
# The role of Security Operation Center to improve Cyber Resilience

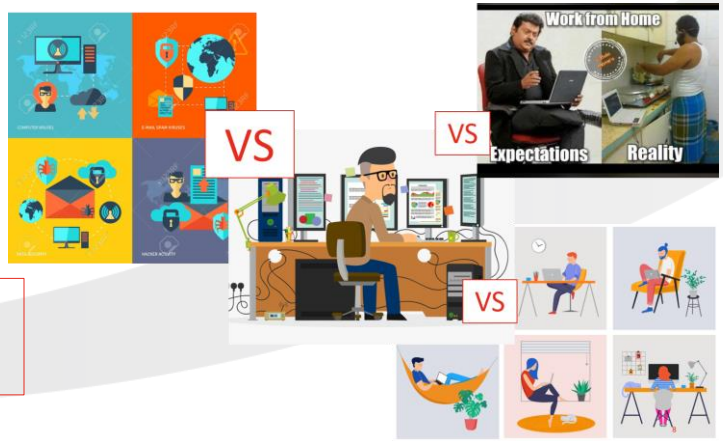
Focus Group Discussion: Membangun Kesadaran Keamanan Siber

Dr. Toto A Atmojo, CISSP, CISA


# Focus Group Discussion: Membangun Kesadaran Keamanan Siber

# Cyber Security: Unfair battle*

- Most software is poorly written and insecure
- Growing attack surface: From your IT crown jewels to IoT device
- Computerized system are getting more complex: Attack is easier than defense
- Interconnecting device: More vulnerability
- Computer Fail differently:
  - Distance doesn't matter.
  - Ability to attack is decoupled from skill needed
- During Covid-19: Battle of three frontlines




It is now commonly accepted that it's no longer a matter of '**if**' but '**when**' an organization will suffer a cyber attack.

*Schneier, B. (2018), Click Here to Kill Everybody. W. W. Norton & Company

# Cyber Resilience:

## Definition & Why do we need it

**Resilience Definitions***

The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from **disruptions**. Resilience includes the ability to **withstand** and **recover** from deliberate **attacks**, accidents, or naturally occurring threats or incidents.

**Cyber Resilience****

the ability of an organization to **prepare**, **respond**, and **recover** when cyberattacks happen

An organization **has cyber resilience** if it can **defend** itself against these attacks, **limit the effects** of a security incident, and guarantee the **continuity of its operation** during and after the attacks.

Cyber Security + Business Resilience = Cyber Resilience***

* Presidential Policy Directive (PPD-21) - Critical Infrastructure Security and Resilience

** https://blog.rsisecurity.com/what-is-cyber-resilience-and-why-is-it-important/

*** https://en.wikipedia.org/wiki/Cyber_resilience

# Digging into more detail

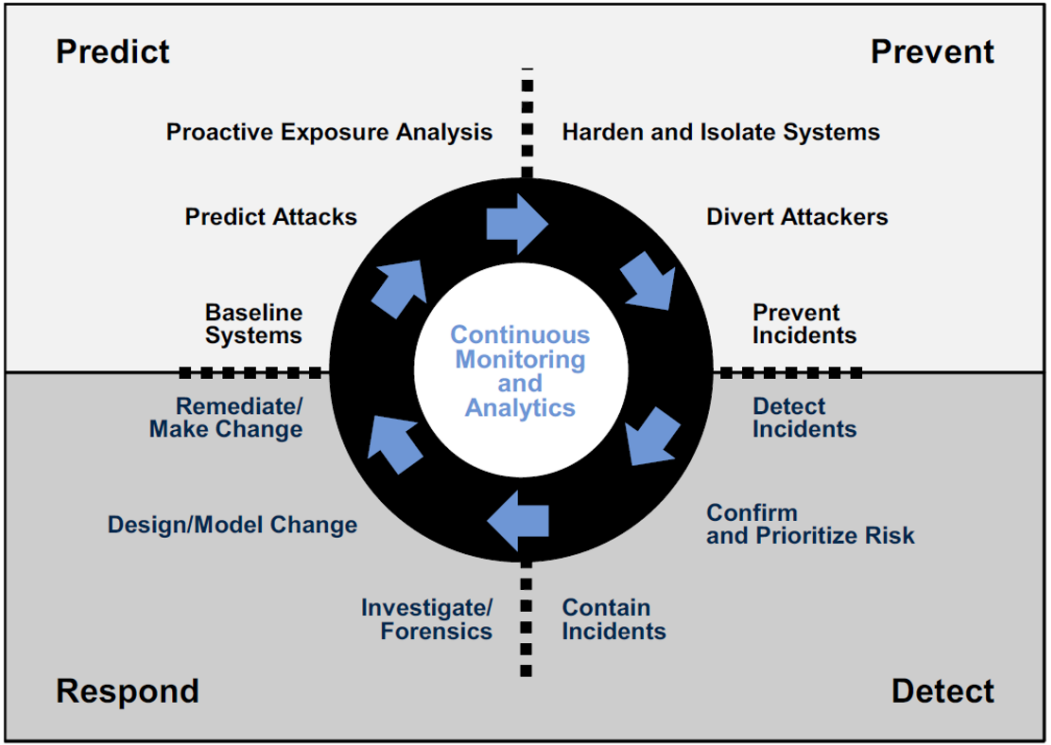
| | Before | | | | | | | | | During | | | After | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Strategy Development | Assets | | | Vulnerabilities | | | Threats | | | Attacks | | | Breaches | | | Impacts | | | | | | |
| | Digital | Discover | Classify | Design | Discover | Remediate | Political | Predict | Prevent | Access | Detect | Respond | Confidentiality | Confirm | Recover | Operational | Avoid | Accept | Transfer | Mitigate | | |
| | Physical | | | Implementation | | | Economic | | | Copy | | | | | | Physical | | | | | | |
| | | | | | | | Social | | | Theft | | | Integrity | | | Personal | | | | | | |
| | | | | Operation | | | Technological | | | Modification | | | | | | Legal | | | | | | |
| | Social | | | | | | Environmental | | | Disruption | | | Availability | | | Reputational | | | | | | |
| | | | | Management | | | Legal | | | Destruction | | | | | | Financial | | | | | | |
| | Asset Management | | | Vulnerability Management | | | Threat Management | | | Incident Management | | | Continuity Management | | | Crisis Management | | | | | | |
| | Risk Management | | | | | | | | | | | | | | | | | | | | | |
| Strategy Execution | People | | | | | | | | | | | | | | | | | | | | | |
| | Process | | | | | | | | | | | | | | | | | | | | | |
| | Technology | | | | | | | | | | | | | | | | | | | | | |
| | Communication | | | | | | | | | | | | | | | | | | | | | |


* The Security Artist: Journey to cyber resilience

# Another (More Common) Architecture*

Gartner Recommendation:

Develop a security operations center that supports **continuous monitoring** and is responsible for the continuous threat protection process



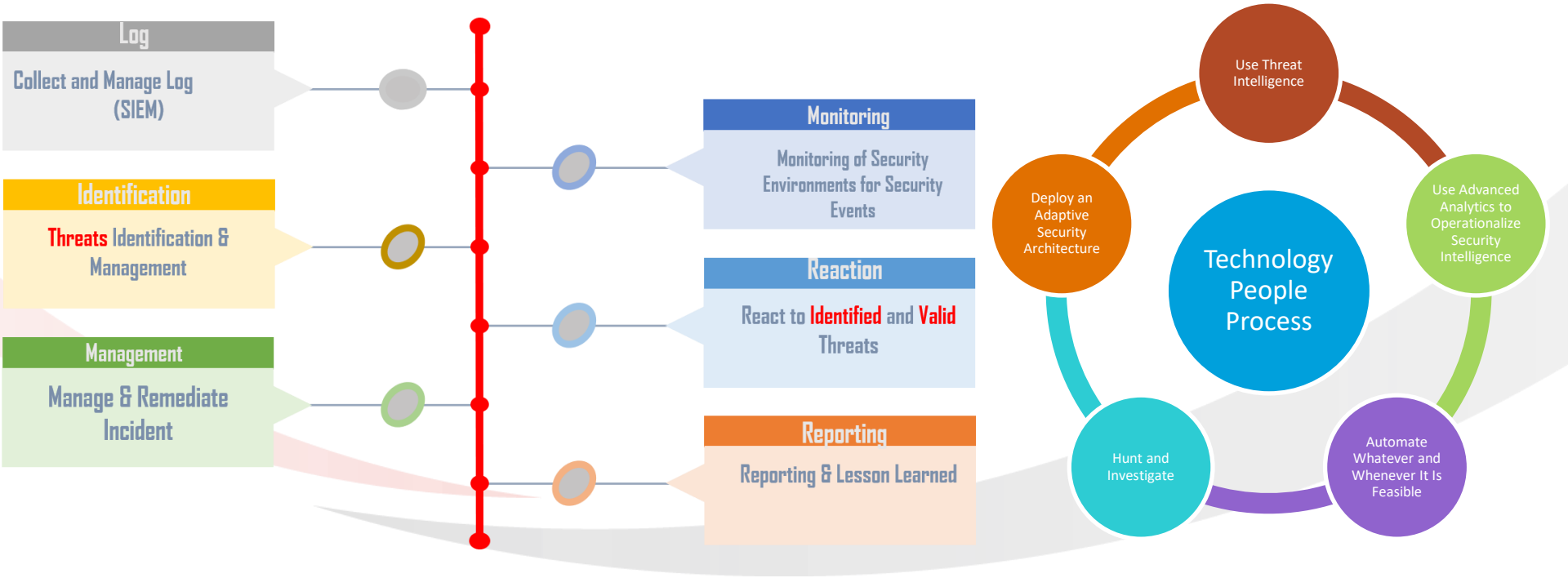

*Gartner "Designing an Adaptive Security Architecture for Protection From Advanced Attacks"

# Security Operation Center*

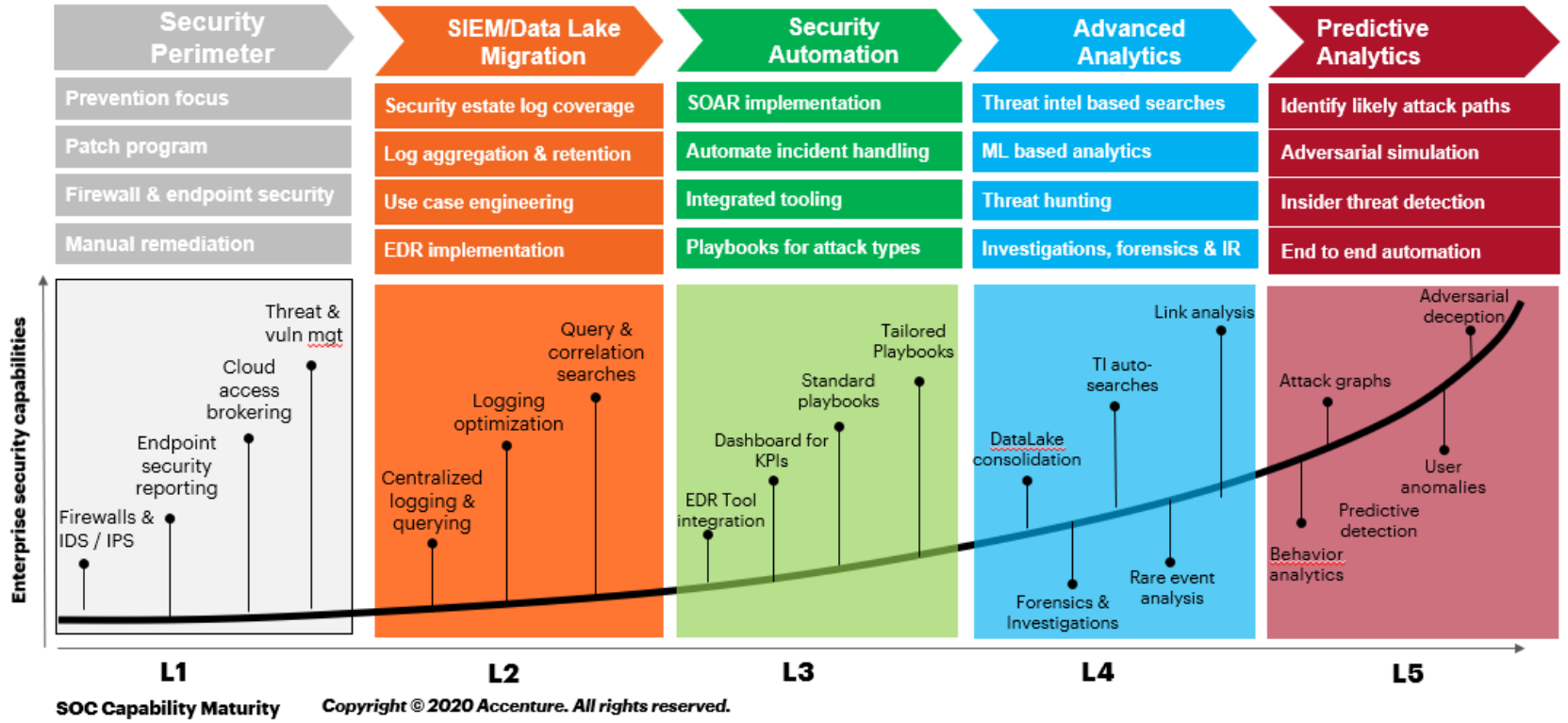
"‥ a centralized security organization that assists companies with **identifying**, **managing** and **remediating** distributed security attacks."


* Jacobs, P., Arnab, A., & Irwin, B. (2013). Classification of Security Operation Centers. 2013 Information Security for South Africa, 1–7. http://doi.org/10.1109/ISSA.2013.6641054

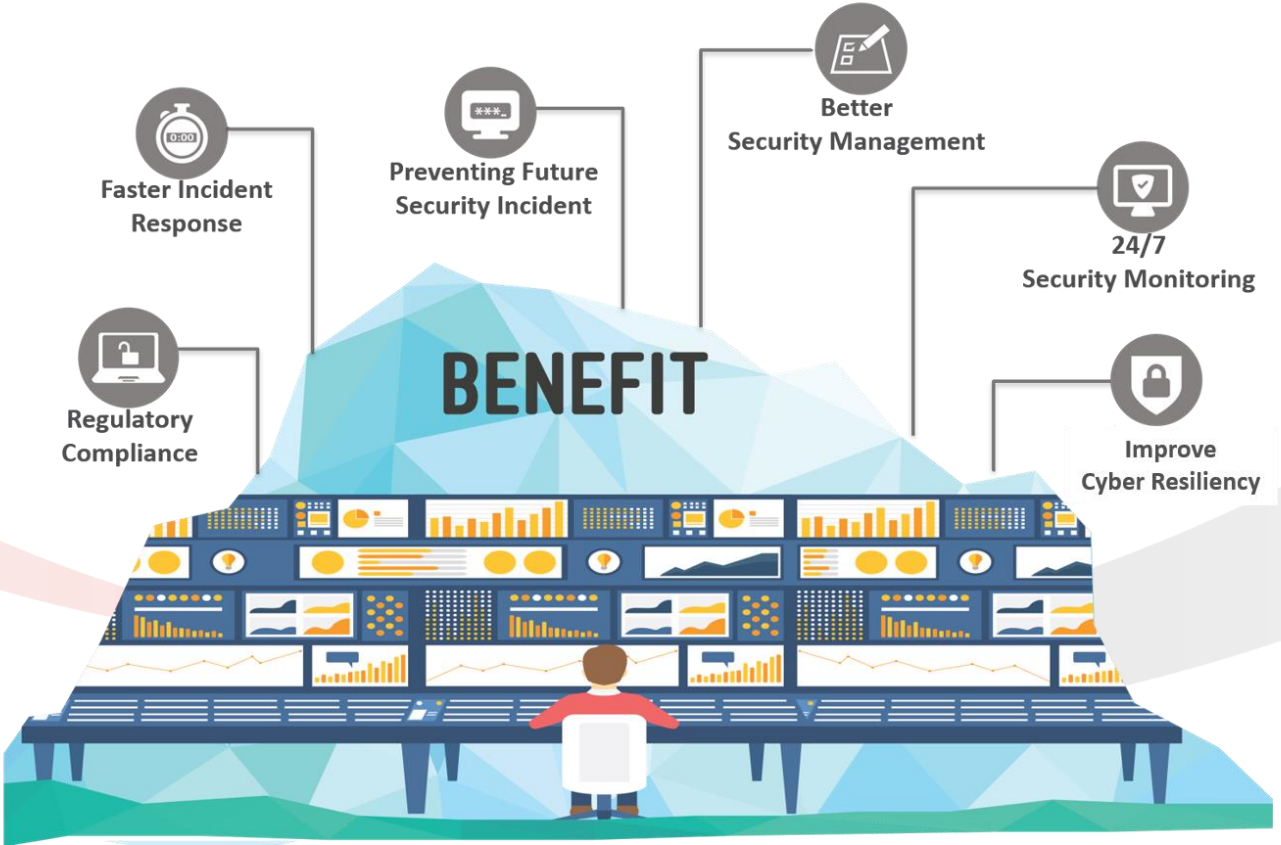
# SOC Characteristics & Intelligence-Driven SOC



# SOC Maturity Level



# SOC Benefit: Above the surface



# SOC Challenge: Bellow the surface

# Internal Development vs Outsource Self Assessment (Min score: 15)*

Build and operate SOC is a BIG Challenge to maintain it's Technology, People & Process.

If your organization is not ready, then leave it to the expert using MSSP model.

| Item | What | Answer | Points |
|---|---|---|---|
| 1 | Give yourself 1 free point because you will have an incident at some point in time. | | 1 |
| 2 | Has your constituency detected an incident that had a measurable impact on the mission or came at a significant cost within the last six months? | | |
| 3 | Is there a perception that your constituency faces a targeted external cyber threat beyond the normal Internet-based opportunists such as script kiddies? | | |
| 4 | Does your constituency serve a high-risk or high-value business or mission *and* is that mission heavily dependent on IT, such as finance, healthcare, energy production, or military? | | |
| 5 | Does your constituency offer IT services to directly connected third parties in a B2B, B2G, or G2G fashion? | | |
| 6 | Does your constituency serve sensitive or privacy-related data to untrusted third parties through some sort of public-facing portal such as a Web application? | | |
| 7 | Does your constituency retain sensitive data provided or owned by a third party, such that the constituency faces significant liability if that data is stolen or lost? | | |
| | **Subtotal** | | |
| | How many thousands of hosts are in your constituency? | | |
| | Multiply the subtotal by the number of thousands of hosts in your constituency. This is your total. | | |

** C. Zimmerman. Ten strategies of a world-class cybersecurity operations center. MITRE Corporation report release, USA, 2014.*


# Thank You

www.defenxor.com