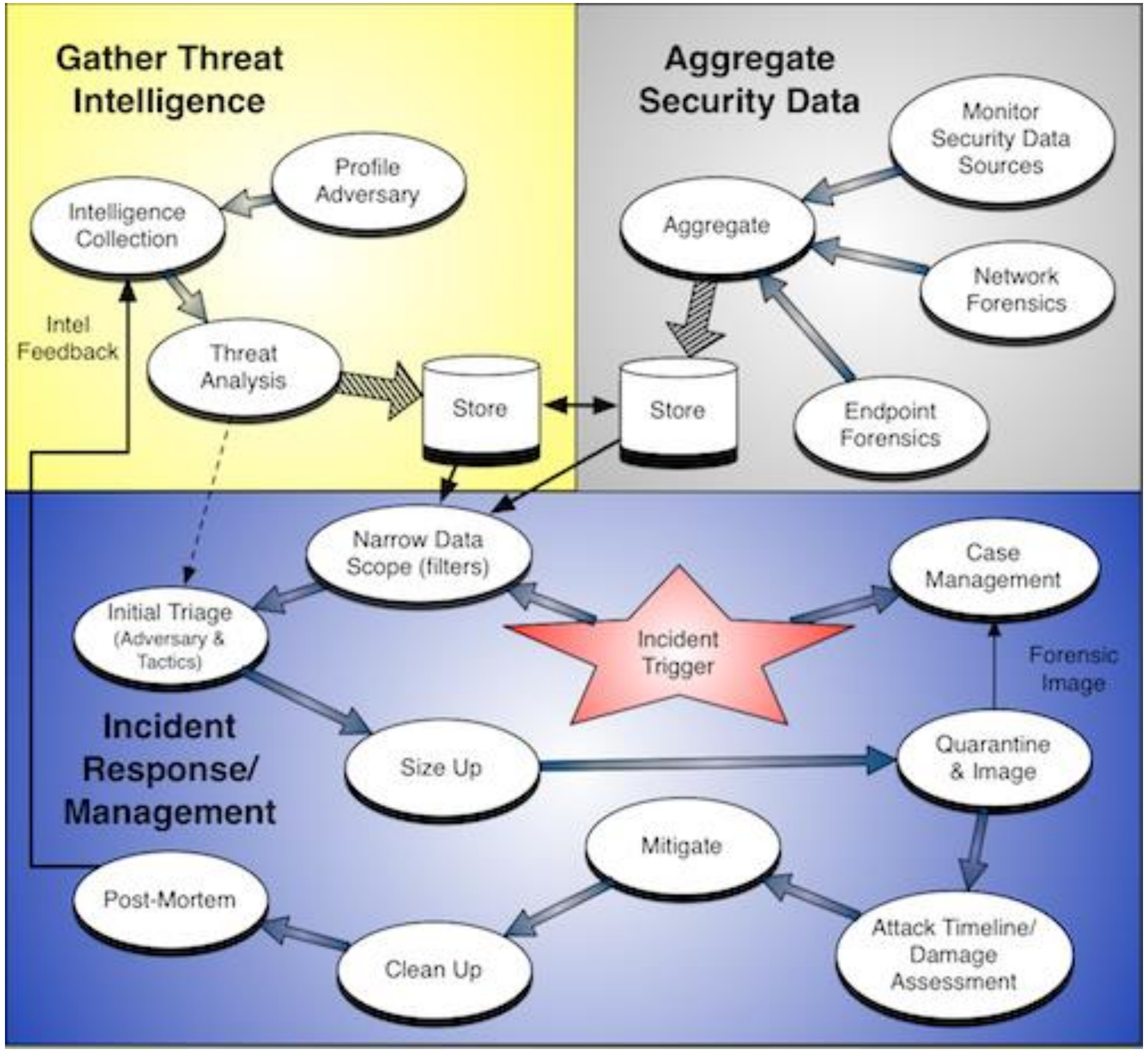
- **Improved Risk Management**

With cybercriminals continuously looking for new vulnerabilities to penetrate an enterprise’s network, threat intelligence provides proper visibility into identifying new vulnerabilities, reducing the risk of data loss. Additionally, it helps in blocking and minimizing the damage in day-to-day operations

- **Cost Savings**

If the response to a data breach is slow, organizations can lose more money. Threat intelligence helps identify data breaches and enables security teams to mitigate them quickly, minimizing the overall expense.

Final Stage of IR with CTI



https://securosis.com/research/publication/leveraging-threat-intelligence-in-incident-response-management “one organization’s detection to become another’s prevention”

Summary

- Tren ancaman keamanan siber semakin kompleks, dan banyak yang mengarah kepada serangan yang *targeted* terhadap organisasi dan juga individu tertentu
- *Threat Actor* berevolusi dengan berbagai macam Tactic Technic serta Procedure, oleh karena itu, organisasi juga harus berevolusi dan menaikkan kapasitas cyber resiliency
- Organisasi perlu mengingkatkan kapabilitas dalam defensive security untuk mendeteksi, serta memproteksi adanya kemungkinan adanya Comrpmise Incident dari aplikasi, OS, DB dan infrastruktur
- Organisasi perlu mempersiapkan jika terjadi Incident, dengan **Menyusun Incident Response Plan** serta mempersiapkan dan **mematangkan tahapan dalam incident response readiness program**
- Perlu adanya pendekatan upaya baru dalam penanganan Incident Response, salahs atunya dengan **Intelligence Driven Incident Response**, dengan harapan hal ini dapat membantu proses IR agar lebih cepat serta memberikan konteks yang mendalam dari TTP threat Actor.

Q&A