



#### 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**





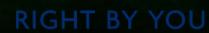














- 20 years information security experience (Group CISO, Global Head of Security, CISO, CTO Security) CISSP, CSSLP, CCISO
- 15 years management of application and software development
- Sloan Fellow M.Sc. in Leadership and Strategy, London Business School
- OWASP former chairman & global Board member, 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...?

5/29/2017 00:47:55









Maersk Chairman: "NotPetya attack totally destroyed Maersk's computer network" - up to \$300 Million



#### SINGHEALTH PATIENTS' DATA STOLEN

#### WHO'S AFFECTED

1.5 MILLION PATIENTS WHO VISITED THESE SPECIALIST OUTPATIENT CLINICS AND POLYCLINICS BETWEEN MAY 1, 2015 AND JUL 4, 2018, INCLUDING PM LEE HSIEN LOONG

POLYCLINICS
SEDOK
SUKIT MERAH
GEYLANG
MARINE PARADE
OUTAR
PASIR RIS
PUNGGOL
SENGKANG
TAMPINES

CHANG GENERAL HOSPITAL
SENSKANG GENERAL HOSPITAL
KK WOMEN'S AND CHILDREN'S
HOSPITAL
NATIONAL FANCE CENTRE
NATIONAL HERKT CENTRE
SINGAPOSE NATIONAL EYE CENTRE
SEIGHT VISION HOSPITAL

## YAHOO!



Over 1 Billion Accounts
May Have Been HACKED!





on only have 3 days to submit the payment. After that the price will be doubled.

Payment is accepted in Bitcoin only. For more information, click "About bitcoins.

Please check the current price of Elicoin and buy some bitcoins. For more information

And send the correct amount to the address specified in this window. After your payment, click «Check Payment». Best time to sheck: 9:00am - 11:00a

Use, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.







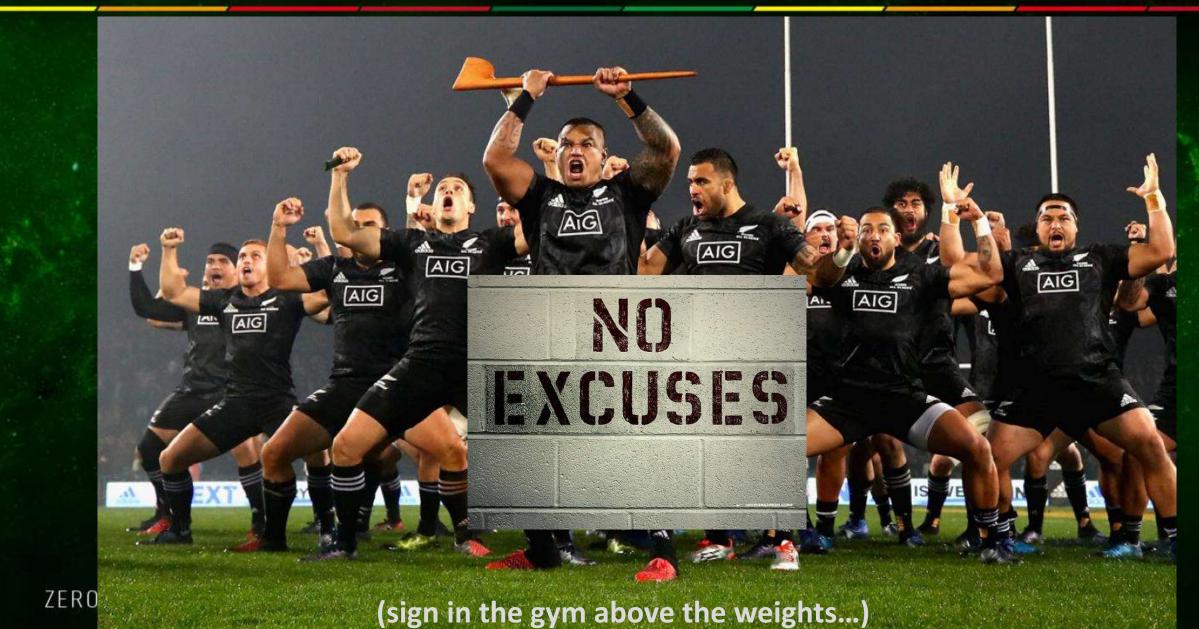


2017: 465,000 pacemakers vulnerable to hacking, need a firmware fix

#### 2. Do the basics well







### 3. Dynamic Defense





John Boyd's OODA Loop

• From static







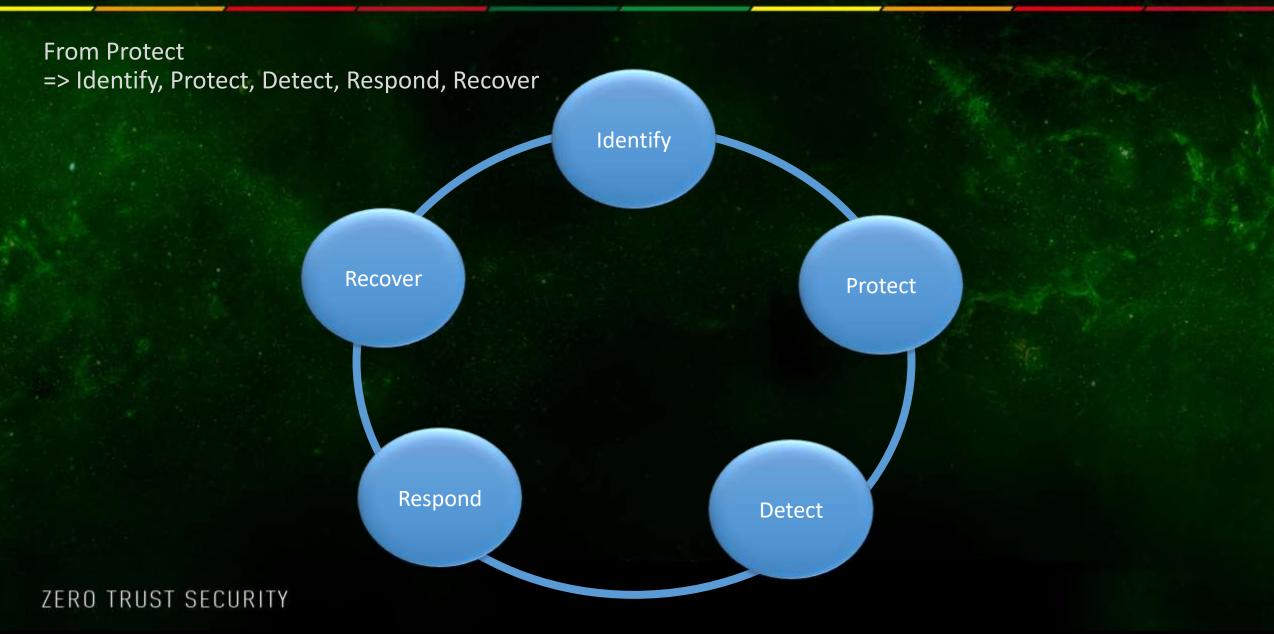


ZERO TRUST SECURITY

### 4. NIST Cyber Security Framework (1.1)











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

 Boundaries, access control, authentication, authorization, segmentation, defense in depth, ...

Protect

- Data (data-at-rest, data-in-transit),
- People: Awareness & Training
- Network & Systems (secure config, firewalls, AV, integrity (patching, updates, ...))





Add capabilities & investments from Protect

=> Identify, Protect, Detect, Respond, Recover

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

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, ...))

Detect

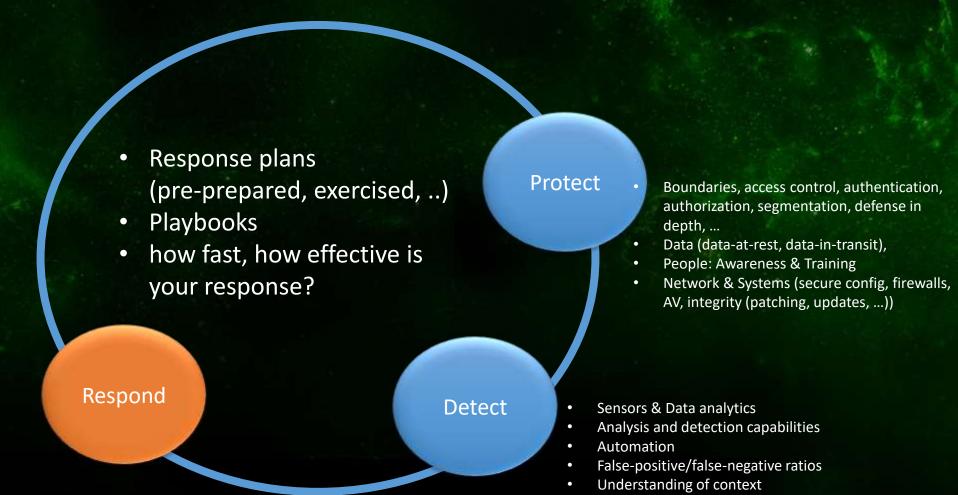
Protect

ZERO TRUST SECURITY





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



ZERO TRUST SECURITY

ZERO TRUST SECURITY



False-positive/false-negative ratios

Understanding of context



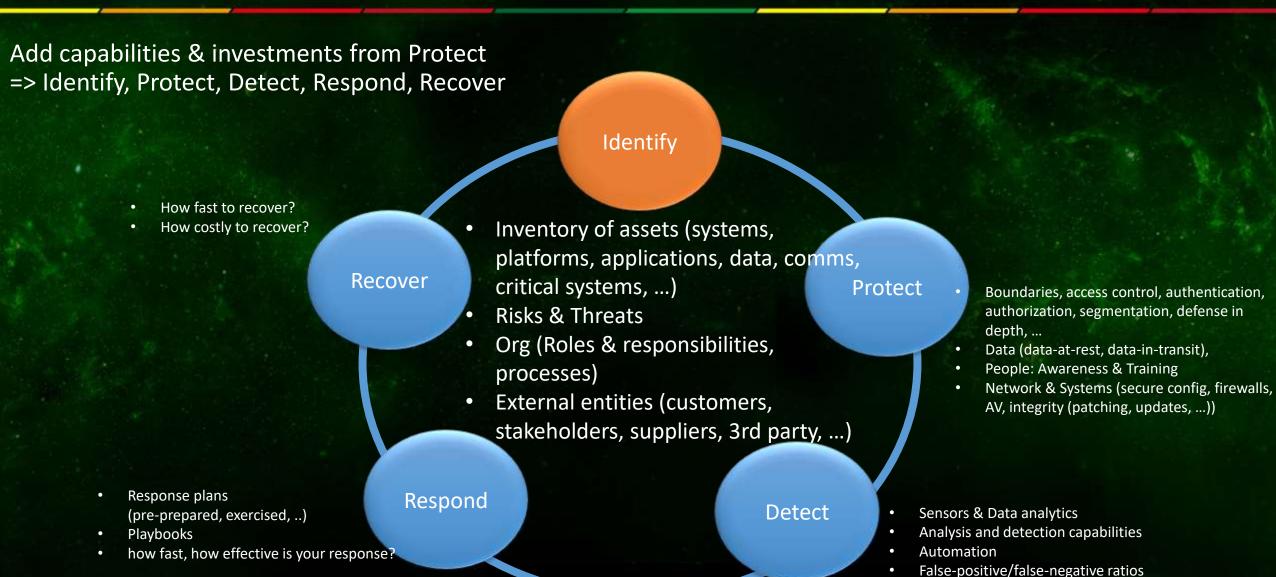
Add capabilities & investments from Protect => Identify, Protect, Detect, Respond, Recover How fast to Recover Protect Boundaries, access control, authentication, recover? authorization, segmentation, defense in depth, ... How costly to Data (data-at-rest, data-in-transit), recover? People: Awareness & Training Network & Systems (secure config, firewalls, AV, integrity (patching, updates, ...)) Response plans Respond Detect Sensors & Data analytics (pre-prepared, exercised, ..) Analysis and detection capabilities **Playbooks** Automation how fast, how effective is your response?

ZERO TRUST SECURITY



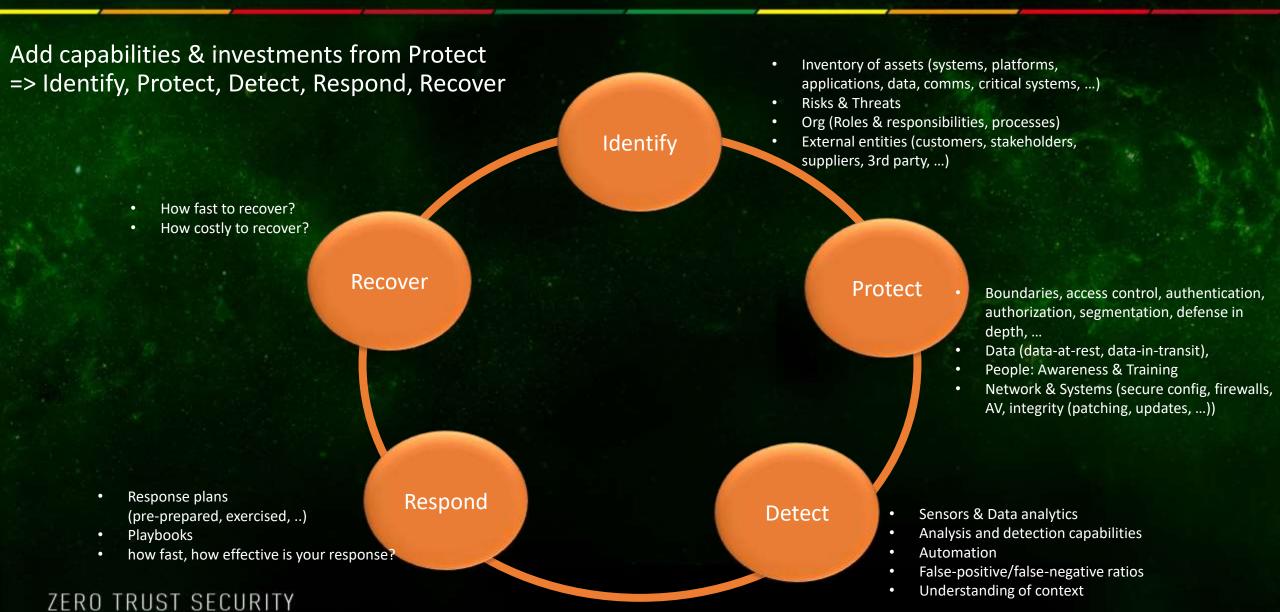
Understanding of context











#### 5. Al 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")



\* P.s.: by the way: if you are a good "good guy" or "good lady", we are hiring (Singapore, Shanghai,...)