Challenges in Cybersecurity Implementation

How to address
How to respond
to THREAT

By A. Rully

- Security Related

Word Cloud

Five Level of Addressing Threat

Level 0: Instinct	Level 1: Basic	Level 2: Analysis
Level 3: Extended	Level 4: Center	Level 5: AI

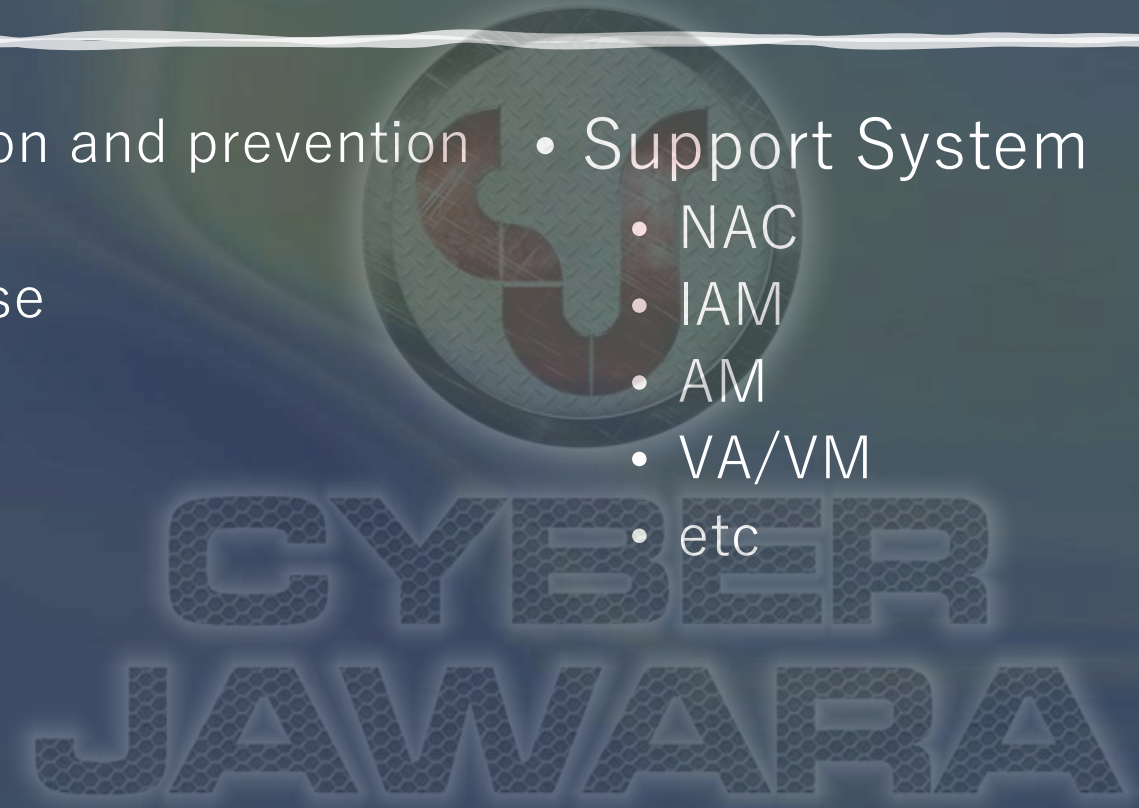
L0: Human Instinct

- Living in digital world, but:
  - Unaware of the risk
  - Aware but don’t care
  - Aware and prepare something
  - Just live up with the risk

CYBER JAWARA

L1: Basic Security

- Malware detection and prevention
  - Anti-Virus
- Perimeter defense
  - FW
  - IDS
  - WAF
  - IPS
  - Anti-DDOS
  - etc
- Support System
  - NAC
  - IAM
  - AM
  - VA/VM
  - etc



L2: Analysis of Security Related Information

- Log analysis (segmented/individual)
  - syslog, winlog, any log that have security implications
- Security Information and Event Management (SIEM)
  - Gather all log and information related to security

L3: Extended Detection & Response

- Incident Response (start from Morris Worm)
  - First CSIRT in Carnegie University in 1988
- Extended Detection and Response (XDR)
  - Endpoint Detection and Response (EDR)
  - Network Detection and Response (NDR)

L4: SCC (Security Command Center)

- Consolidate threat hunting with human analysts
  - Attack vector mapping
  - Attack Detection
  - Malware analysis
- Center for Incident Detection and Response
- Security components are coordinated and orchestrated
- Some parts are automated

L5: Goes AI (ML)

- AI help security/incident analyst
  - Augment human analysis: Generative AI ((LLM)
  - Automated defense
- Fully AI (when?)
  - Arm race with attacker

CYBER JAWARA

Which level are you?