Strategi Membangun Kapabilitas Deteksi Serangan Siber

Cyberhub Webinar Series
23 April 2025

Digit Oktavianto
https://threathunting.id

About Me

- **Infosec Consulting Manager at FPT Metrodata Indonesia (FMISEC)**
- **Co-Founder BlueTeam.ID (https://blueteam.id)**
- **Born to be DFIR Team**
- **Community Lead @ Cyber Defense Community Indonesia**
- **Member of Indonesia Honeynet Project**
- **Opreker and Researcher**
- **{GCIH | GMON | GCFE | GICSP | GCTI | CEH | CSA | ECSA | ECIH | CHFI | CTIA | ECSS | eCMAP | eCTHP | eCIR} Certifications Holder**

Trend Criminal as A Service

- Selama beberapa dekade terakhir, cyber security underground criminal telah berevolusi dari beberapa kelompok kecil yang meretas dan hanya melakukan untuk kesenangan semata, menjadi industri kriminal yang berkembang pesat yang menelan kerugian dalam ekonomi global sekitar USD 300+ miliar per tahun[1]
- Dari informasi di atas dapat kita lihat bahwasannya :
  - Bagaimana threat actor mengubah permainan dengan **berkolaborasi** untuk menghasilkan lebih banyak uang dari hasil kejahatan
  - Bagaimana organisasi kita mungkin sudah menjadi bagian dari sasaran oleh threat actor tersebut
  - Dan bagaimana kita dapat meningkatkan perlindungan (dan menghindari menjadi korban).

[1] http://www.mcafee.com/nl/resources/reports/rp-economic-impact-cybercrime.pdf

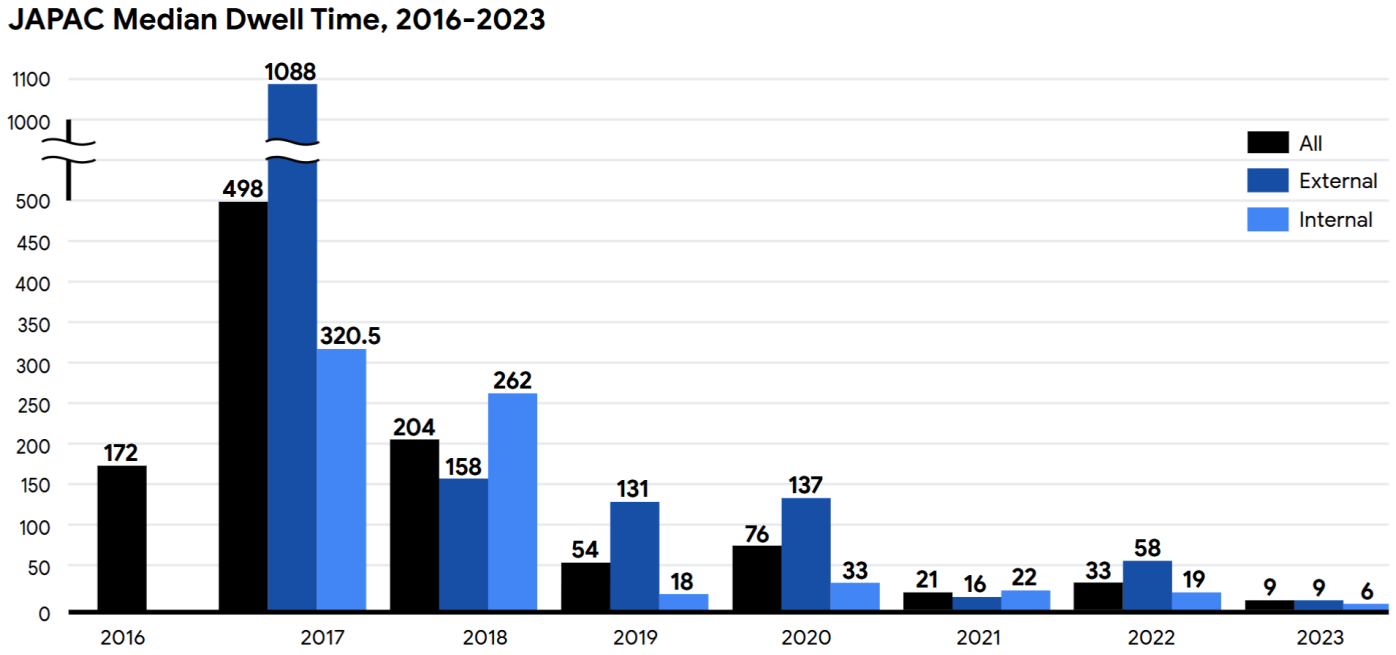

There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.
John Chambers
Chief Executive Officer of Cisco

Dwell Time In Cyber Security

Dwell time is calculated as the number of days an attacker is present in a victim network before they are detected. The median represents a value at the midpoint of a data set sorted by magnitude.

Change in JAPAC Median Dwell Time

33 days in 2022 ↘ 9 days in 2023



Mandiant M-Trend Report 2024

Cyber Security Incident dan Impact Terhadap Business

Immediate Implications for the Business

- Loss of data
- Corruption or destruction of data
- Unauthorized access
- Account takeovers
- Compromised systems and applications
- Unavailability of services

Impact on the Business

- Reputational loss
- Financial loss/fraud
- Regulatory compliance incidents and penalties
- Client loss

http://pubdocs.worldbank.org/en/513651432913969312/Ruth-Wandhoefer-Citi-FinSAC-Cyber-Seminar-18-19-May.pdf

Trend Detection dan Response Keamanan Siber

- Hampir Sebagian besar organisasi saat ini berupaya semaksimal mungkin untuk meningkatkan visibilitas dan kemampuan untuk mampu melakukan **early detection** terhadap serangan siber. Hal ini dikarenakan organisasi mulai sadar technology prevention saja tidak cukup. **Prevention may and can be fail at anytime**.
- **People, Process, dan Technology di area Detection** yang saat ini dimiliki oleh organisasi masih sangat amat terbatas. Banyak area yang belum di cakup oleh teknologi tersebut
- **People, Process, dan Technology di area Response** yang membantu organisasi pada saat terjadi breach atau compromise terjadi juga **belum banyak di implementasikan**. Teknologi Orchestration yang d gadang dapat membantu untuk speed up saat terjadi suatui intrusion dan attack juga belum banyak di adopsi oleh organisasi.

Common Problem Dalam Organisasi terkait Cyber Security

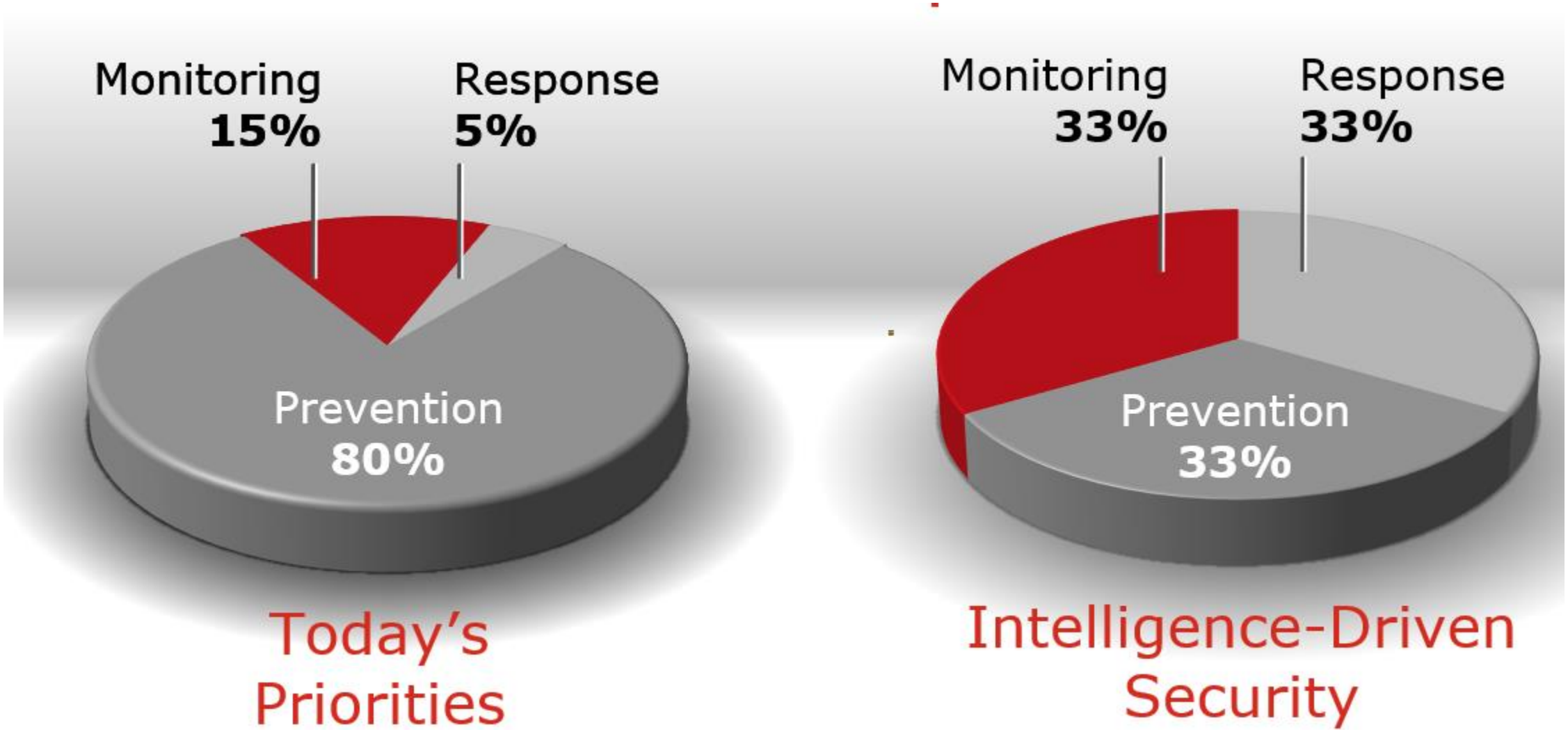
- **Fokus di Area Prevention / Protection**

  Serangan yang Advance dan Modern Sebagian besar berhasil membobol / membypass teknologi di area Prevention / Protection. Sehingga jika kita masih focus di area tersebut, maka attacker akan dengan sangat mudah melakukan bypass terhadap keamanan kita tanpa kita sadari. **Perlu ada upaya shifting terhadap Detection baik di area Endpoint dan Network.**

- **Tidak adanya Evaluasi terhadap Existing System**

  Teknologi yang sudah di investasikan tidak pernah dilakukan gap assessment dan juga evaluasi apakah teknologi yang digunakan sudah efektif dan efisien? Atau teknologi tersebut tidak mampu melakukan Prevention, Detection, serta Response saat incident Cyber terjadi. Perlu adanya suatu mekanisme Proses yang paling tepat adalah dengan mengevaluasi teknologi tersebut melalui **Adversary Emulation / Adversary Simulation.**

Shifting Prioritas dalam Cyber Security



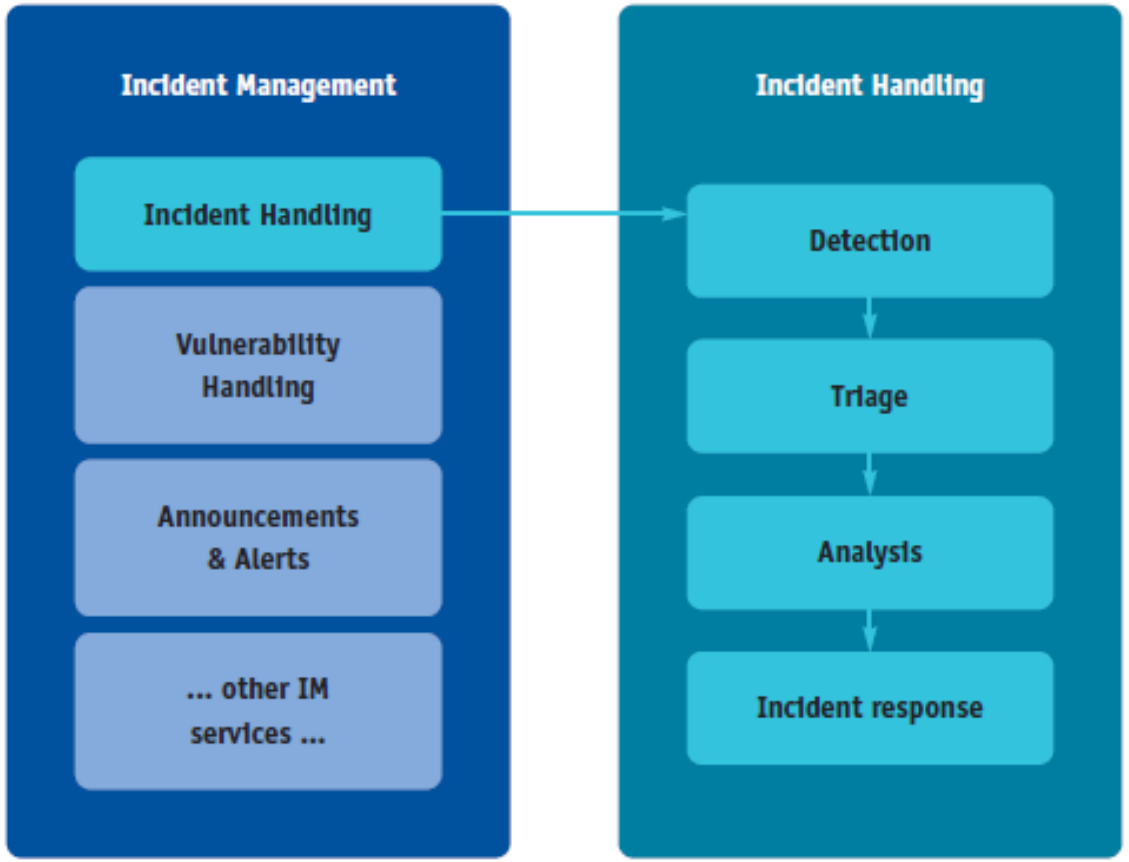
Jadi, Bagaimana Dengan Kita?

Prepare Battle Ground

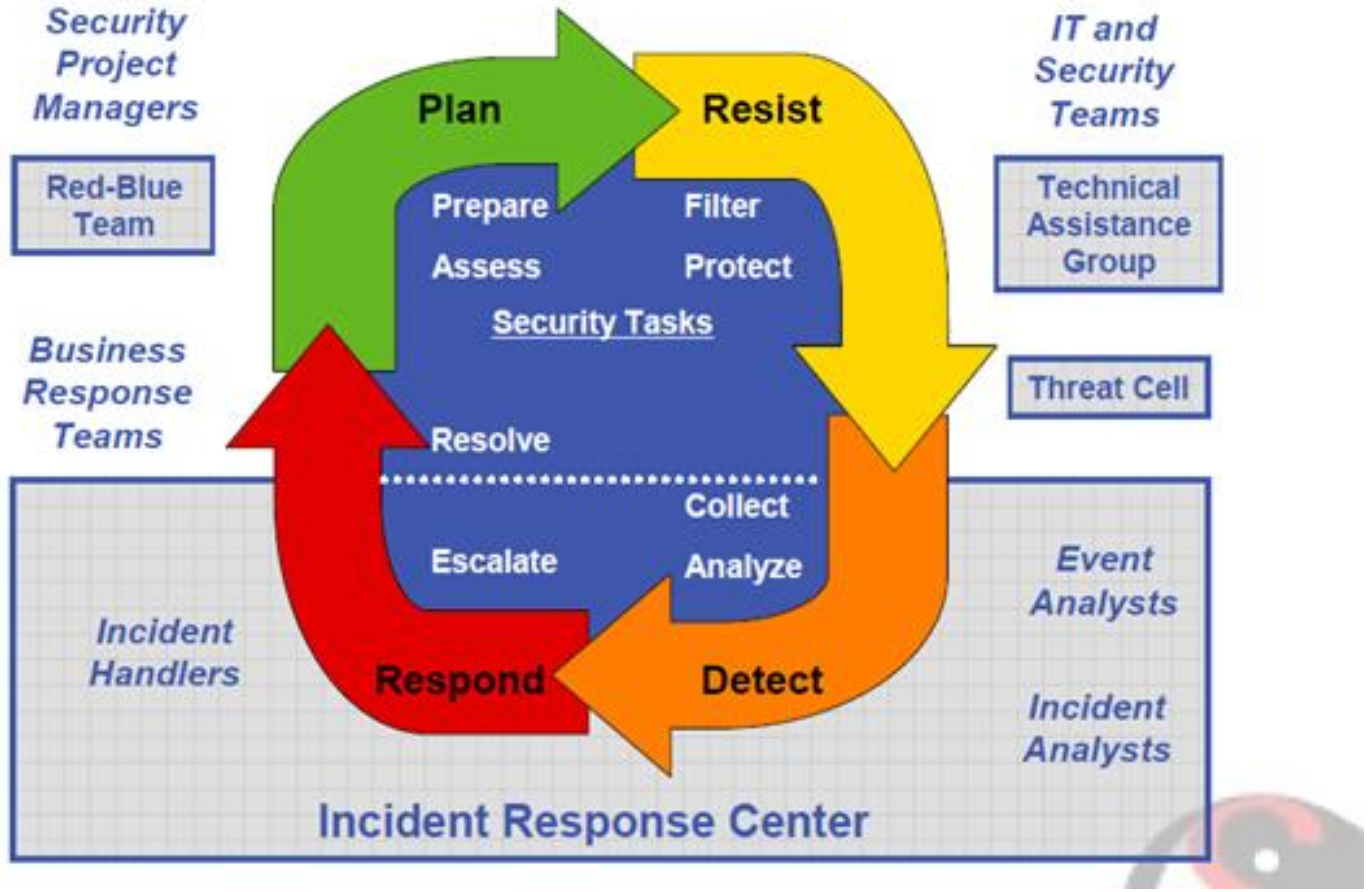
- ✓ **Cyber Defense Operation, Continuous Security Monitoring, Incident Response Preparedness**
- ✓ Mempersiapkan 3 Komponen Utama : **Protection, Detection, Response**
- ✓ **Security Awareness** untuk **Semua Orang di Dalam Organisasi**


Businesses whose cyber security is 'all sorted'
misconfigured firewalls
out of date software
using the same password for everything
no access controls

Incident Management dan Incident Handling



Security Incident Life Cycle

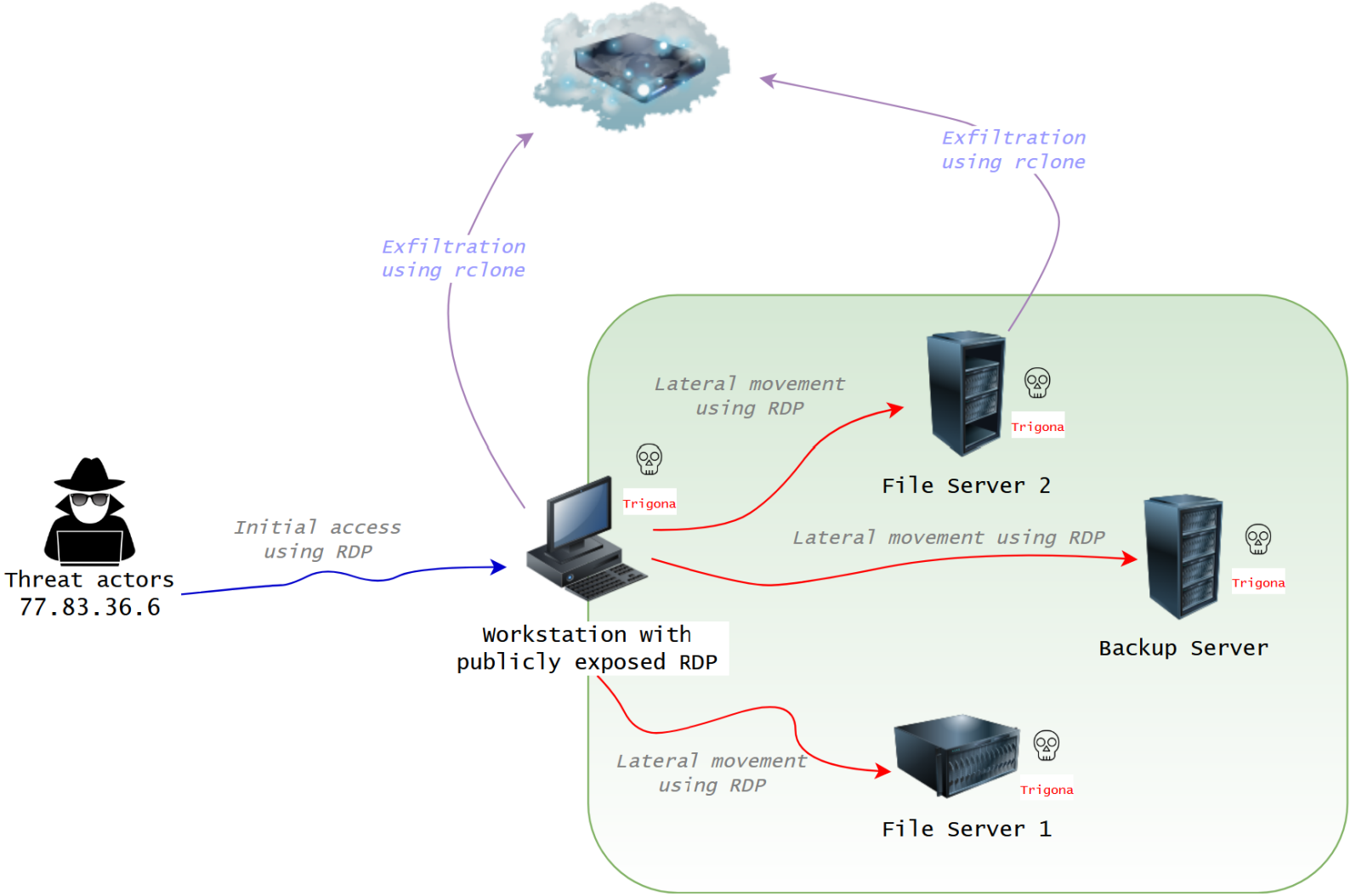


Siklus dan Phase Cyber Security Incident

Cyber Security Incident Phase

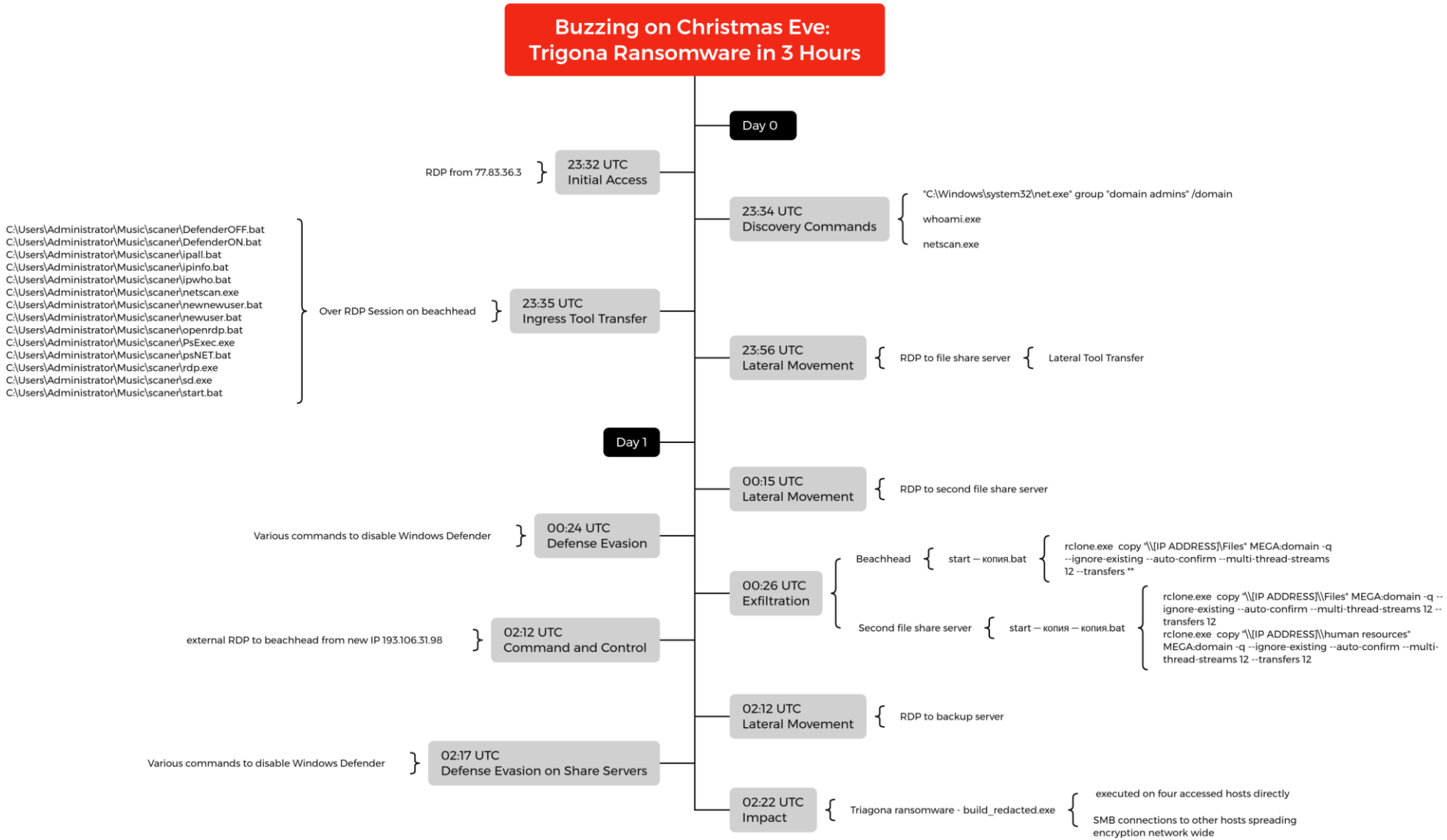
- **Before Incident :**
  - Penguatan ketahanan Sistem
  - Memiliki visibilitas terhadap sistem keseluruhan dan juga memiliki kapabilitas deteksi yang baik dan mumpuni
  - Melakukan Security Monitoring dan Analisis
  - Persiapan / Readiness System sebelum incident terjadi (Cyber Drill, DFIR Readiness 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

Sample Incident : Trigona Ransomware in 3 Hours



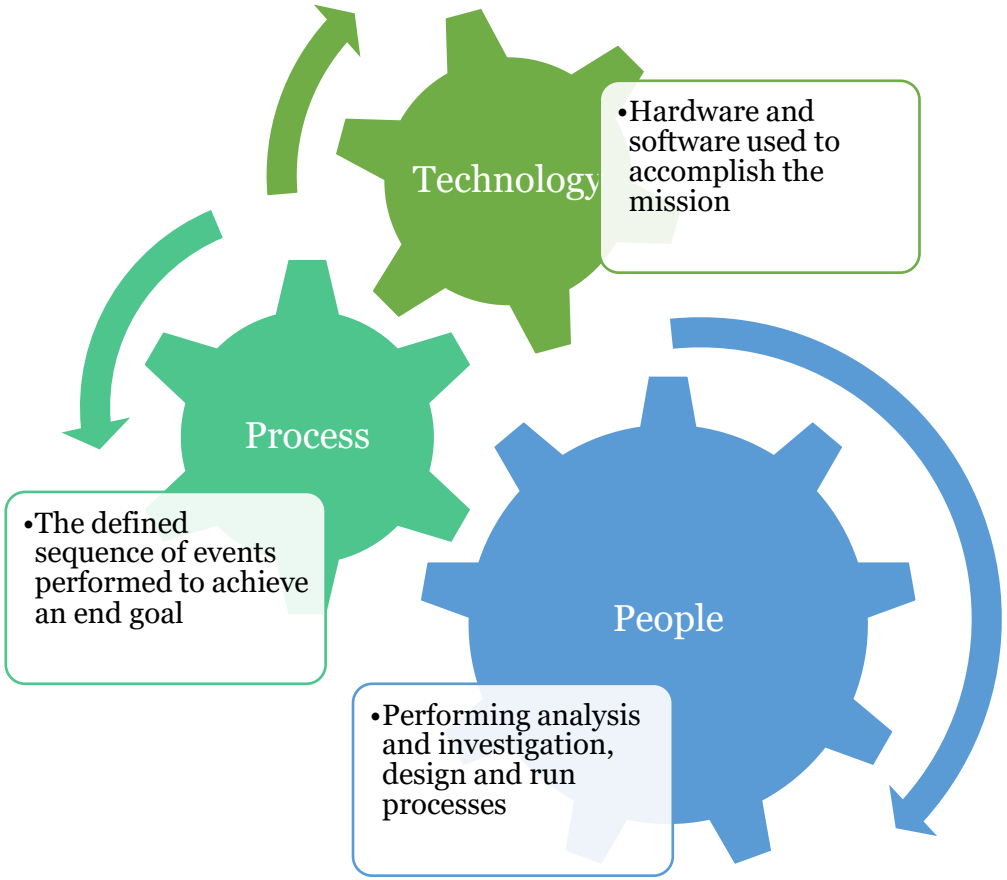
https://thedfirreport.com/2024/01/29/buzzing-on-christmas-eve-trigona-ransomware-in-3-hours/

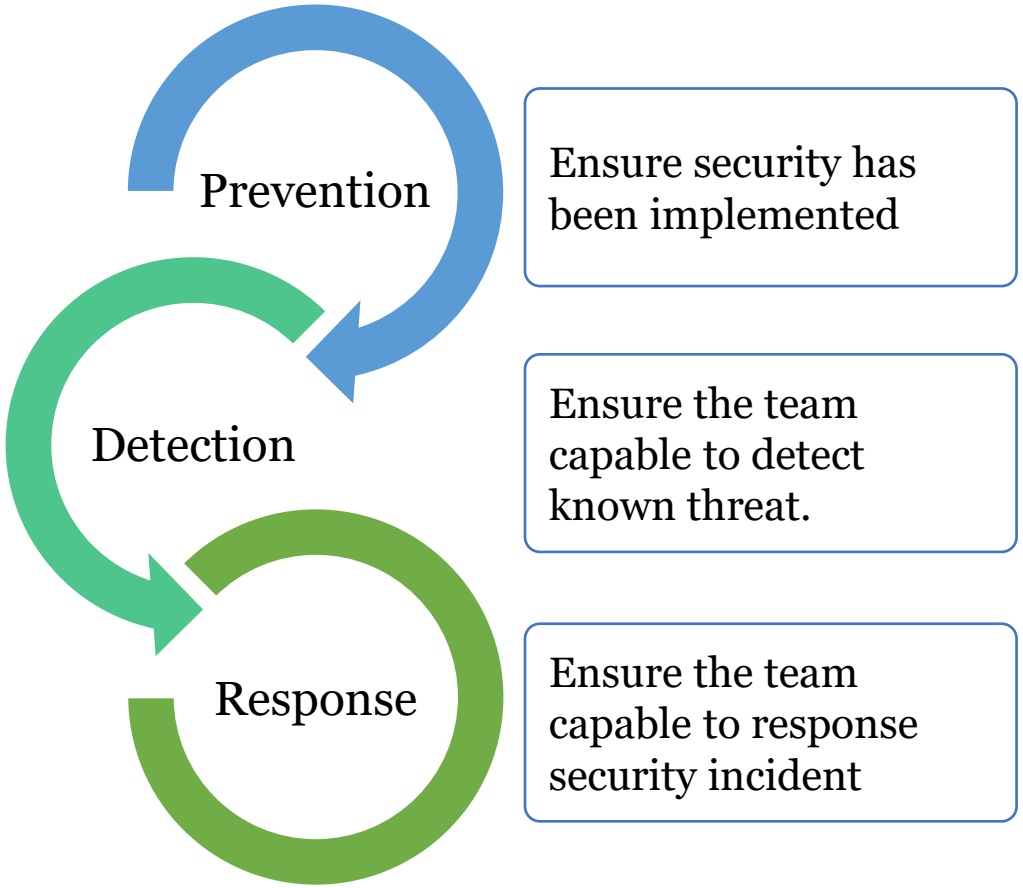
Sample Incident : Trigona Ransomware in 3 Hours



Defensive Security Capability

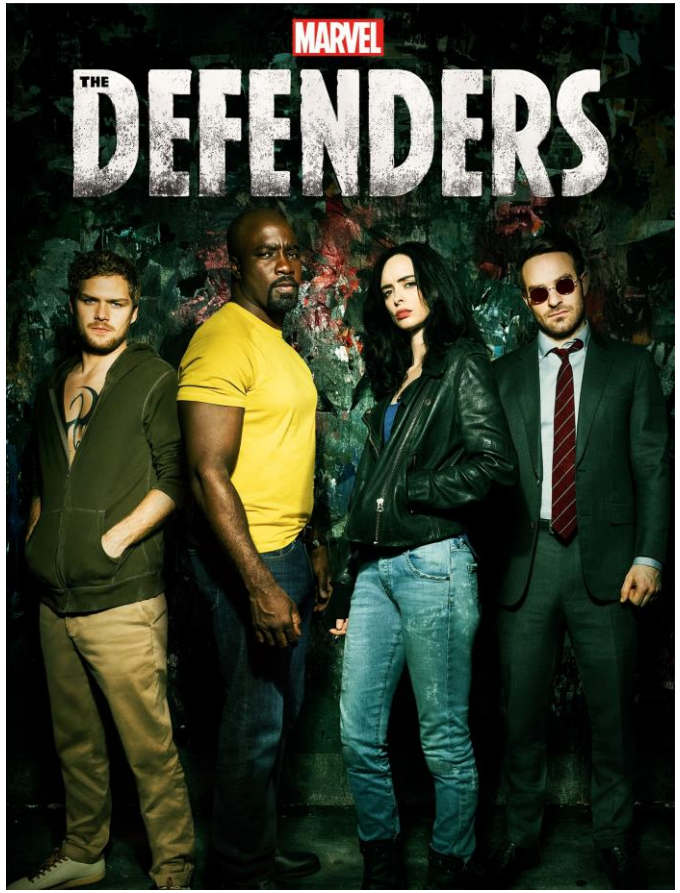
Kapabilitas Defensive Cyber Security Team





You Need Some Heroes

- The Defenders
- A **Blue Team** is a group of individuals who perform an analysis of information systems to:
  - Identify and give some recommendation for critical assets & systems
  - Ensure security has been implemented
  - Identify security flaws and inform into system owners
  - Verify the effectiveness of each security measure
  - Make certain all security measures will continue to be effective after implementation.
- Example : **Security Analyst, Security Engineer, Incident Responder, Threat Hunter, Digital Forensic Investigator, Malware Analyst**



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Awareness Control	Anomalies and Event	Response Planning	Recovery Planning
Business Environment	Awareness and training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Process	Analysis	Communications
Risk Assessment	Info Protection and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	

Kapabilitas dan Fungsi Blue Team

1. Collection
2. Detection
3. Triage
4. Investigation
5. Incident Response

Detection Engineering

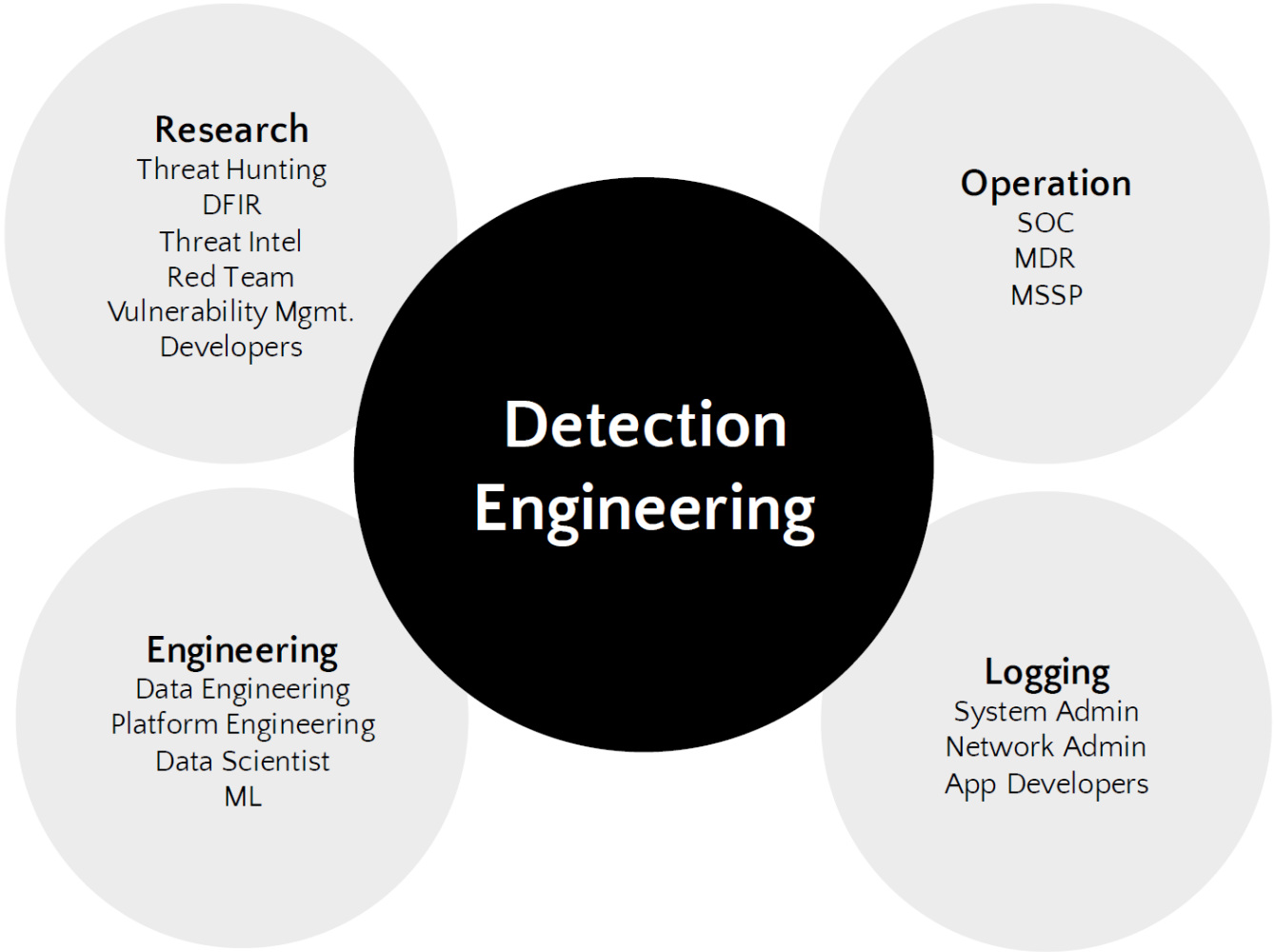
Detection Engineering

Detection engineering is a **set of practices and systems to deliver modern and effective threat detection.**

When building a solid detection engineering, **the main goal is to catch malicious things and to not catch too many not malicious things**. If the detection system interrupt an analyst's activities because calling attention to things that are not malicious, then you're creating more work for the analysts.

Detection products only **create value by detecting things that are truly bad**, and most detection products lean towards detecting more activity so as to not miss anything.

Detection Engineering in Cyber Security Org



Detection Engineering In Modern Day Security Organization by Tondang Mangatas and Sylvain Lu
https://www.youtube.com/watch?v=Q5uR-XePEYE

Requirements for Detection Engineering Program

Subject Matter Experts

Environmental awareness

- Logs, Data, Platform and Organizational

Risk and Threat awareness

- Internal, External, etc.

Logs and Telemetry

From all kind of sources

- Better if already Data Engineered
- Better if Centralized (such as using SIEM)

Platform

A place for Detection Engineer to play and work with telemetry and alerts

- SIEM is a good start

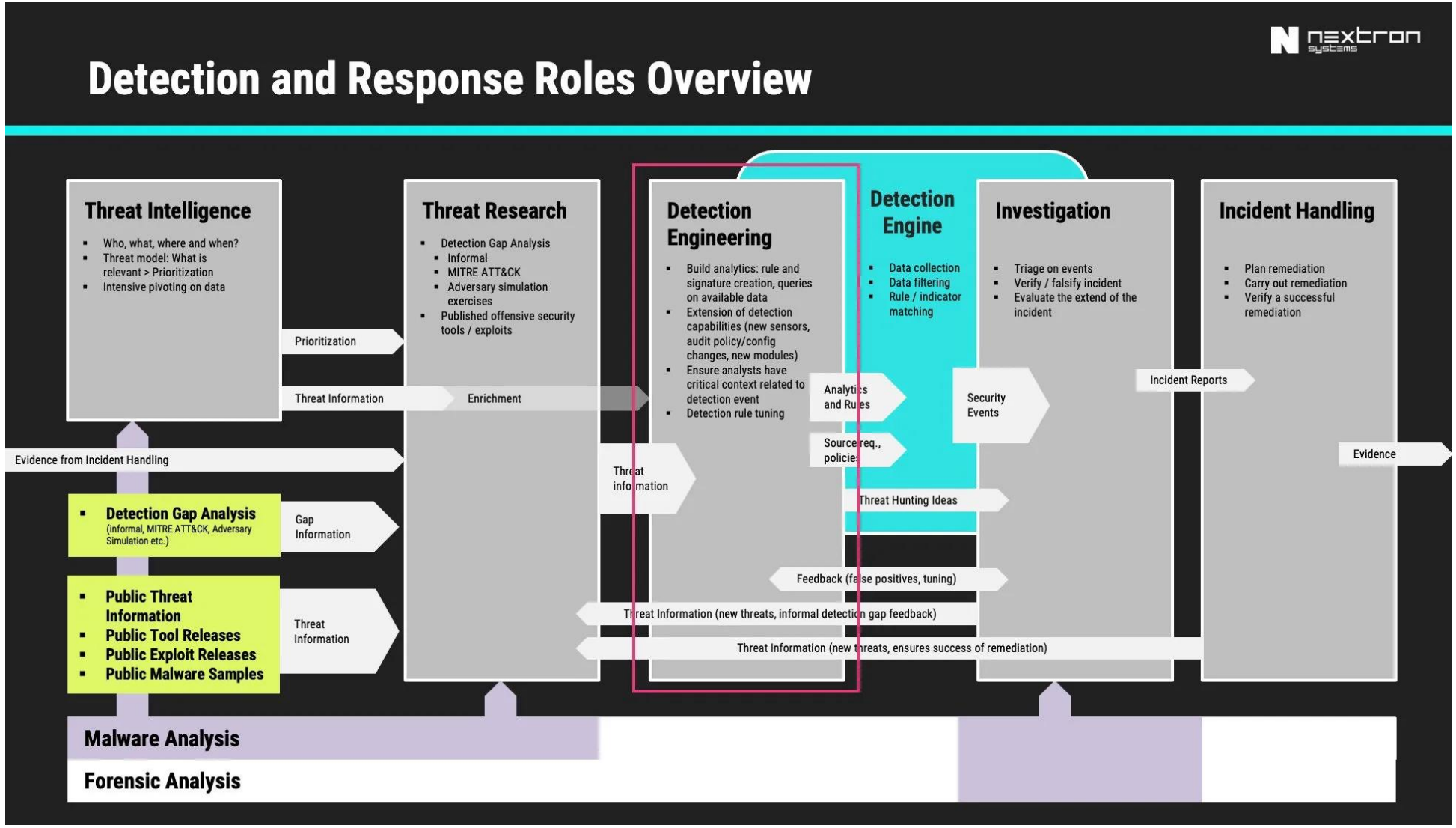
Organization Maturity

The organization should have other security arms ready

- Escalation and Investigation by SOC
- Incident Response by DFIR
- Platform Engineering

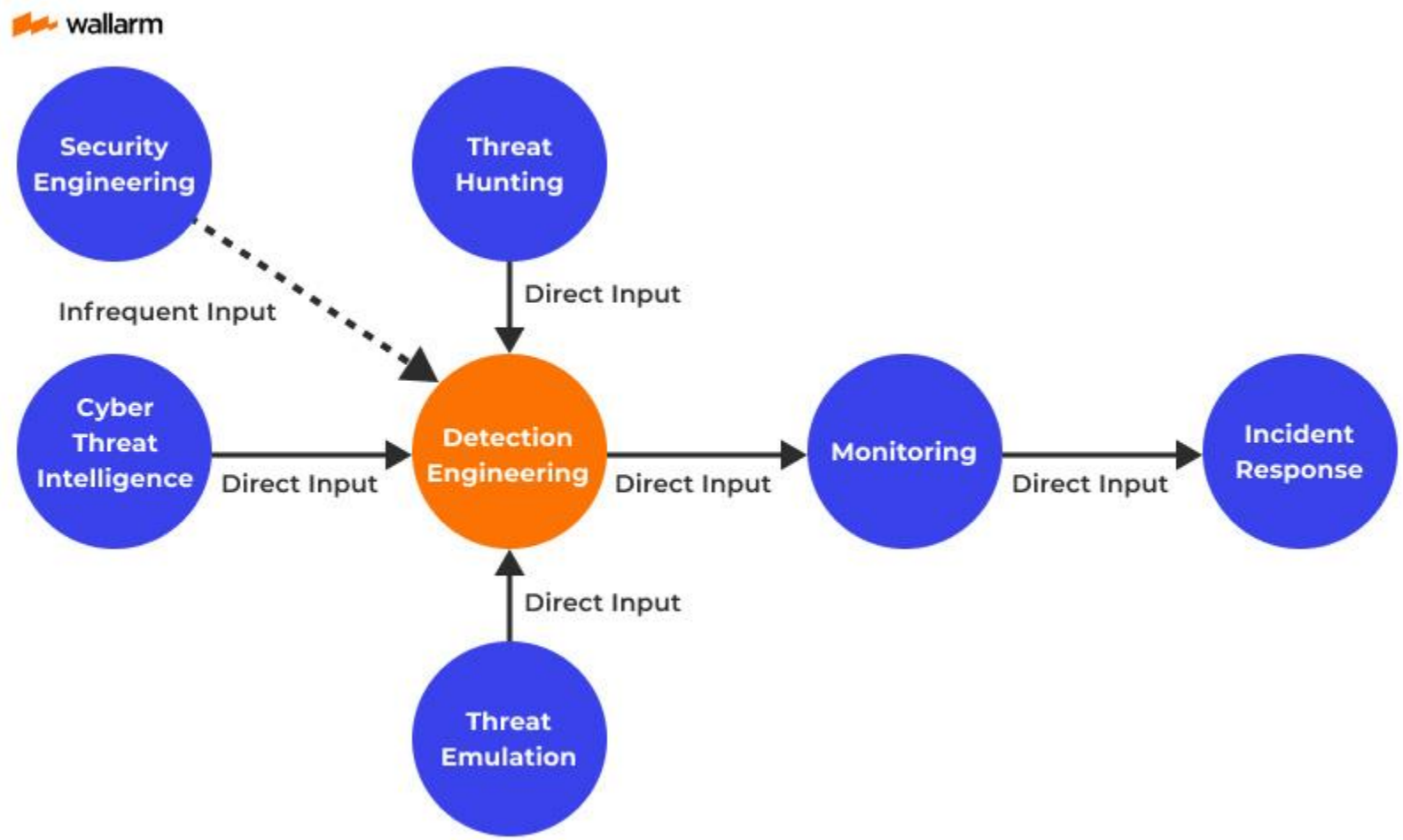
Detection Engineering In Modern Day Security Organization by Tondang Mangatas and Sylvain Lu
https://www.youtube.com/watch?v=Q5uR-XePEYE

Detection and Response Roles Overview

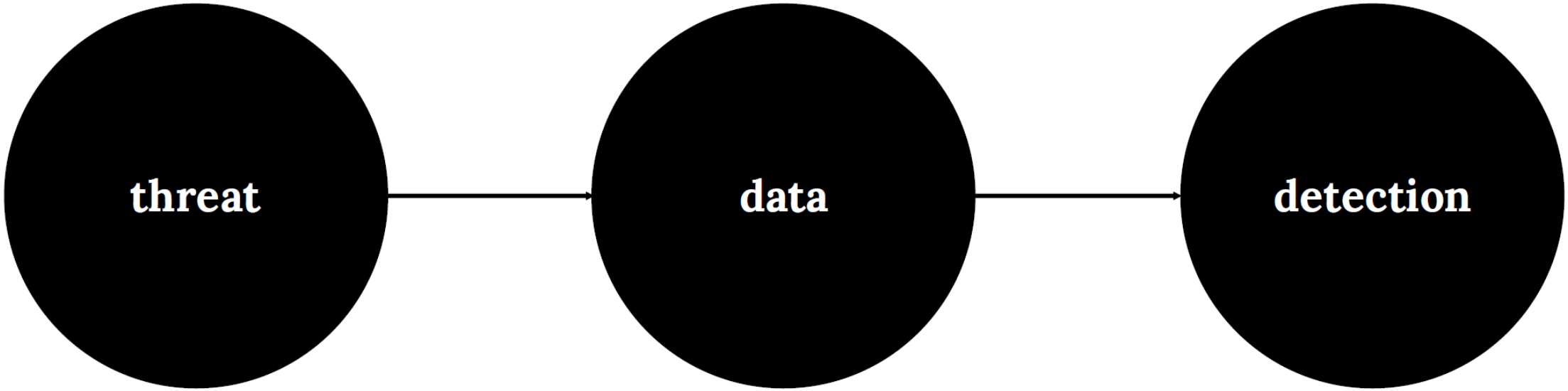


https://cyb3rops.medium.com/about-detection-engineering-44d39e0755f0

Relationship Between Detection Engineering and Other Entities



https://www.wallarm.com/what/detection-engineering



Detection Engineering In Modern Day Security Organization by Tondang Mangatas and Sylvain Lu
https://www.youtube.com/watch?v=Q5uR-XePEYE

Threats (TTP)

- Some great sources to learn about Threats
  - Past cyber security incidents or breaches
  - Threat Intelligence Reports
  - Security Advisories
  - Known frameworks such as Pyramid of Pain, MITRE ATT&CK and Lockheed Martin Cyber Kill Chain
  - Other Sources : Conference, Blog Post

- Understanding the threat = Knowing **what** to detect the threat

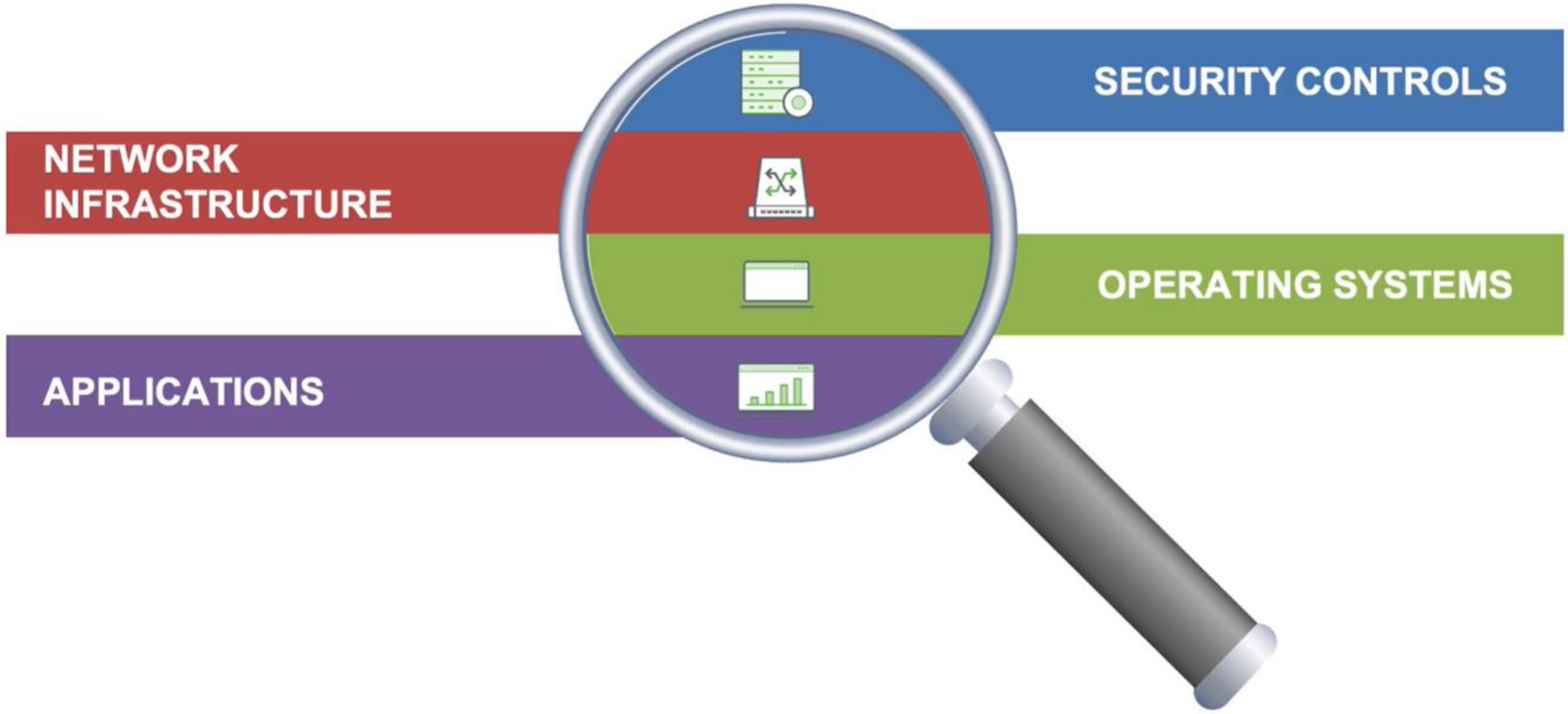
Data (Logs or Telemetry)

- Divided into 3 distinct domains
  - Network
  - Endpoint(Host, Server, Desktop, Mobile Device, IoT, ICS…)
  - Cloud (Including Cloud Apps)
- Knowing the baseline of our own environment
- Understanding the data = Knowing **where** to detect the threat

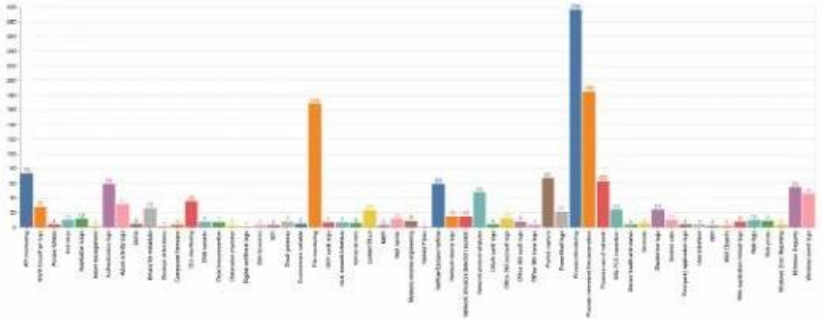
Detection Engineering

- Depends on your data and tech stack
  - SIEM, SOAR, EDR, NIDS, HIDS, etc.
- Can be simple or complex
  - IOC
  - TTPs
  - Correlation
  - Dashboards
  - Thresholds
  - ML
- Understanding the Detection = Knowing **how** to detect the threat, using the data and threat

Log Sources and Telemetry



Obviously we need to have data



Windows:
Event logs
Sysmon
EDR logs
PowerShell scriptblock, modules and transcripts
ETW
Debug logs

Linux:
Syslog
EDR logs
Auditd
Osquery

OS X:
Syslog
EDR logs
Osquery

Network:
Proxy
DNS
Firewall
IDS/IPS
Bro/Zeek
Netflow
PCAP data
Appliance logs

Cloud platforms
Email log
SaaS apps
Webserver Logs
Internal applications
Sandboxes
Much much more.....

@olafhartong

Endpoint Telemetry

HIDS/EDR/AV

Such as Sysmon, OSQuery, MDE, Crowdstrike

- Process Activity
- Module, Library, DLLs, Pipe activity
- File Activity
- Registry Activity
- Network Activity
- Detection/Prevention Activity

Host System

Such as Windows, Linux, MacOS, Android, iOS

- Execution
- Apps and System Activity (PowerShell, Scheduled Task, etc.)
- Web Browser Data
- Authentication/Permission/IAM
- Network (Filtering, etc.)

Server/App

Such as AD/ADFS, Email Server, Web Server, App Server

- Auth/Permission/IAM
- Apps activity
  - Login, User Changes, Orders, etc.

Detection Engineering In Modern Day Security Organization by Tondang Mangatas and Sylvain Lu
https://www.youtube.com/watch?v=Q5uR-XePEYE

Network & Network Security Telemetry

Appliances

Such as Firewall, Anti DDOS, Load Balancer, Router, DNS Server

- Allowed/Dropped Connectivity
- Address Translation
- Access Control
- Routing
- Appliances Commands

NIDS

Such as Bro, Zeek, Suricata

Protocol Based

- FTP
- SSH
- Auth Protocol (Kerberos, RADIUS, TACACS, etc.)
- Signature Alerts (e.g., SNORT)

Detection Engineering In Modern Day Security Organization by Tondang Mangatas and Sylvain Lu
https://www.youtube.com/watch?v=Q5uR-XePEYE

Cloud Telemetry

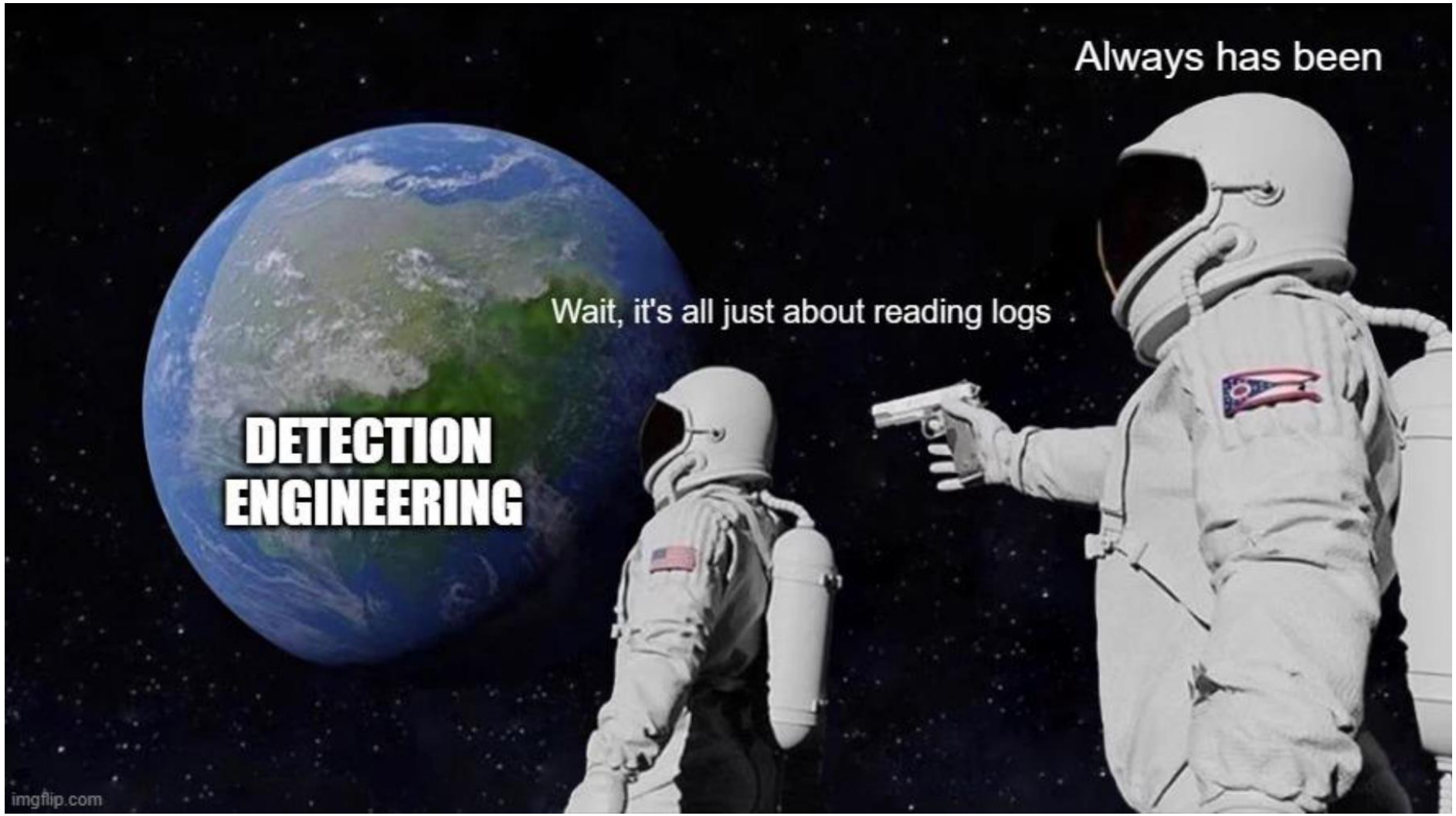
Cloud

- Auth/Permission/IAM
  - e.g., Okta Logs, Azure AD Logs
- User/Admin Activity
- Cloud Security Solution (e.g., M365D, Wiz, Trend Micro, Proofpoint)

Cloud Apps

- Apps Activity
  - File Storage Activity
  - Email Activity
- User/Admin Activity
- API Activity

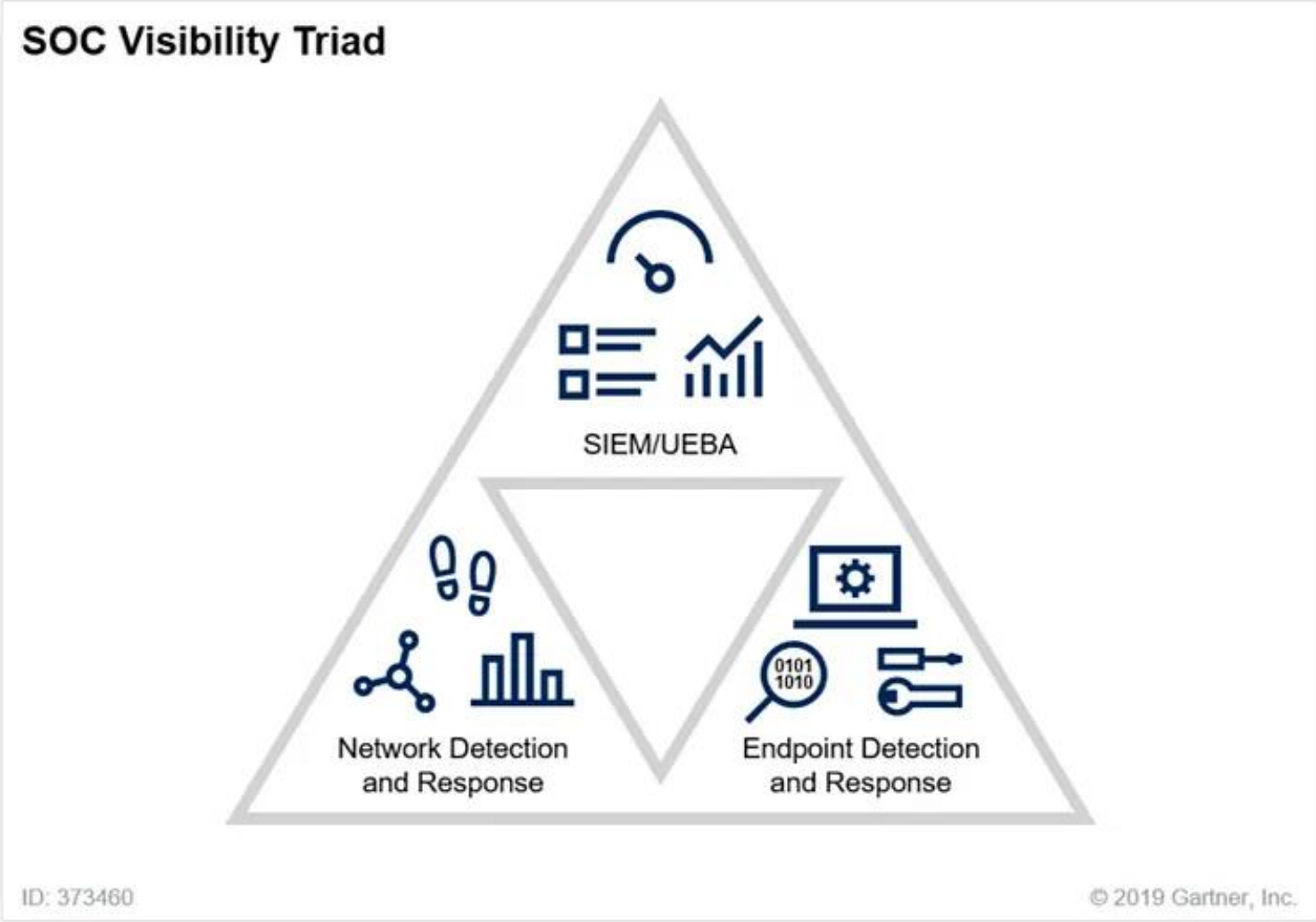
Detection Engineering In Modern Day Security Organization by Tondang Mangatas and Sylvain Lu
https://www.youtube.com/watch?v=Q5uR-XePEYE


Always has been
Wait, it's all just about reading logs
DETECTION ENGINEERING
imgflip.com

Teknologi Cyber Security Dalam Organisasi

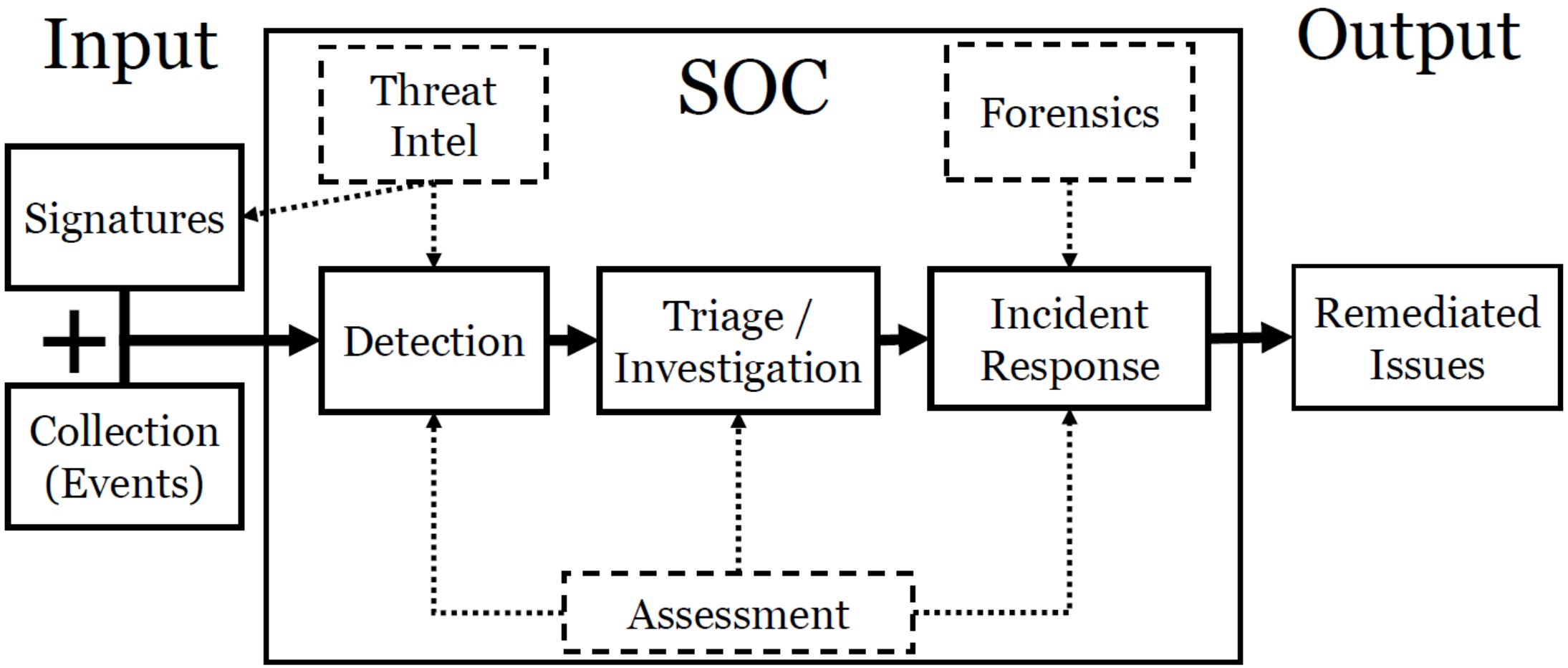

BUDGET BEFORE DATA BREACH
BUDGET AFTER DATA BREACH
imgflip.com

SOC Visibility Triad



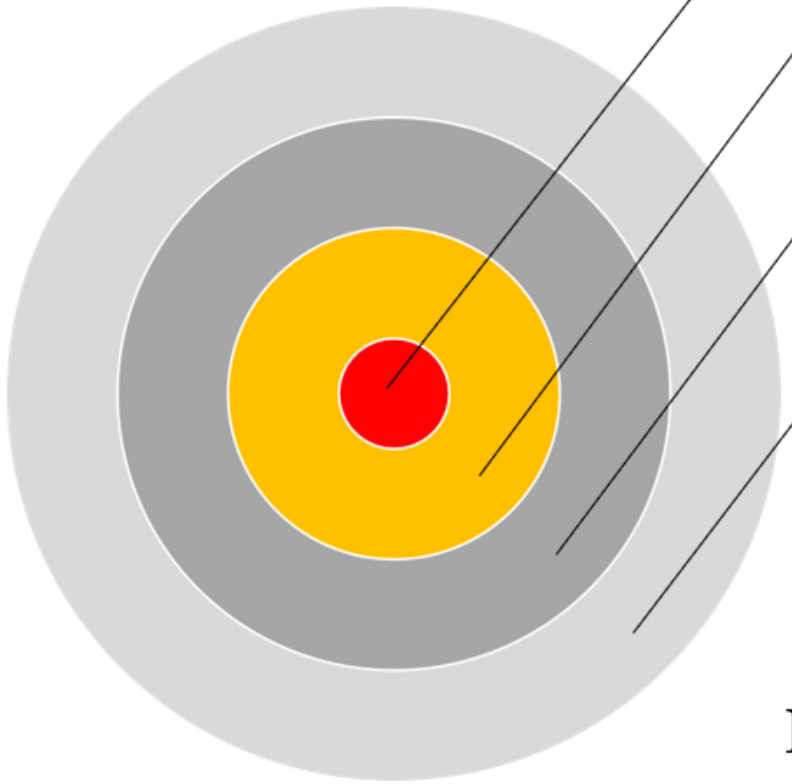
SOC Vibility Triad by Gartner

Holistic SOC Process in a Flow



Source : https://www.sans.org/webcasts/faster-better-cheaper-improving-security-operations-open-source-tools-112900/

SOC Data Funnel



Things have been qualified as bad (incidents)

Things that *might* be bad (alerts)

Everything you can see (events)

ALL activity

3. Investigation → 4. I.R.

2. Detection

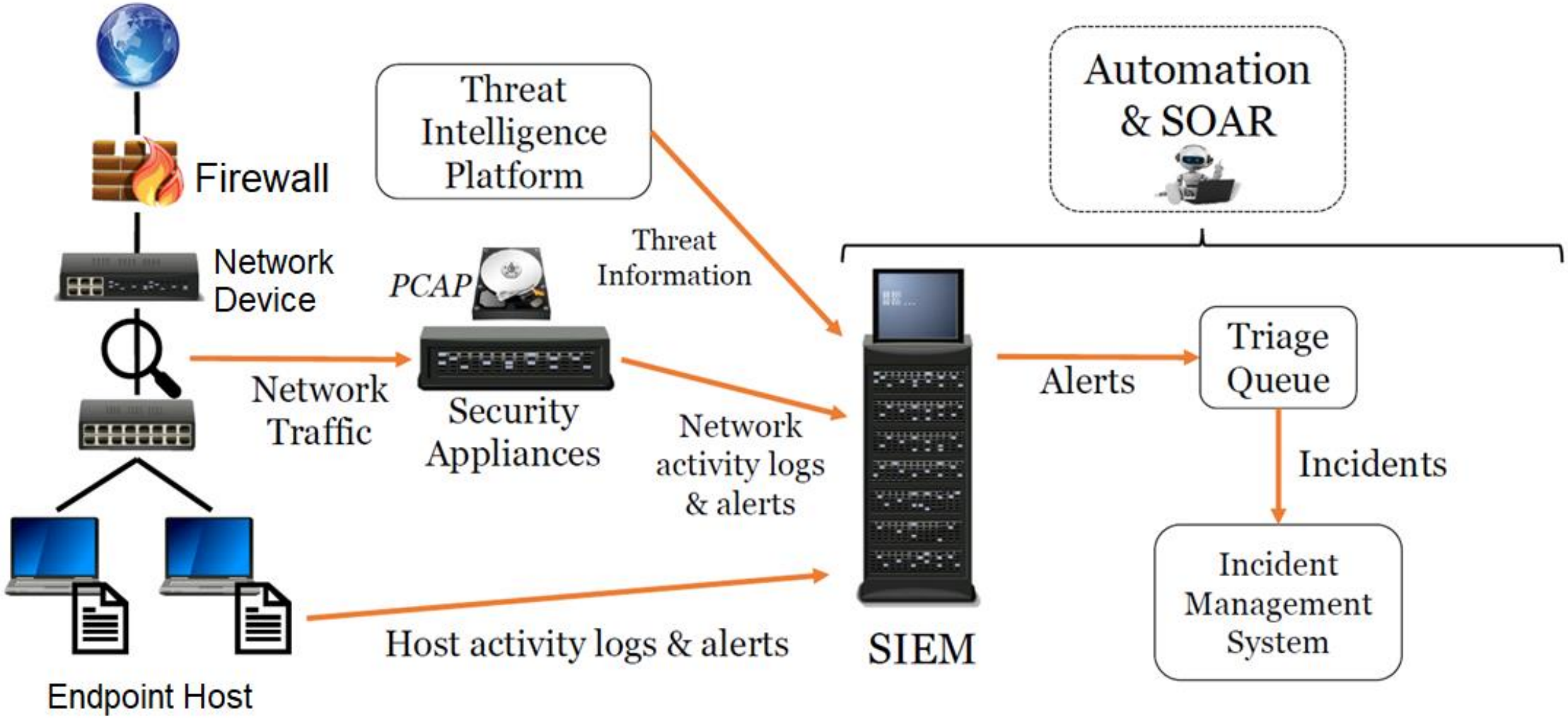
1. Collection

Items that aren't captured in earlier stages won't make it to later stages

In other words: Good collection is VERY important

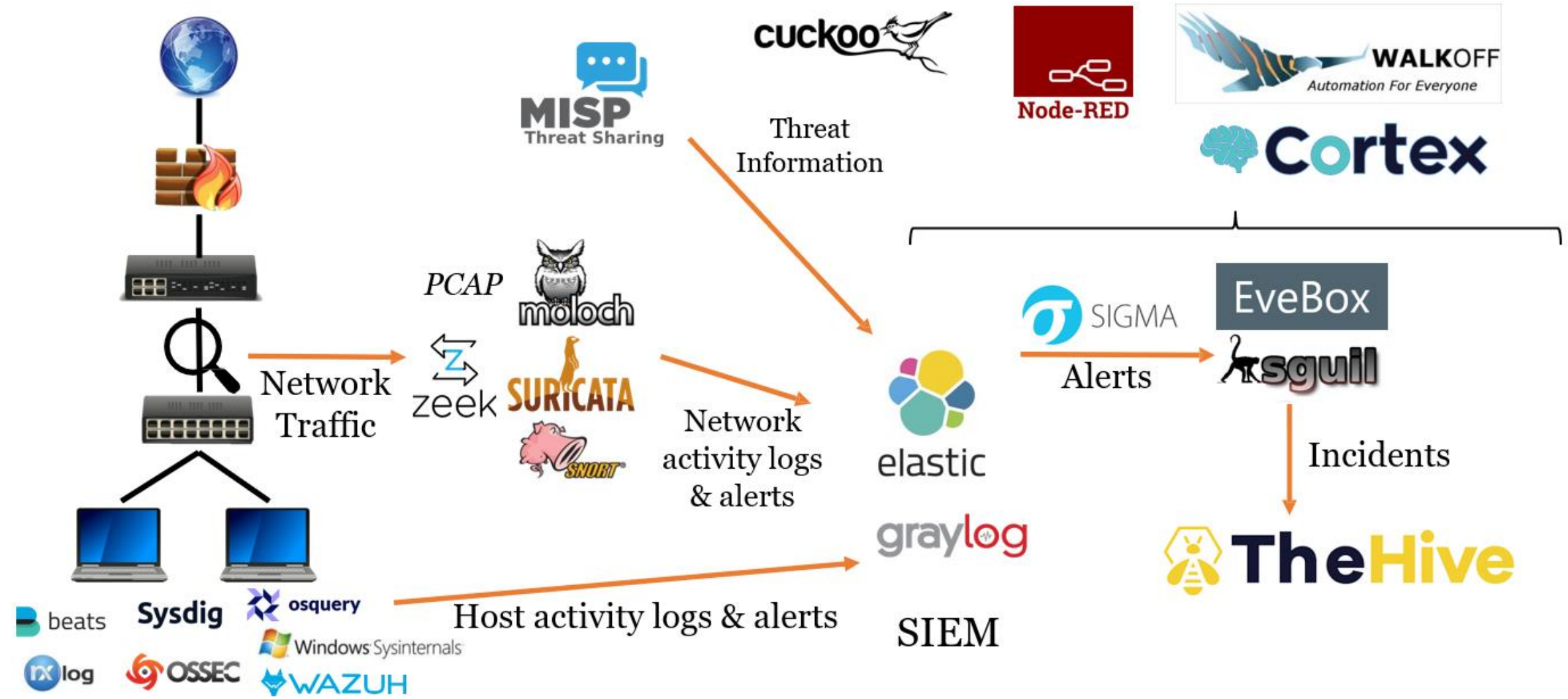
Source : https://www.sans.org/webcasts/faster-better-cheaper-improving-security-operations-open-source-tools-112900/

Technology dan Data Flow Dalam Blue Team



Source : https://www.sans.org/webcasts/faster-better-cheaper-improving-security-operations-open-source-tools-112900/

Solusi Open Source Full Stack

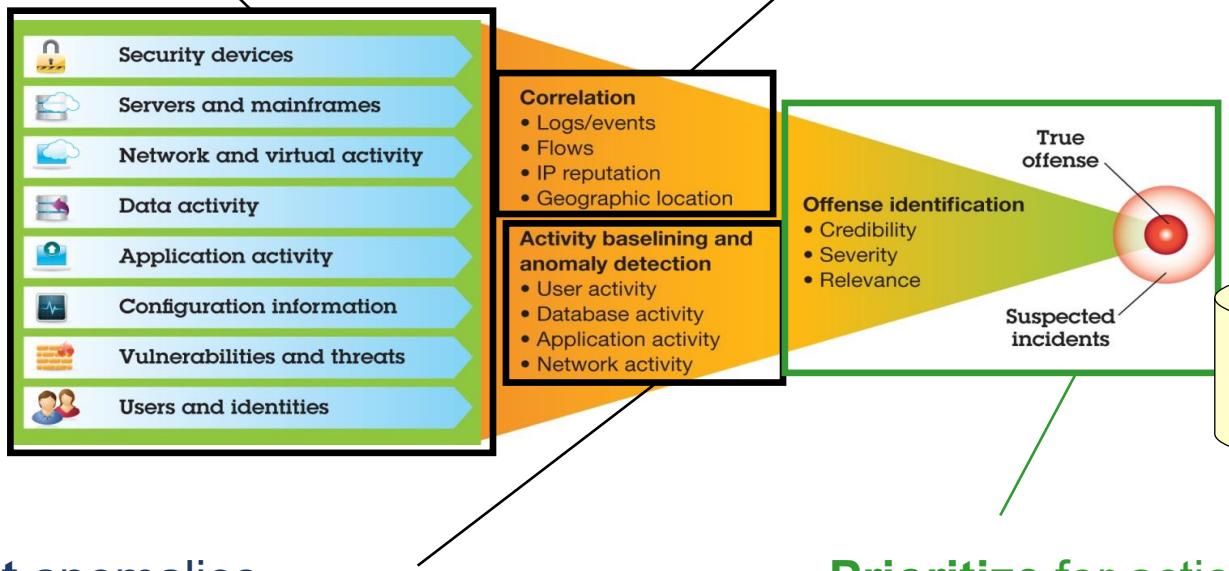


Source : https://www.sans.org/webcasts/faster-better-cheaper-improving-security-operations-open-source-tools-112900/

Cyber Security Operation Architecture

Monitor everything
Logs, network traffic, user activity

Correlate intelligently
Connect the dots of disparate activity



Detect anomalies
Unusual yet hidden behavior

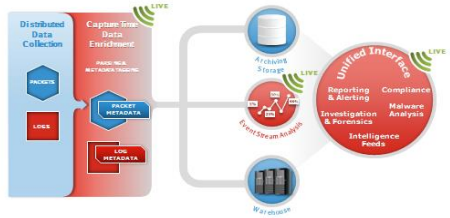
Prioritize for action
Attack high-priority incidents

Threat Intelligence

Internal	External
• Logs • Contextual Data • Vulnerability Assessments • Asset Inventories • Reports and Analytics	• XFORCE • CrowdStrike • SecureWorks • Deepsight

Threat Ingestion - Structured Threat Information eXpression (STIX™)

SIEM Environment



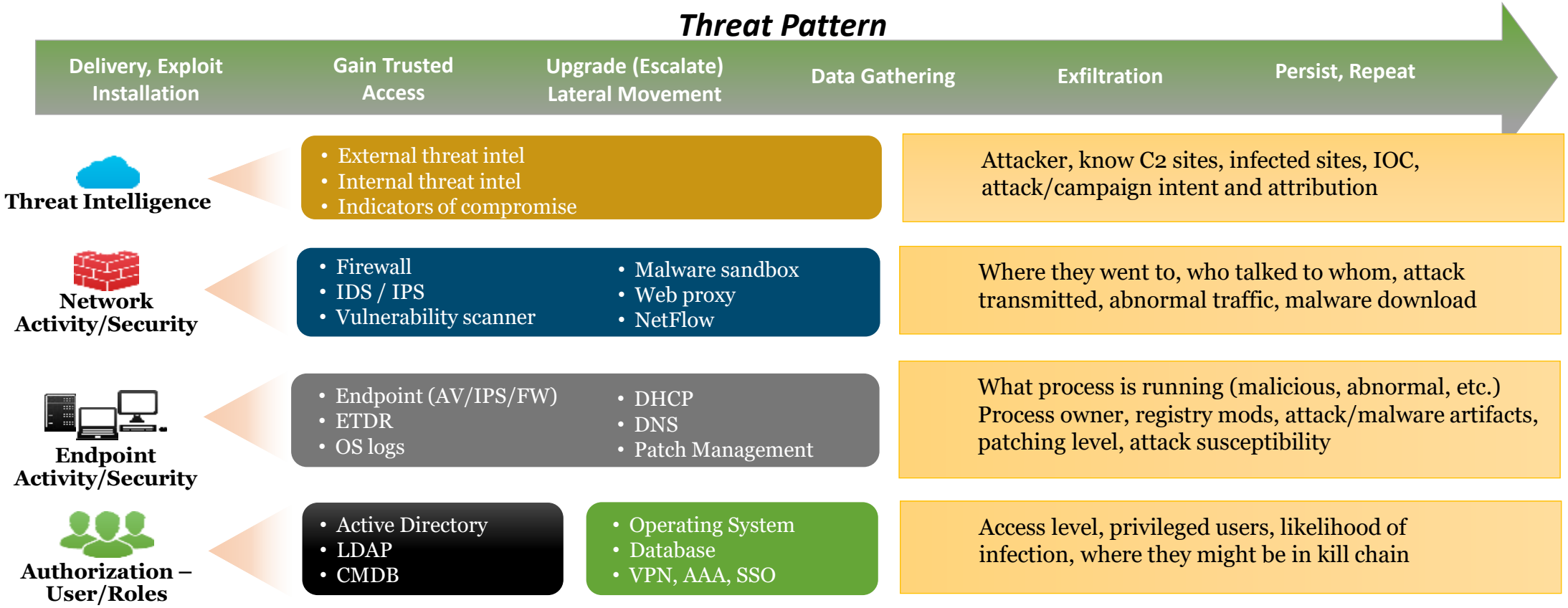
Machine Learning – Analytics
Artificial Intelligence

Single, Unified and Integrated Management Console

Incident Management Automation

*** Source - IBM**

Connecting Dots



*** Source - IBM**

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.

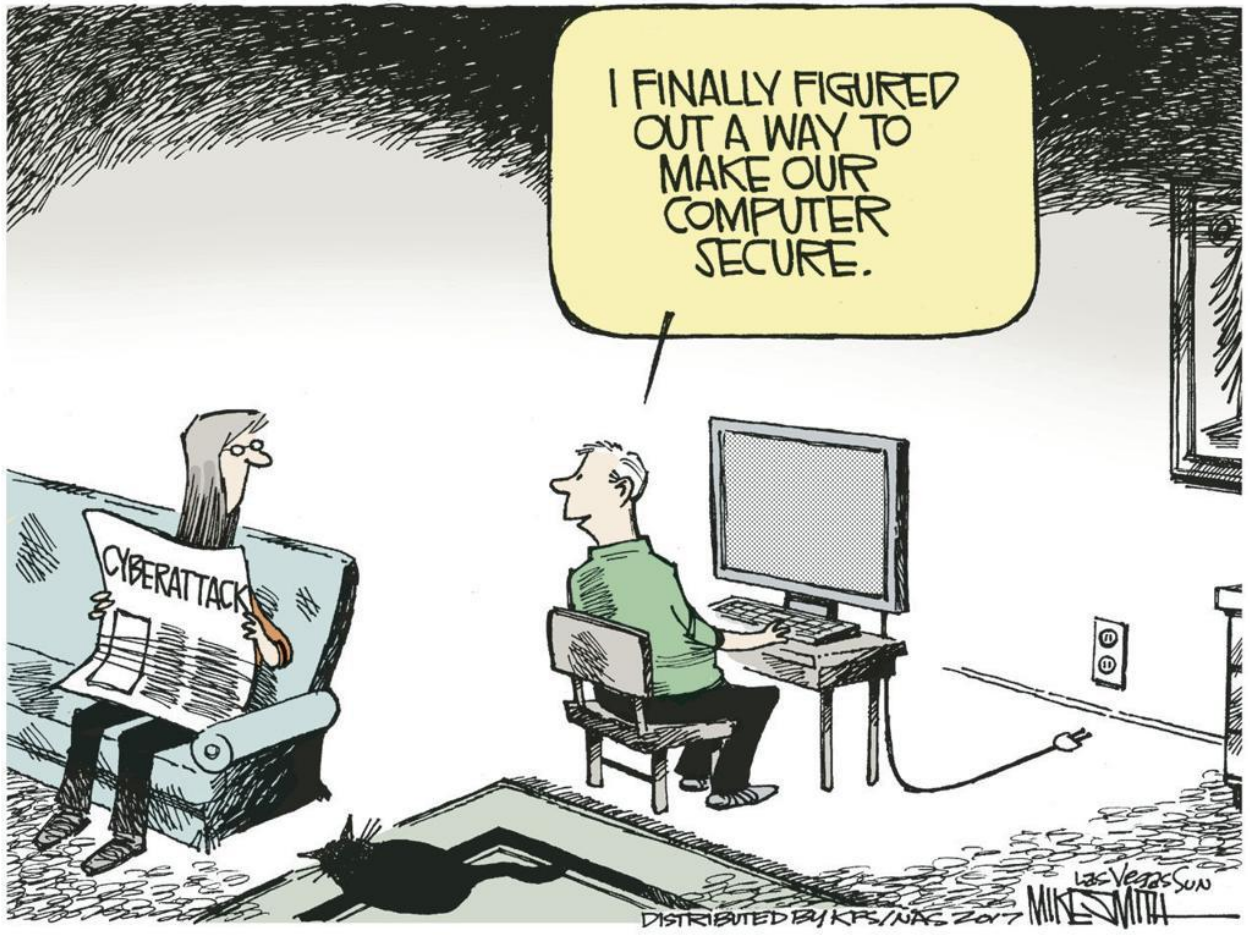
Analysis

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

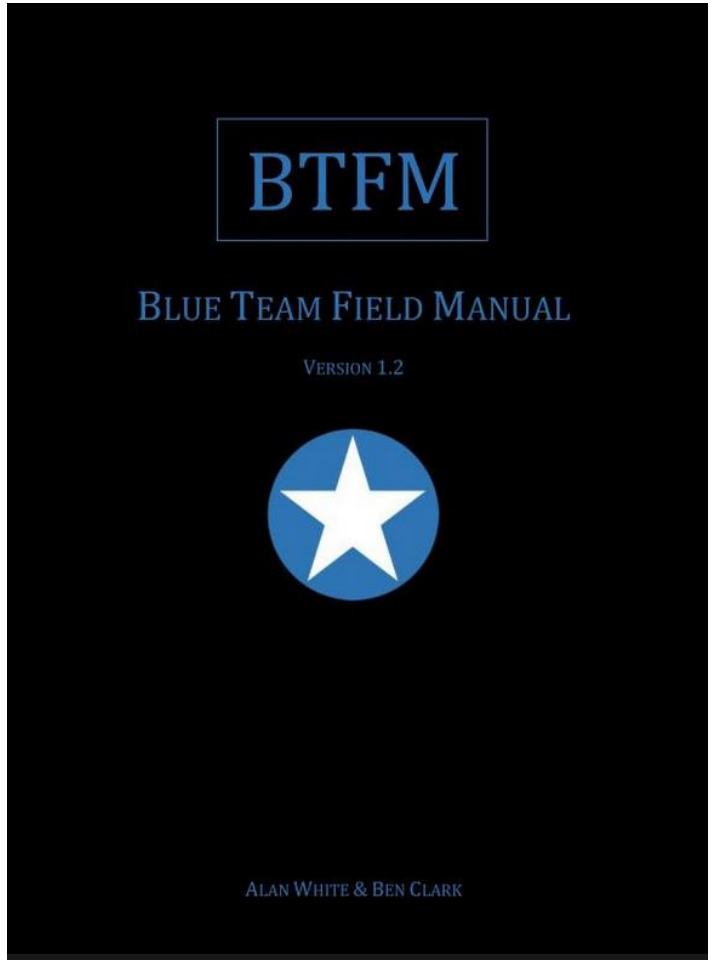
Action

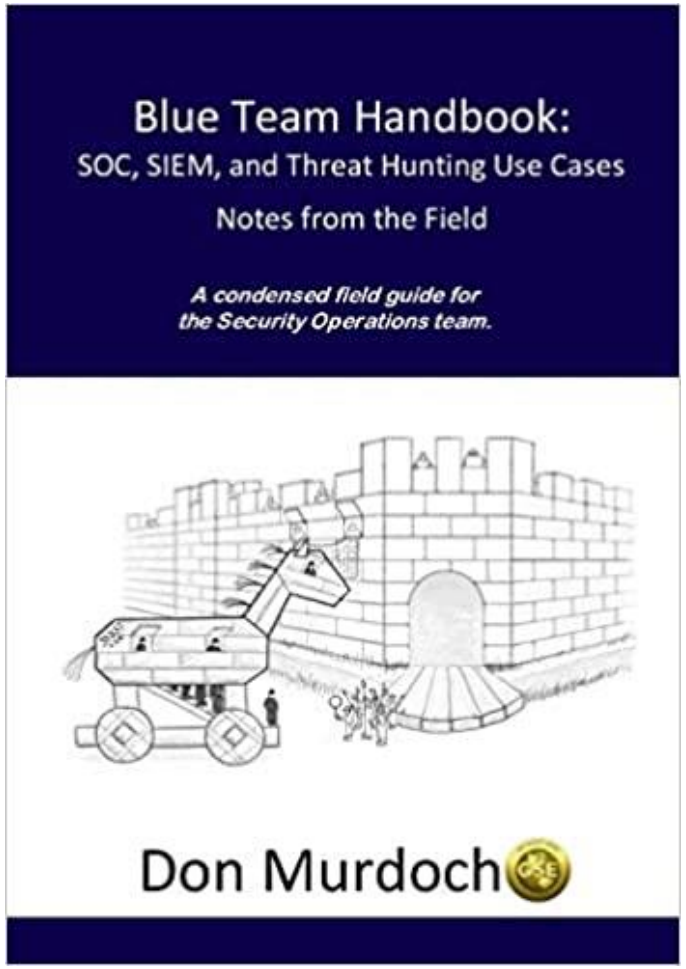
Based on findings, automated and manual interventions can be made to include patching, firewall modification, system quarantine or reimage, and credential revocation.

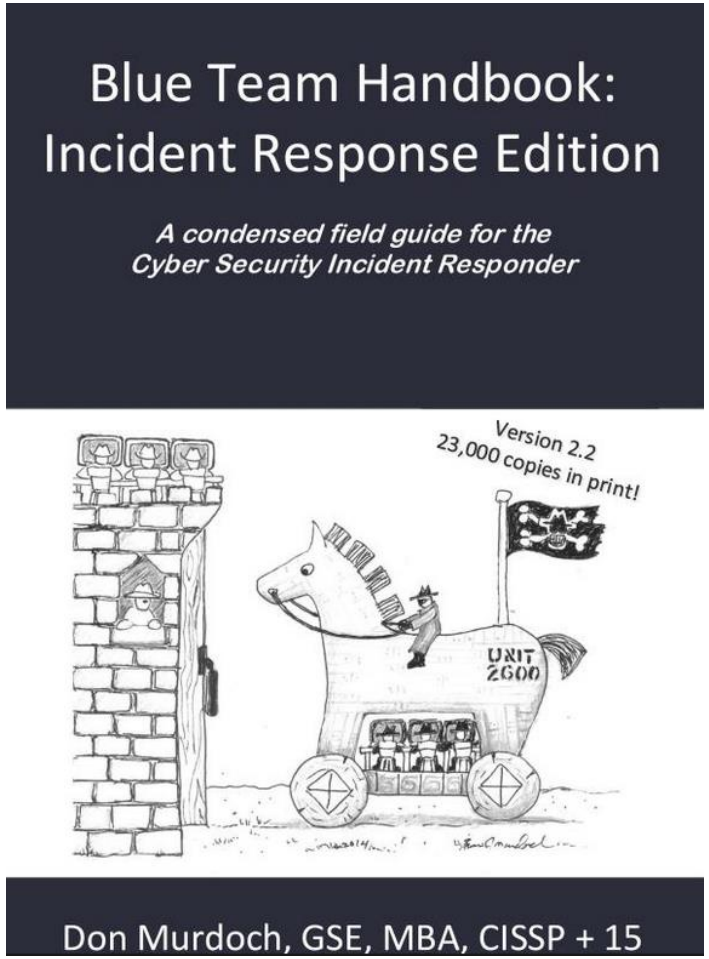
Finally


I FINALLY FIGURED OUT A WAY TO MAKE OUR COMPUTER SECURE.
CYBERATTACK
DISTRIBUTED BY KFS/NAS 2017
LAS VEGAS SUN
MIKE SMITH

Books Recommendation







Summary

- Tren ancaman keamanan siber semakin kompleks, dan banyak yang mengarah kepada serangan yang *targeted* terhadap organisasi dan juga individu tertentu
- Organisasi perlu mengingkatkan kapabilitas dalam defensive security untuk mendeteksi, serta memproteksi adanya kemungkinan adanya Compromise Incident dari aplikasi, OS, DB dan infrastruktur
- *Threat Actor* berevolusi dengan berbagai macam Tactic Technic serta Procedure, oleh karena itu, organisasi juga harus berevolusi dan menaikkan kapasitas cyber resiliency
- Visibilitas organisasi terhadap keseluruhan infrastruktur di dalam organisasi sangat penting. Tanpa adanya visibilitas, tidak akan bisa memiliki kapabilitas deteksi dengan baik.
- SOC adalah bagian penting dari organisasi, dan bagian fundamental dari SOC ini adalah bagaimana organisasi memiliki fungsi deteksi yang mumpuni
- SOC tanpa deteksi dan tanpa visibilitas tidak akan bisa bekerja dengan baik.
- Detection Engineering menjadi pionir untuk membangun kapabilitas deteksi di dalam organisasi. Role Detection Engineer juga menjadi semakin penting dan dibutuhkan oleh organisasi

THANK YOU
Q & A