RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: CXO-W10

Security Leadership Lessons from the Dark Side

Adam Shostack
Founder
Confidenza Security
@adamshostack

Overview

- Why Can't Vader and Moff crush the rebellion?
- Concrete approaches to Leadership
- Cyber Portfolio Management
- Call to Action

Why Can't Vader and Moff Execute?

- Darth Vader: Former Jedi, turned to the dark side
  - "Search your feelings," "You know it to be true" and "Ancient religions"
- Grand Moff Tarkin
  - Focused on running a galactic empire for a crazy despot
- Culture and language

Leadership

Effective

- Vision
- Focus
- Execution
- Communication

The Empire

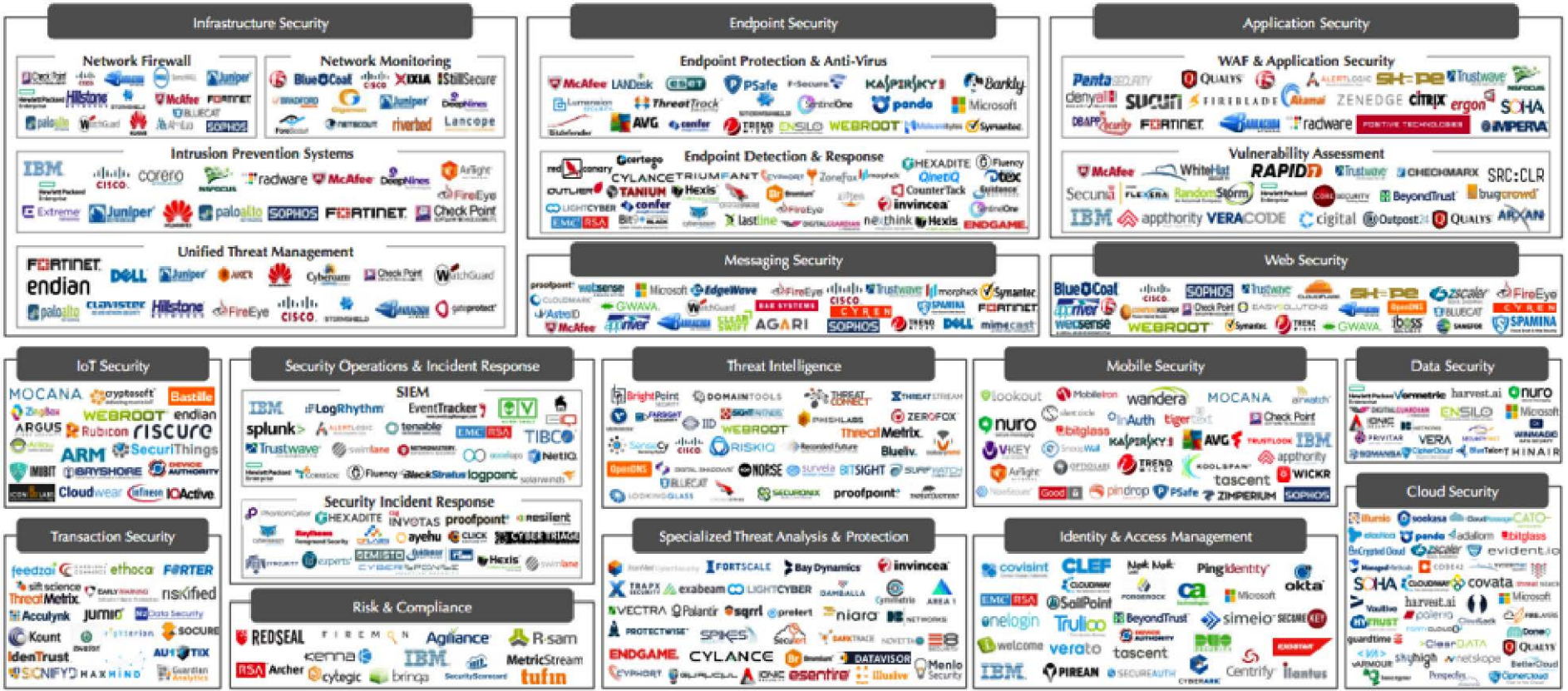
- ✓ Focus
- ✓ Execution
- — Vision
- — **Communication**

RSAConference2017

How Security Communicates

CYBERscape 2.0: Our Landscape Taxonomy

The Security Sector Is Dynamic And Vast. We Are Ceaseless & Vigilant In Our Coverage.



Source: Momentum Partners.

Gartner's Top Ten Security Tech for 2016

- Cloud Access Security Brokers
- Endpoint Detection & Response
- Nonsignature endpoint detection
- User Behavior Analytics
- Microsegmentation & flow visibility
- Sec testing for devops
- Intel-driven sec ops
- Remote browser
- Deception

Can you bring these to your board?

http://www.information-age.com/gartner-picks-out-top-ten-cyber-security-technologies-2016-123461612/

"That's okay, I don't know what the chart means either."

Leadership: Vision & Communication

Effective Vision

- Concrete
- Compact
- Communicative/Clear
- Contextual

Challenging Muddle

- No grounding
- Compliance (with what?)
- Risk (abstract)
- No request

Collaboration is key to moving large organizations

RSAConference2017

Cyber Portfolio Management

Analogy: A Financial Portfolio

Account	Value
Checking	$2,500
401K	$50,000
Mortgage	($500,000)
Student loans	($94,000)

Analogy: Financial Portfolio Analysis

Activities:

- Inventory
- Analyze (mathematical)
- Assess (judgment)

Analysis

- Some broadly applicable tools
  - Debt:Asset, savings rate
  - Churn, free cash flow
- Some very specific
- Anyone can invent new tools

Cyber Portfolio Management: Steps

- Inventory (step 1)
- Analyze (step 2)
- Assess (step 3)

- Keeping our eyes on assessment & decisions

Cyber Portfolio: Assessment

Key questions

- Right strategy & governance?
- Managing the right threats?
- Explain what and why?

Answers are:

- Concrete
- Compact
- Communicative/Clear
- Contextual

Cyber Portfolio: Governance example

- Governance isn't about Archer
- It is about the right resources and leadership
- "A neck to choke"
- Leadership, budget, staffing is rarely a "one slide view"
  - (0/10 Fortune 500s interviewed under NDA)

Cyber Portfolio: Analysis (Step 2)

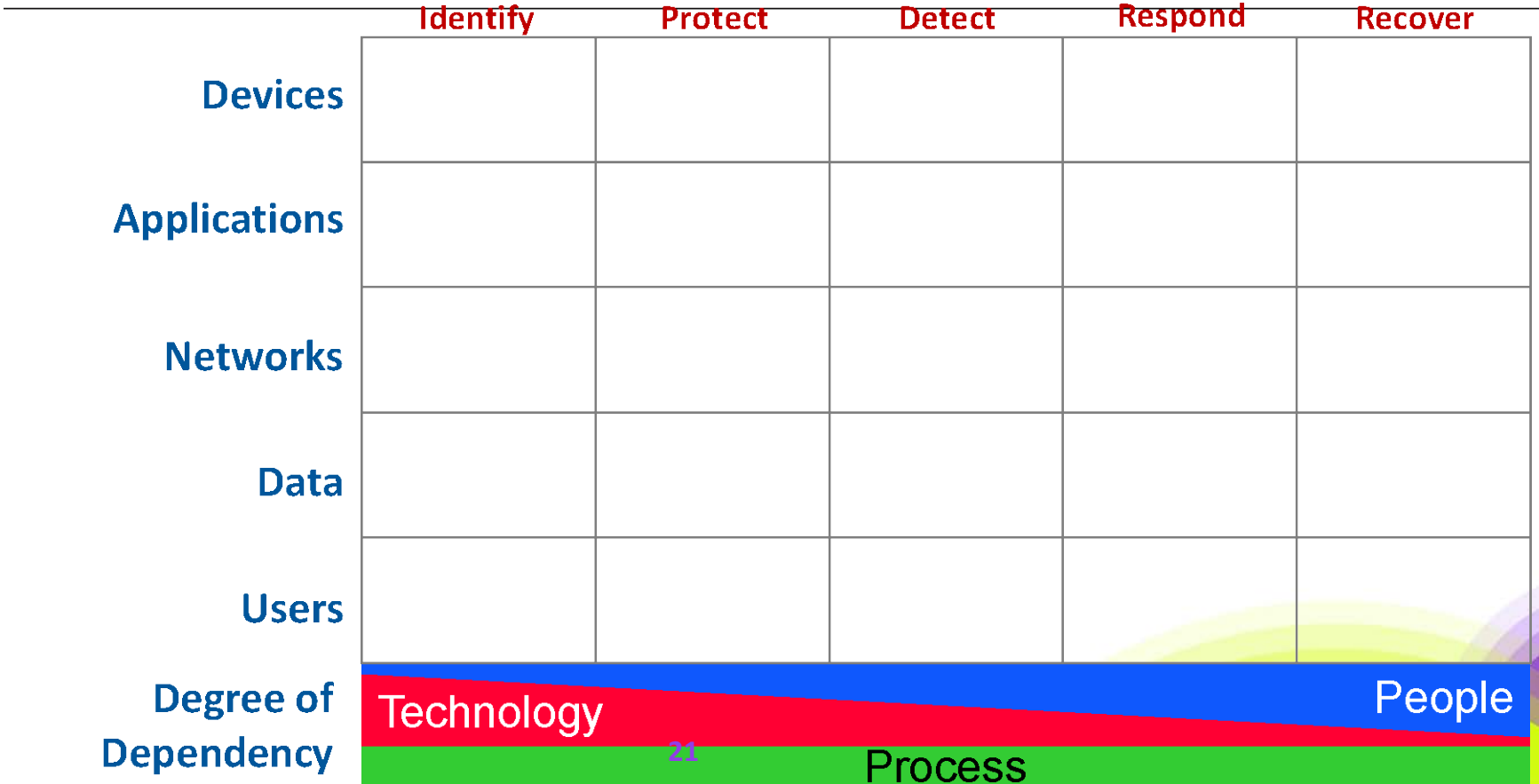
Department	Security Leader	Security Budget	Sec Staff
Mortgage banking	Alice, VP	$5.2m/12%	35/100 (35%)
Retail banking	Bob, Director	3.4m/17%	29/400 (7%)
Marketing	None	$1m/2%	1/35 (3%)
Death Star	Grand Moff Tarkin	Small moon	"Security is everyone's responsibility"

Numbers shown as security/total department

Cyber Portfolio: Inventory (step 1)

- Where does your money go?
  - Easy to ask, hard to answer
- Focus on spending, not “assets” — how is money allocated?
- Look across multiple views
  - Capex & OpEx
  - Salaries
  - Projects & Programs
  - Report-outs
- Good enough is good enough

Analyze (Step 2): Yu's Cyber Defense Matrix



Cyber Portfolio: Presentation - Investments

RSAConference2017

Applying
Cyber Portfolio Management

Improve Security

Manage Resources

Manage Relationships

Improve Security

- Gap analysis
- Improve coverage
- Orchestration /
  & platform opportunities

Acme Data Center	Iden. fy (8%)	Protect (39%)	Detect (45%)	Respond (8%)	Recover (0)
Devices (34%)	3	14	12	5	
Apps (22%)	2	5	15		
Data (3%)				3	
Network (30%)		15	15		
People (11%)	3	5	3		

* For controls that span func. ons cost has been allocated evenly

Manage Resources

- Identify duplication
- Low hanging fruit
- Vendor management
- Incident recovery

Acme Breach Response	Identify (Q1)	Protect (Q2)	Detect (Q3)	Respond (Q4)	Recover
Devices	Bob	Bob			
Apps	Alice	Sue			
Data	Alice	Alice			
Network	Nancy	Nate			
People	Jim	Jim			

Manage Relationships

- Set & communicate about priorities
- Rhythm of business
- Exec briefings & education

Offer for attendees

- Book on the subject is in the works
- Free for today's attendees! Just promise me feedback!
- How:
  - Give me (or my lovely assistants) a card (or)
  - adam.shostack.org/newthing.html
  - Sign up for "Adam's new thing" mail list– less than 12 emails/year, guaranteed

Apply What You Have Learned Today

- Next week you should:
  - Inventory your security investments
  - Get the free book!
- In the first three months following this presentation you should:
  - Analyze your investments
  - Brief your peers and get their feedback
- Within six months you should:
  - Brief leadership
  - Set a new standard
  - Benchmark with peers

RSA Conference2017