Cybersecurity : Fortune favors the prepared mind *(Louis Pasteur, 1854)*

Exploration of the current threat landscape and potential solutions

Martin Dion (CISSP/CISM), VP EMEA Services

«He who lives by the crystal ball will eat shattered glass»

Ray Dalio

Founder of Bridgewater

PS: Great book just got published

KUDELSKI SECURITY

Elements we will reflect on today

- A busy year so far
  - Wannacry/Petya – A clever go-to-market brought to you by a cyber criminal near by
  - Mirai – The raise of the IoT Botnet
  - Equifax & Deloitte – When those who preach fail to practice
- Three key issues
  - Too many point solutions
  - Flawd security reference model
  - Lack of understanding within the ecosystem

KUDELSKI SECURITY

WannaCry & Petya and variants

- Earlier this year, Shadow Broker released a series of state sponsor exploit research. Eternal Blue, one of the exploits was picked up by criminals who built it into a malware / cryptolocker
- That exploit affected Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012, and Windows Server 2016
- MERK reported 310 millions of loss…
- Over 500,000 machines have been infected by the variants so far. Two interesting point:
  - Initial infection wave (300K) and 200k more infected since then…
  - Regardless of the fact that the patch had been available for over 7 months
- BadRabbit is the latest spin off…
- My biggest concern: Eternal Blue was 1 of 18 «known» exploit and people don’t/can’t patch.

KUDELSKI SECURITY

MIRAI IoT Botnet

- MIRAI is a Japanese word that stands for: The Future. It is botnet deployment and operation tool that automatically infects network connected, Linux-based devices. As it happen, a majority of IoT devices are exactly that.
- The actor vection was super simple, using default user and passwords of routers and cameras to infect the devices and turn them in zombies to launch a large and coordinated DDoS attack.
- The infection was very efficient, 900K devices in less than a few months. The attack volume reached up to 1 Terra of traffic per second! The suspected author is the owner of a DDoS mitigation company.
- The solution to this problem have been available for years, just change the default password…
- My bigget concern: This is just the tip of the iceberg +
    - Total lack of accountability for the trusted people who made that possible (ISPs, manufacturers of consumer products…)

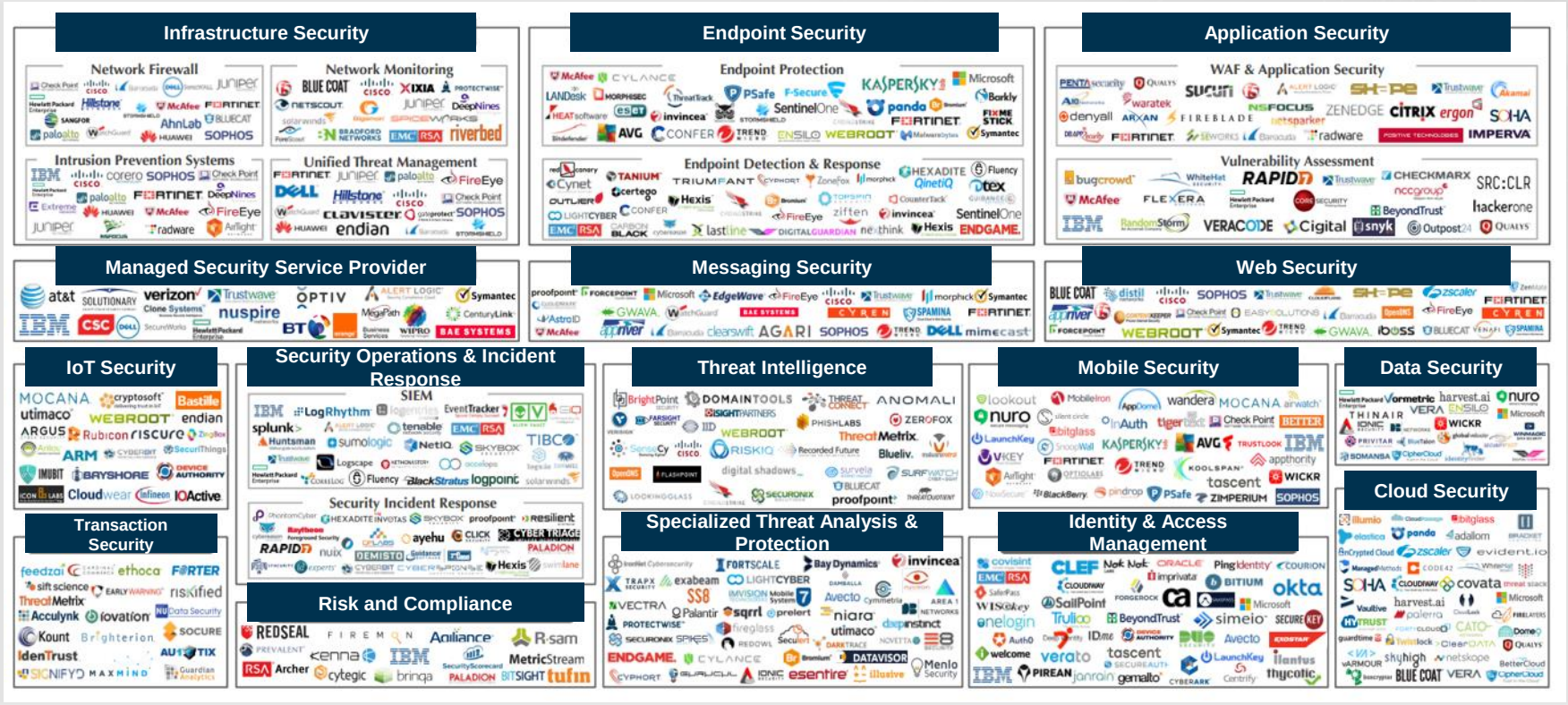
KUDELSKI SECURITY

Equifax & Deloitte: Giants with feet of clay..

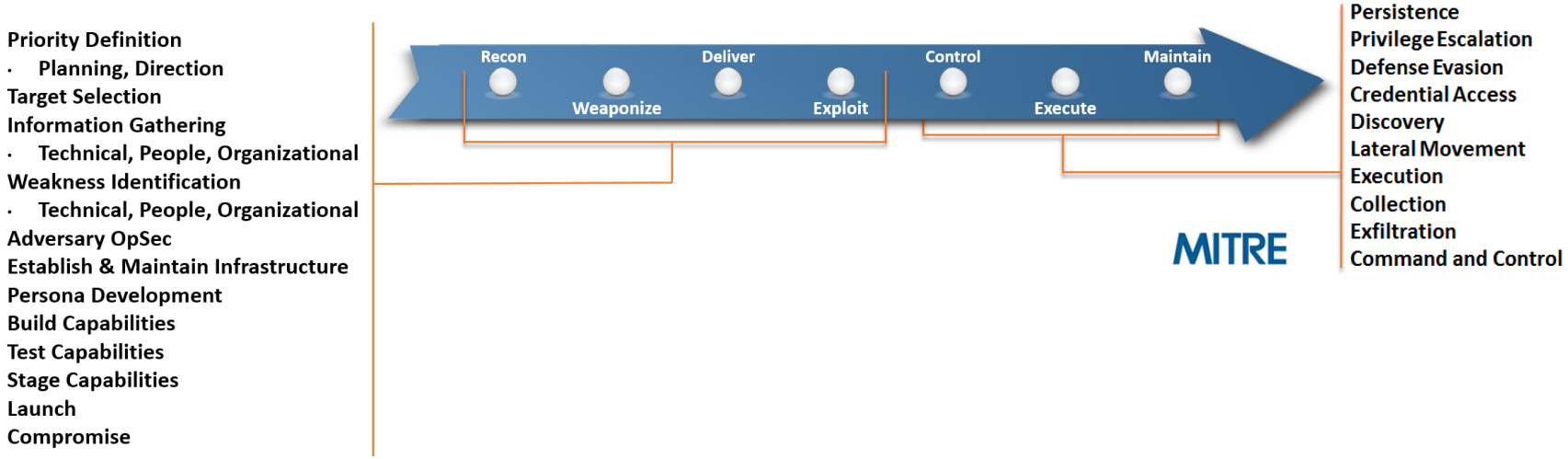
- One is entrusted with the most personal and sensitive information available and the other one is the largest and commercially recognize «security preacher» telling CEO's how security should be done
- Both were rooted like juniors using year-old exploitation techniques.
- Equifax stock loss over 400 millions in market cap in the last month.
- BUT:
  - They spent a lot of money to build their security posture
  - That posture is unfortunately as strong as the weakest link
  - The core business is not security but service delivery
  - You/We are not different, we just got lucky not to make the front page
- My biggest concern:
  - The security models we rely on are broken, we have been doing the same for 20 years…
  - We fail to recognize that there is a time-space continuum disconnect that prevent «normal» people from recognizing the urgency of the situation

KUDELSKI SECURITY

Problem booster: Solution landscape keep exploding



Moving from Lockeed Kill chain to MITRE Att&ck Framework



- Lockeed provides a simple enough model for people to understand **BUT**
- MITRE are the only one looking at the problem scientifically to figure out root causes and help finding real solutions

KUDELSKI SECURITY

Recognizing that the ecosystem is co-dependent and not siloed

Political	Economical	Societal	Technological	Environmental	Legal
		• Educating the next generation • Workforce Education • Cyber Hygiene	• Generation Gap • Too many change too quickly	• Not my problem, I am just a user	• No liabilities
• No PPP in place while PPP is mandatory for success	• Incentives?	• No digital citizenship concept • Lack of skilled workers	• No building code or real standards • IoT is the new Eldorado	• Not better or worse than average mindset • Globalization	• No liabilities
• Accountability • Clarity of role • Budgeting strategy should shift • No RoE	• Competitive-ness issue • No Cyber G20 • No PPP	• Failure to recognize the generation gap • Competing for talent	• CI definition too limited • Lack of impact understanding • Stopgap thinking	• Globalization • Profound differences between physical and cyber world	• No real regulation or framework, local or international

KUDELSKI SECURITY

KUDELSKI SECURITY

Thank You

Martin Dion (CISSP/CISM)

VP, EMEA Services

Kudelski Security