War Games

Cyber-Defense is a Game

Stefan Pfeiffer, Mikail Bulduk,
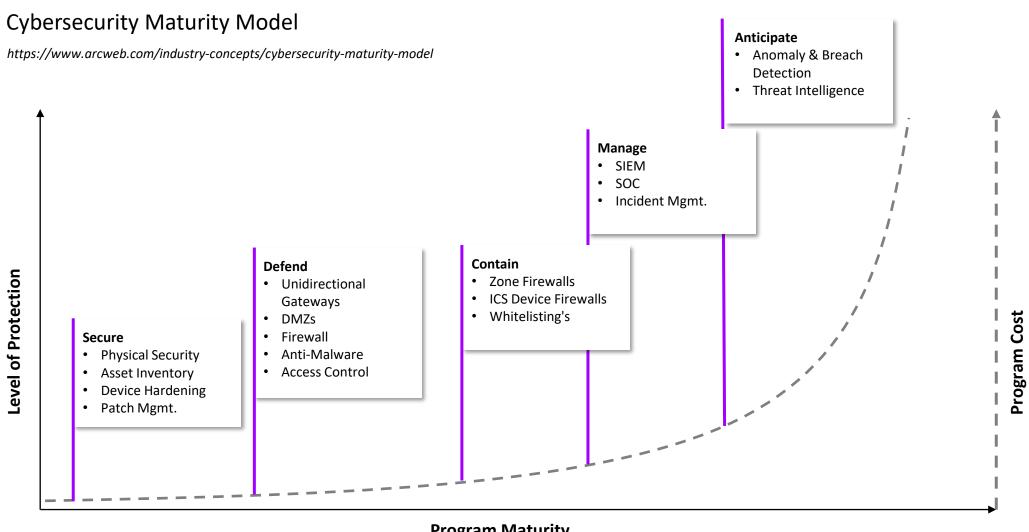Alexander Tauber

7.10.2022

Increasing number
of participants

Growing complexity
for security

Implementation
time flaw

Cybersecurity Maturity Model

https://www.arcweb.com/industry-concepts/cybersecurity-maturity-model

Level of Protection (y-axis)

Program Cost (right y-axis)

Program Maturity (x-axis)

Secure
- Physical Security
- Asset Inventory
- Device Hardening
- Patch Mgmt.

Defend
- Unidirectional Gateways
- DMZs
- Firewall
- Anti-Malware
- Access Control

Contain
- Zone Firewalls
- ICS Device Firewalls
- Whitelisting's

Manage
- SIEM
- SOC
- Incident Mgmt.

Anticipate
- Anomaly & Breach Detection
- Threat Intelligence

Arbeiter: 10/16

6:35 / 11:39   Schneller

ESLRefereeA (3)

Menü

Incomplete   **Complete**
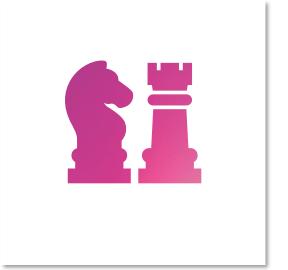
Imperfect

Perfect

- Management of own Resources (Macro)

- Control of Units and Positioning (Micro)

- Economy

- Ground, Air or Stationery Units

- Scouting and Map Awareness

- Order of Structure and Unit building (Build Order)

- Security Maturity and Coverage

- Implementation of Cyber Security

- Company Core Processes

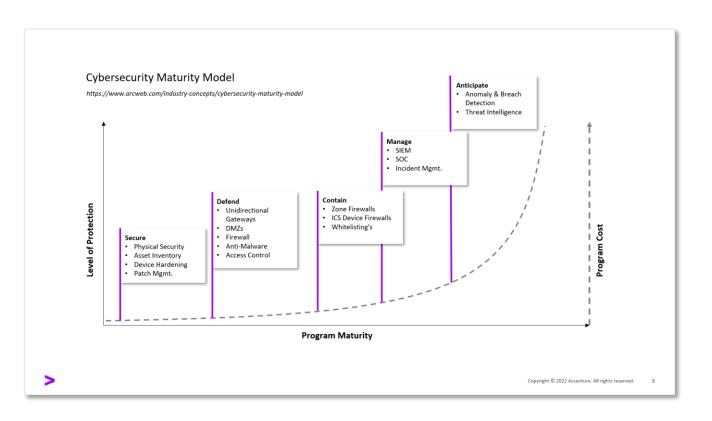- Security Resources

- CTI

- Cyber Defense Maturity Model

- Scouting is key

- Possibility of a Rush opponent must always be taken in mind with every decision

- Focus on defense only will make an impact on the economy

- **Surviving a Rush increase the winning rate**

- Understanding the Threat Landscape is key

- To be target of a campaign must always be considered

- **Common security measurements are more important than defending only against a „rush" attack like DDoS or certain Malware**

https://www.yumpu.com/en/document/view/50119227/starcraft-ii-build-order-visualizer-visualization-university-of-

Cybersecurity Maturity Model

https://www.arcweb.com/industry-concepts/cybersecurity-maturity-model

15

0

16/23

75

0

17/23

0:47 / 13:12   Schneller

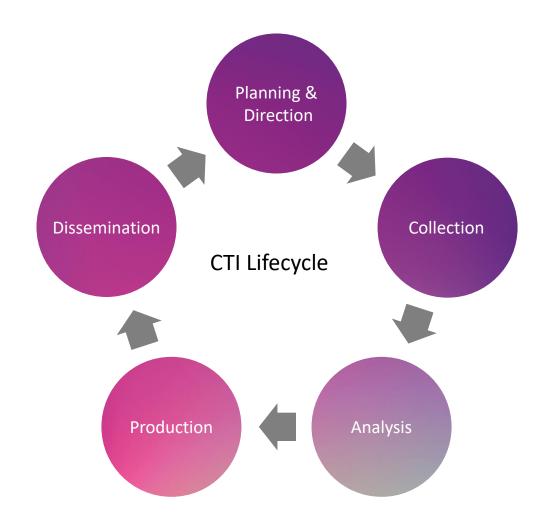herO (1)   Geschwindigkeit erhöhen (+)

Menü

Probe scouts a start build with one Refinery and around 50 gas are missing

Reaper Cost 50 minerals and 50 gas and are common first units in such build orders

CTI Lifecycle

- Planning & Direction
- Collection
- Analysis
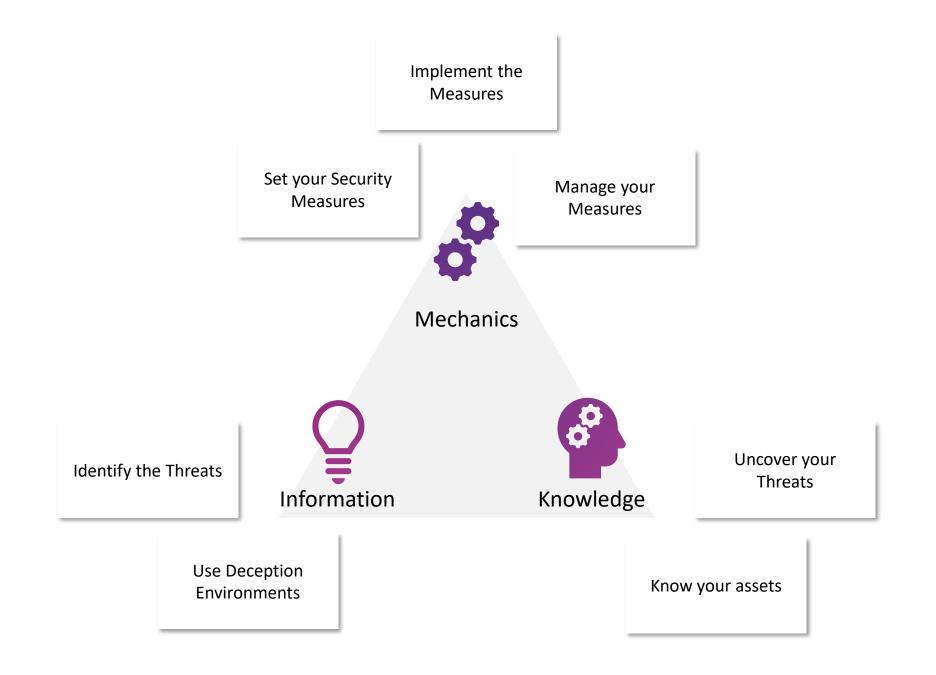- Production
- Dissemination

16

Mechanics

Knowledge

Information

> These three factors are limited by each other. Knowledge will have no meaning if you do not know how to put it into practice mechanically. Mechanics are pointless if your information on the situation is incomplete, and you do not know what to do or what to expect. Information only helps if you have experience in what it means and how to obtain it.
>
> *Team Liquid's Guide on how to improve in SC2*

Implement the Measures

Set your Security Measures

Manage your Measures

Mechanics

Identify the Threats

Information

Knowledge

Uncover your Threats

Use Deception Environments

Know your assets

VICTORY!

[ACN] Security

Score Screen

Return To Game

[All]

Computer Player 2

was defea

Thank You