Contents

DEFENSE –
DYNAMIC SECURITY STRATEGIES FOR AN UNCERTAIN FUTURE

1. ATTACKS IN AN UNCERTAIN WORLD
2. DO THE BASICS WELL
3. STATIC TO DYNAMIC DEFENSE
4. CSF
5. AI AND WHY YOU MAY WANT TO CLEAN UP YOUR ROOM…

Tobias Gondrom

- 20 years information security experience
  (Group CISO, Global Head of Security, CISO, CTO Security)
  CISSP, CSSLP, CCISO
- 15 years management of application and software development
- Sloan Fellow M.Sc. in Leadership and Strategy,
  London Business School
- OWASP former chairman & global Board member,
  OWASP Project Leader for the CISO Survey
  (www.owasp.org)
- Author of Internet Standards on Secure Archiving, CISO training and co-author of the OWASP CISO guide
- Former Chair of the IETF Trust, Chair of IETF WGs on Web Security, DDoS Open Threat Signalling, etc.
  Member of the IETF Security Directorate
- Cloud Security Alliance, Hong Kong chapter board member

1. Attacks in an uncertain world – “sophisticated” attacks vs.“sophisticated” defenses - really…?

Wannacry at the NHS

Maersk Chairman: “NotPetya attack totally destroyed Maersk's computer network”´
- up to $300 Million

2017: 465,000 pacemakers vulnerable to hacking, need a firmware fix

ZERO TRUST SECURITY

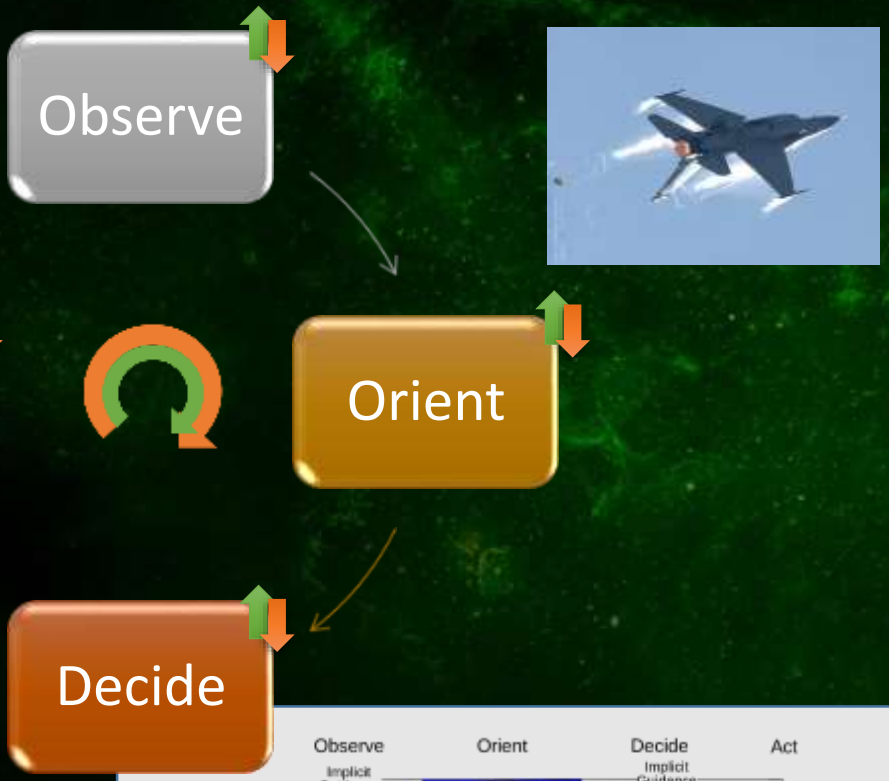
2. Do the basics well

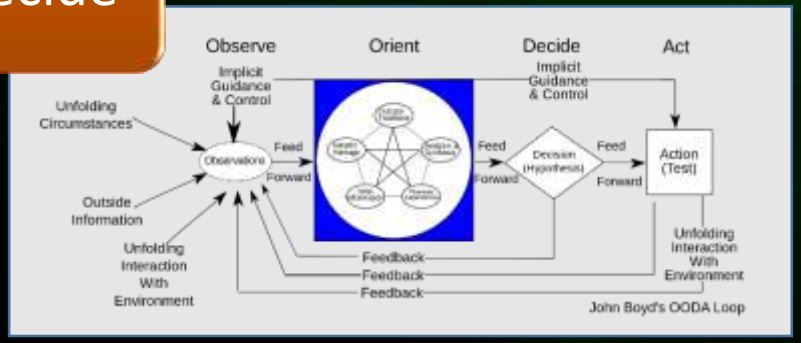
(sign in the gym above the weights…)

3. Dynamic Defense

- From static....

to dynamic...
OODA Loop

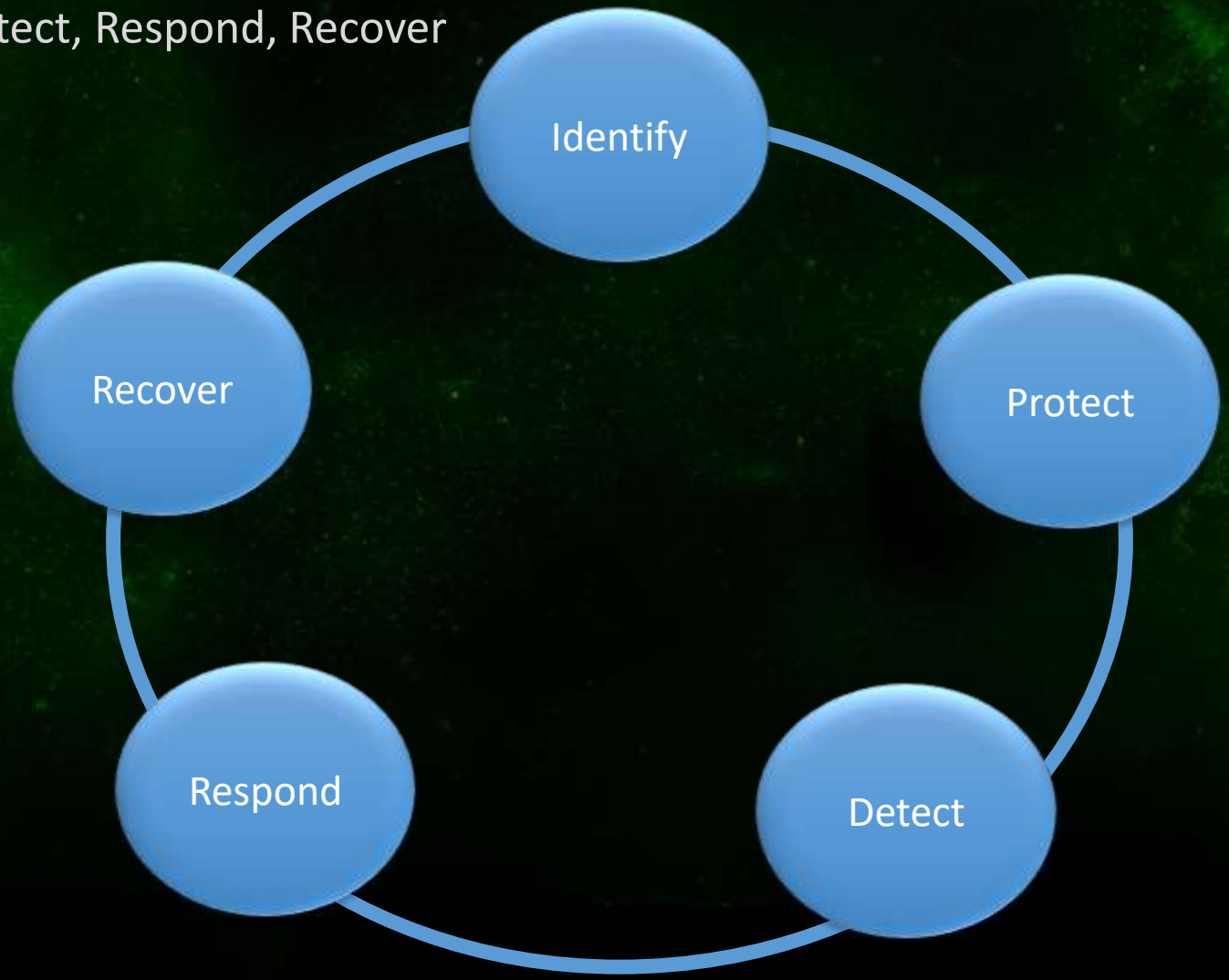




ZERO TRUST SECURITY

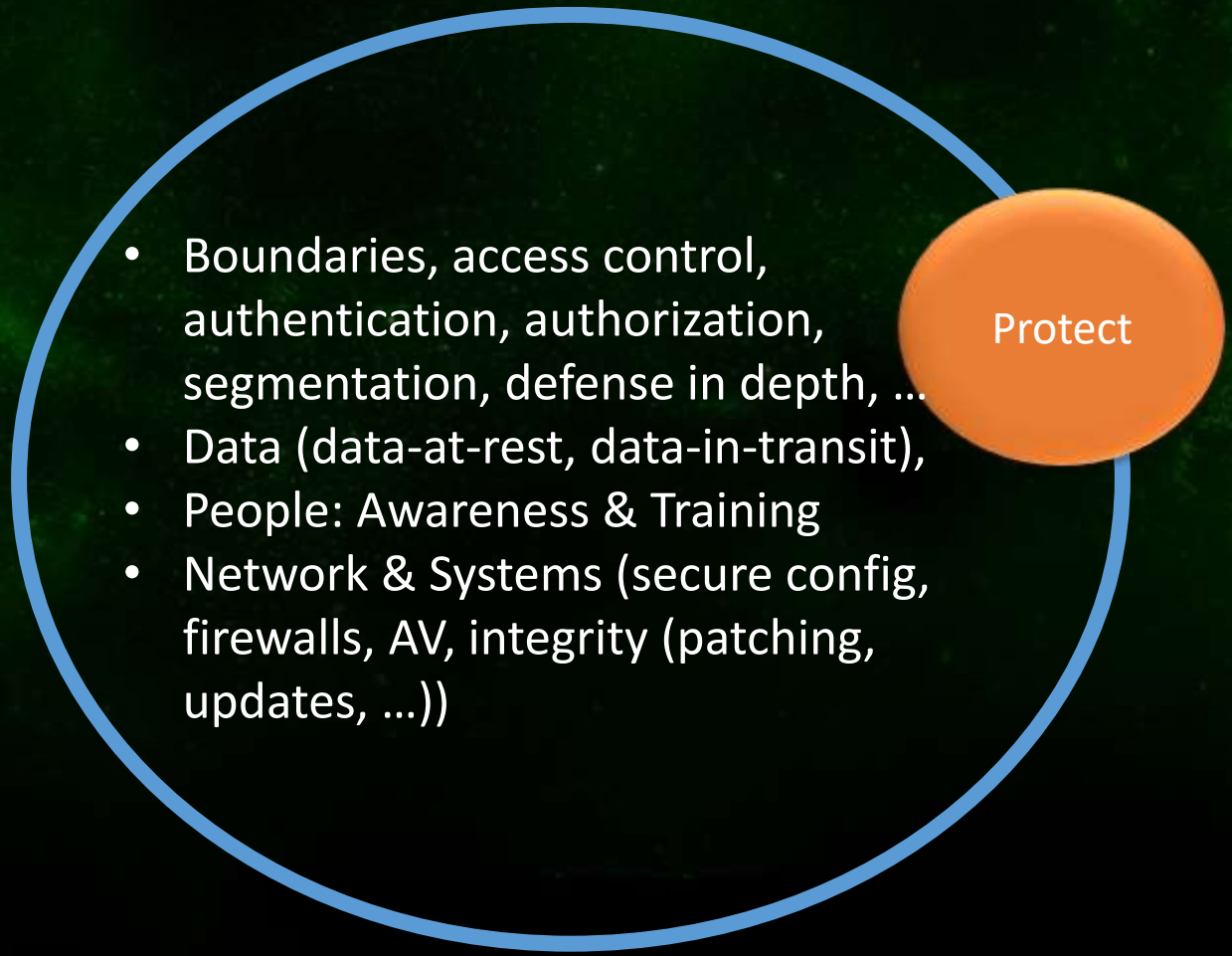
4. NIST Cyber Security Framework (1.1)

From Protect
=> Identify, Protect, Detect, Respond, Recover



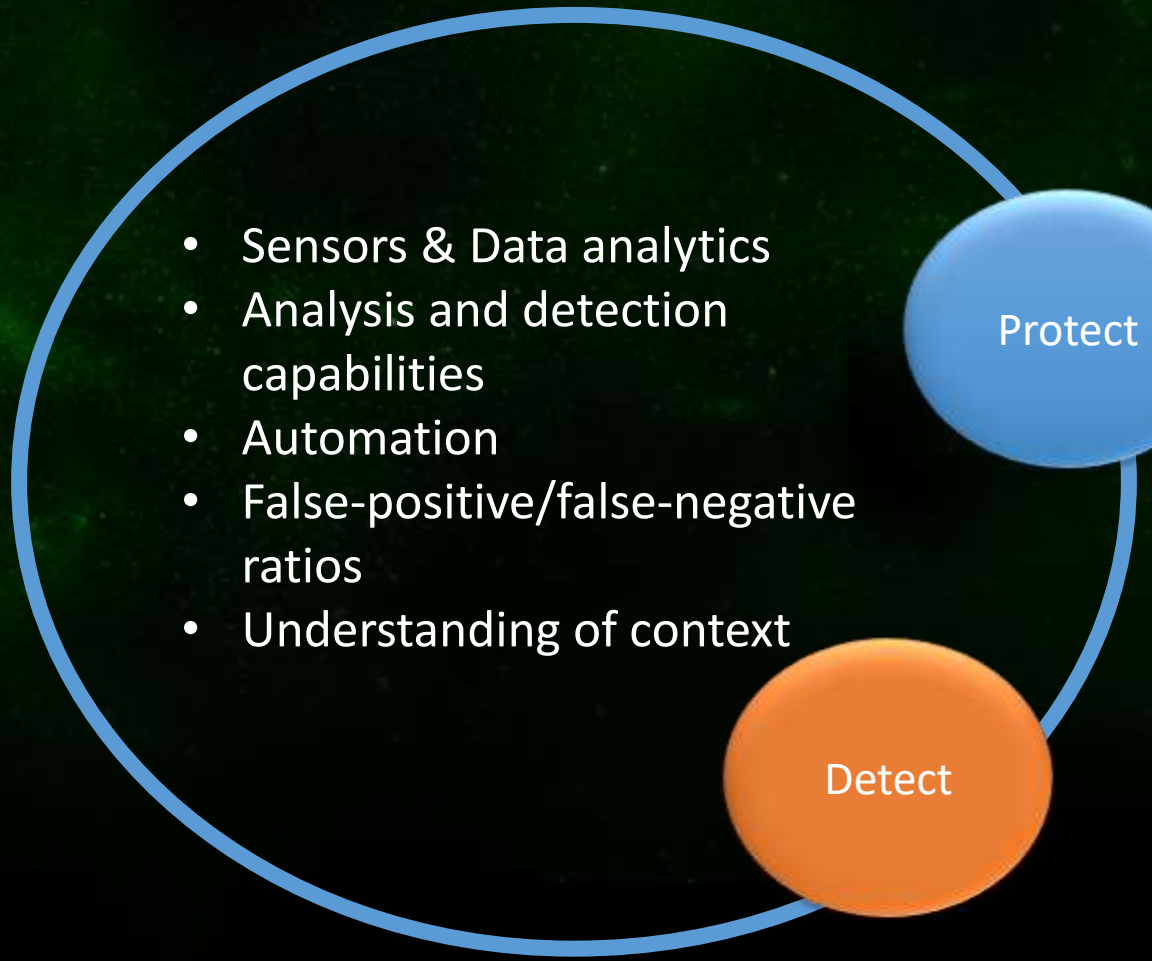
4. NIST CSF (1.1): what does this mean for us?

Add capabilities & investments from Protect
=> Identify, Protect, Detect, Respond, Recover



4. NIST CSF (1.1): what does this mean for us?

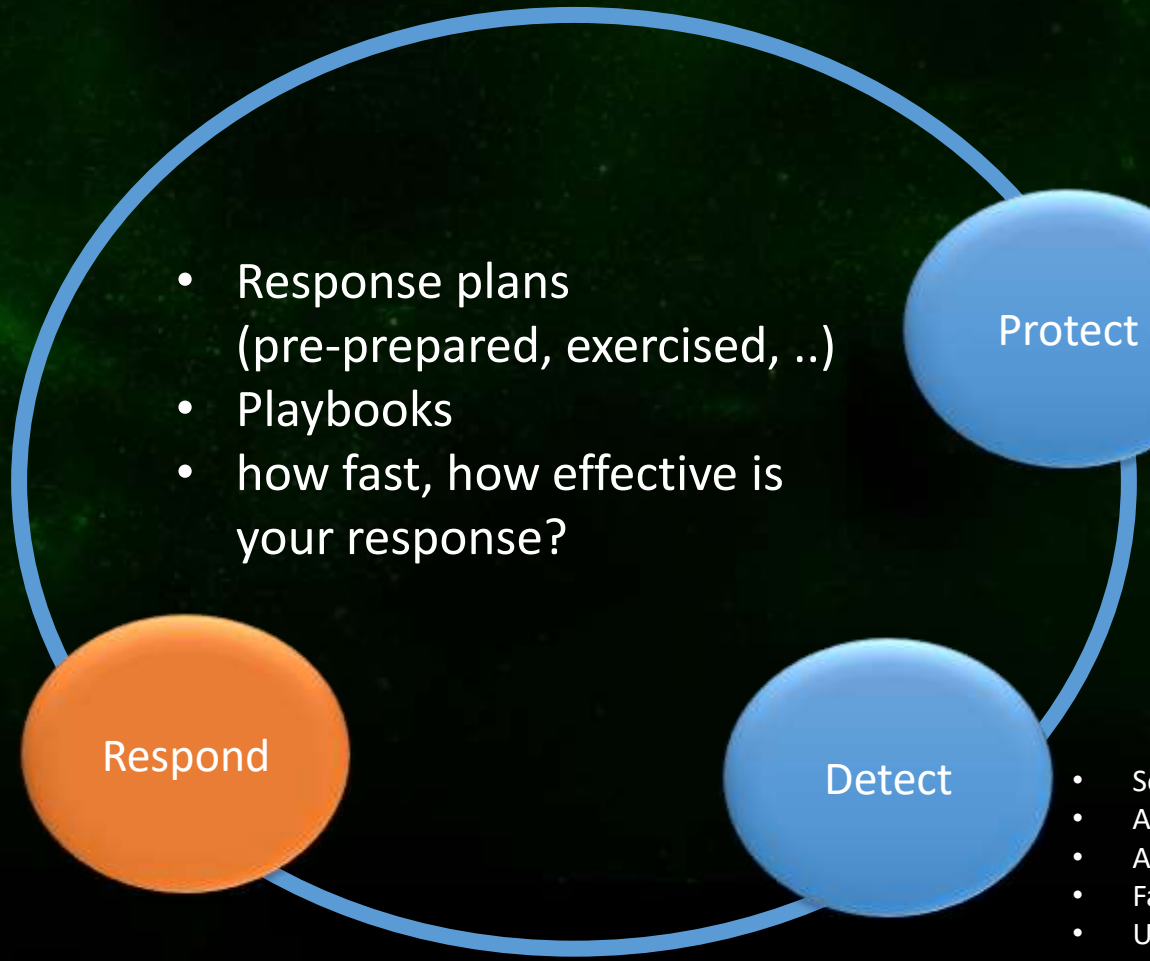
Add capabilities & investments from Protect
=> Identify, Protect, Detect, Respond, Recover



- Boundaries, access control, authentication, authorization, segmentation, defense in depth, …
- Data (data-at-rest, data-in-transit),
- People: Awareness & Training
- Network & Systems (secure config, firewalls, AV, integrity (patching, updates, …))

4. NIST CSF (1.1): what does this mean for us?

Add capabilities & investments from Protect
=> Identify, Protect, Detect, Respond, Recover



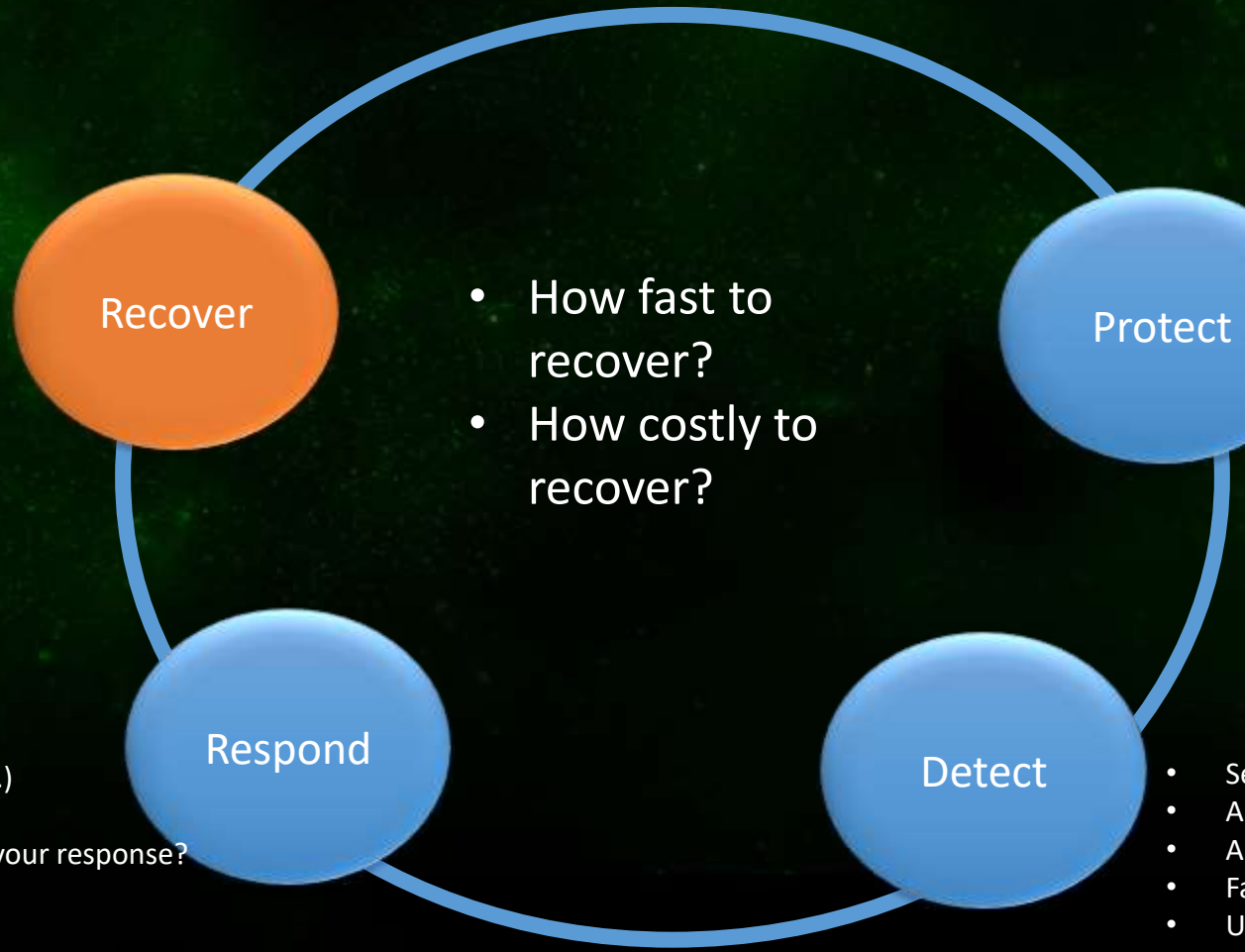
- Response plans (pre-prepared, exercised, ..)
- Playbooks
- how fast, how effective is your response?

- Boundaries, access control, authentication, authorization, segmentation, defense in depth, …
- Data (data-at-rest, data-in-transit),
- People: Awareness & Training
- Network & Systems (secure config, firewalls, AV, integrity (patching, updates, …))

- Sensors & Data analytics
- Analysis and detection capabilities
- Automation
- False-positive/false-negative ratios
- Understanding of context

4. NIST CSF (1.1): what does this mean for us?

Add capabilities & investments from Protect
=> Identify, Protect, Detect, Respond, Recover



- Boundaries, access control, authentication, authorization, segmentation, defense in depth, …
- Data (data-at-rest, data-in-transit),
- People: Awareness & Training
- Network & Systems (secure config, firewalls, AV, integrity (patching, updates, …))

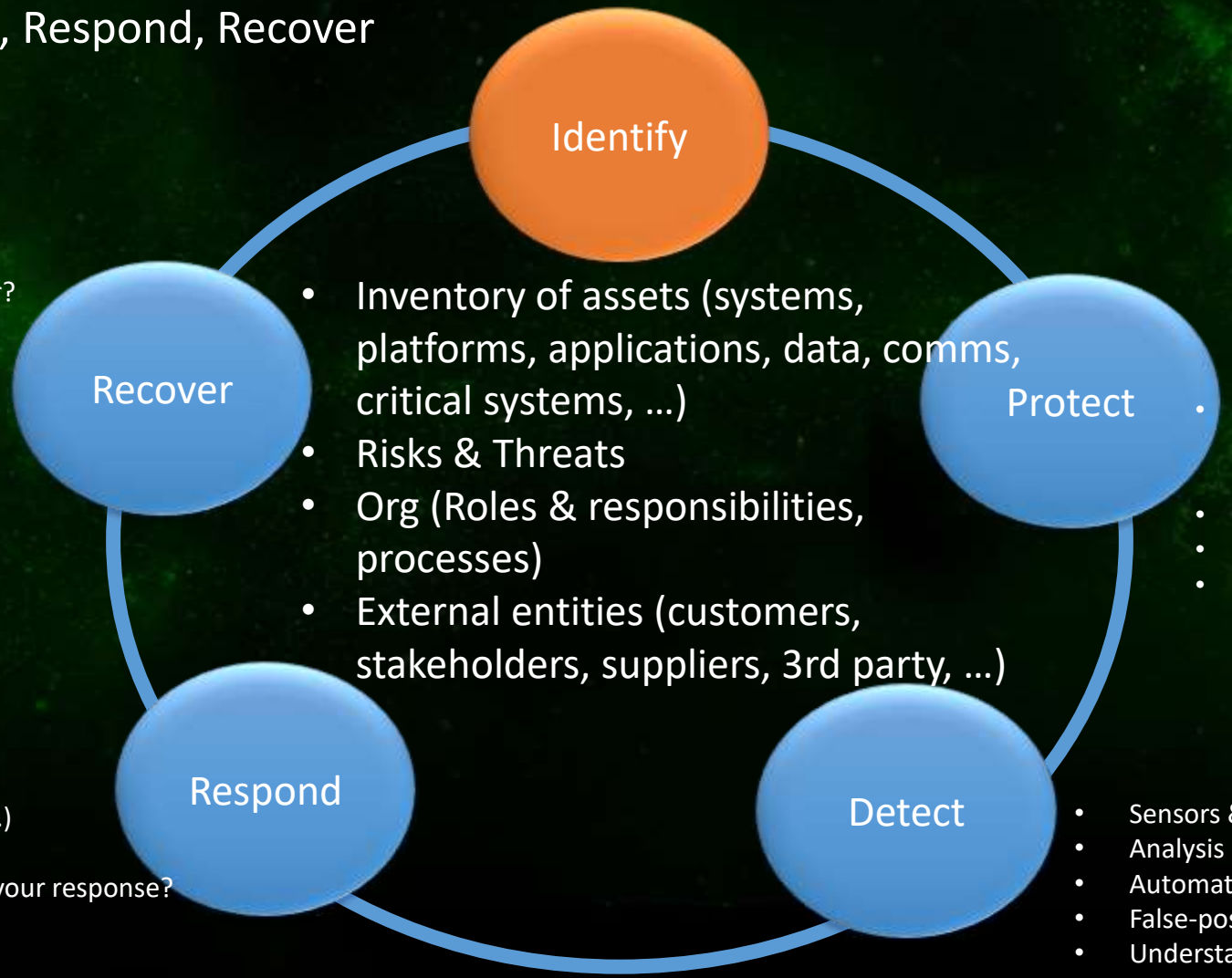
- Sensors & Data analytics
- Analysis and detection capabilities
- Automation
- False-positive/false-negative ratios
- Understanding of context

- Response plans (pre-prepared, exercised, ..)
- Playbooks
- how fast, how effective is your response?

ZERO TRUST SECURITY

4. NIST CSF (1.1): what does this mean for us?

Add capabilities & investments from Protect
=> Identify, Protect, Detect, Respond, Recover



- Inventory of assets (systems, platforms, applications, data, comms, critical systems, …)
- Risks & Threats
- Org (Roles & responsibilities, processes)
- External entities (customers, stakeholders, suppliers, 3rd party, …)

- How fast to recover?
- How costly to recover?

- Boundaries, access control, authentication, authorization, segmentation, defense in depth, …
- Data (data-at-rest, data-in-transit),
- People: Awareness & Training
- Network & Systems (secure config, firewalls, AV, integrity (patching, updates, …))

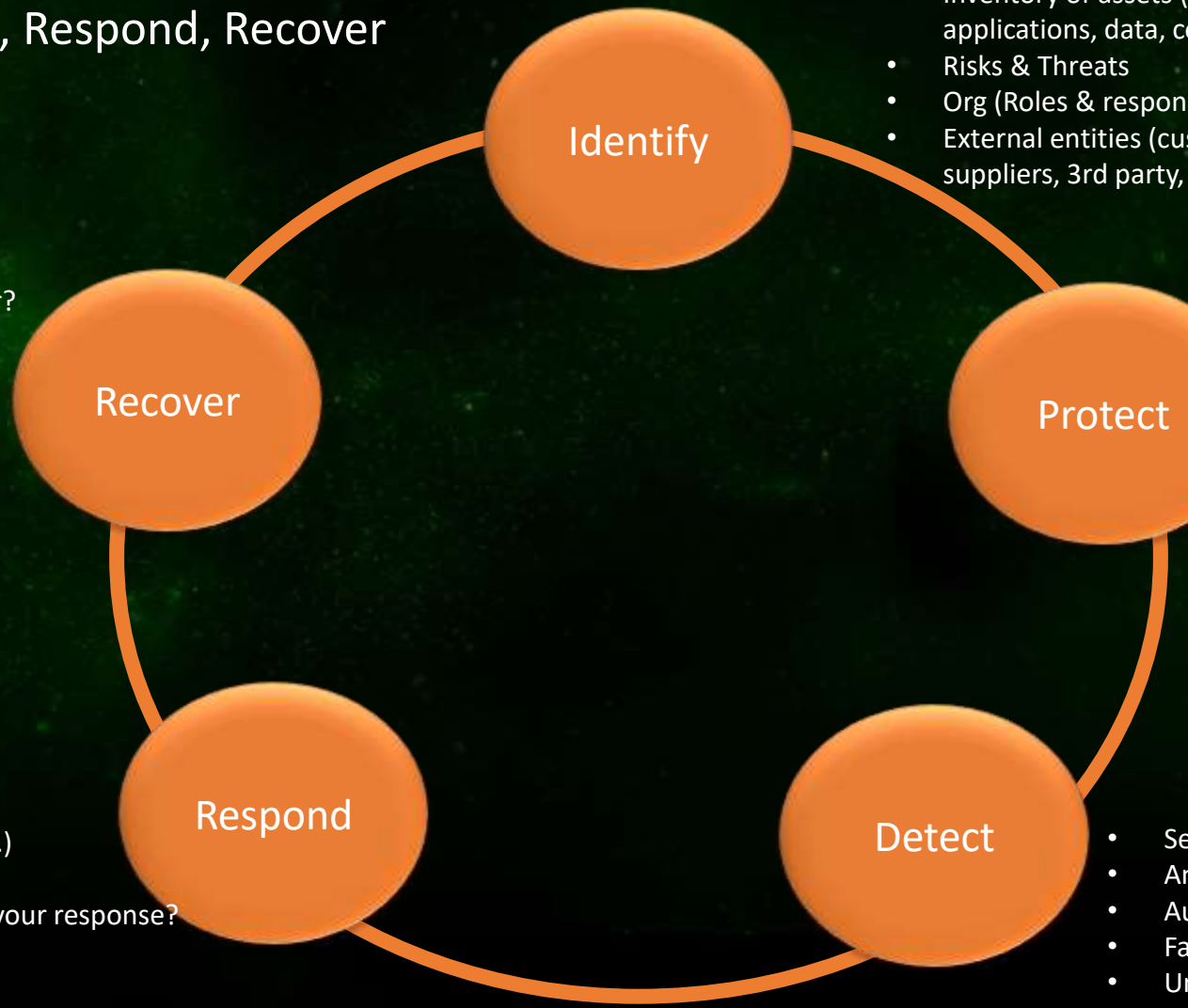
- Response plans (pre-prepared, exercised, ..)
- Playbooks
- how fast, how effective is your response?

- Sensors & Data analytics
- Analysis and detection capabilities
- Automation
- False-positive/false-negative ratios
- Understanding of context

ZERO TRUST SECURITY

4. NIST CSF (1.1): what does this mean for us?

Add capabilities & investments from Protect
=> Identify, Protect, Detect, Respond, Recover



- Inventory of assets (systems, platforms, applications, data, comms, critical systems, …)
- Risks & Threats
- Org (Roles & responsibilities, processes)
- External entities (customers, stakeholders, suppliers, 3rd party, …)

- Boundaries, access control, authentication, authorization, segmentation, defense in depth, …
- Data (data-at-rest, data-in-transit),
- People: Awareness & Training
- Network & Systems (secure config, firewalls, AV, integrity (patching, updates, …))

- Sensors & Data analytics
- Analysis and detection capabilities
- Automation
- False-positive/false-negative ratios
- Understanding of context

- Response plans (pre-prepared, exercised, ..)
- Playbooks
- how fast, how effective is your response?

- How fast to recover?
- How costly to recover?

5. AI and why you need to clean up your room

- A thought about AI/Machine Learning/Advanced Analytics to spot abnormal behavior/deviations from policies and configs, etc.
- A little test: Which item is out of place….?

"Do the basics well…" ☺

THANKS

ISC 互联网安全大会 中国 · 北京

Internet Security Conference 2018 Beijing · China

（原“中国互联网安全大会”）

RIGHT BY YOU 大華銀行

* P.s.: by the way: if you are a good “good guy” or “good lady”, we are hiring (Singapore, Shanghai,…) ☺