Resilience Strategy: Best Practices to Build Confidence to Cyber Attacks

Kurt Van Etten | Chief Product Officer, RedSeal

October 2018

About RedSeal

Ray Rothrock, CEO

Dr. Mike Lloyd CTO

Founded in 2004
Network Modeling & Risk Scoring Platform
Privately Held
Headquartered in Sunnyvale, CA
170 Employees in US, EMEA, Canada and Japan
9 Technology Patents
250 Customers

CSO FROM IDG

CSO Network Security Must Have 2017

BPTW BEST PLACES TO WORK

RED HERRING N. AMERICA WINNER 100

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

2017 WINNER GSN: Government Security News Homeland Security Awards

fedscoop 50 AWARDS

The War on Cyber Attack

It Doesn’t Feel Like It

We Still Fail Basic Hygiene Tests

We Are Rarely In Compliance

We Struggle To Stay Prepared

We Can’t Respond Fast Enough

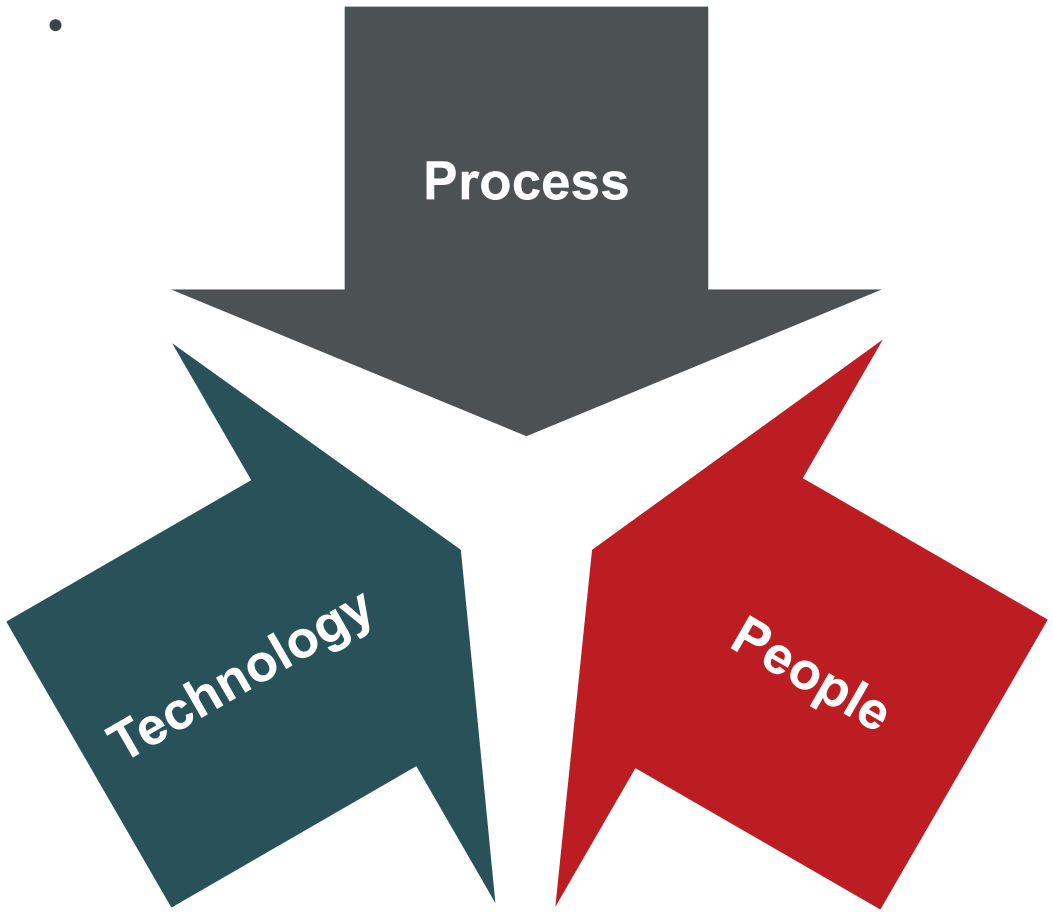
And This

The hackers are in our infrastructures long before we know it.

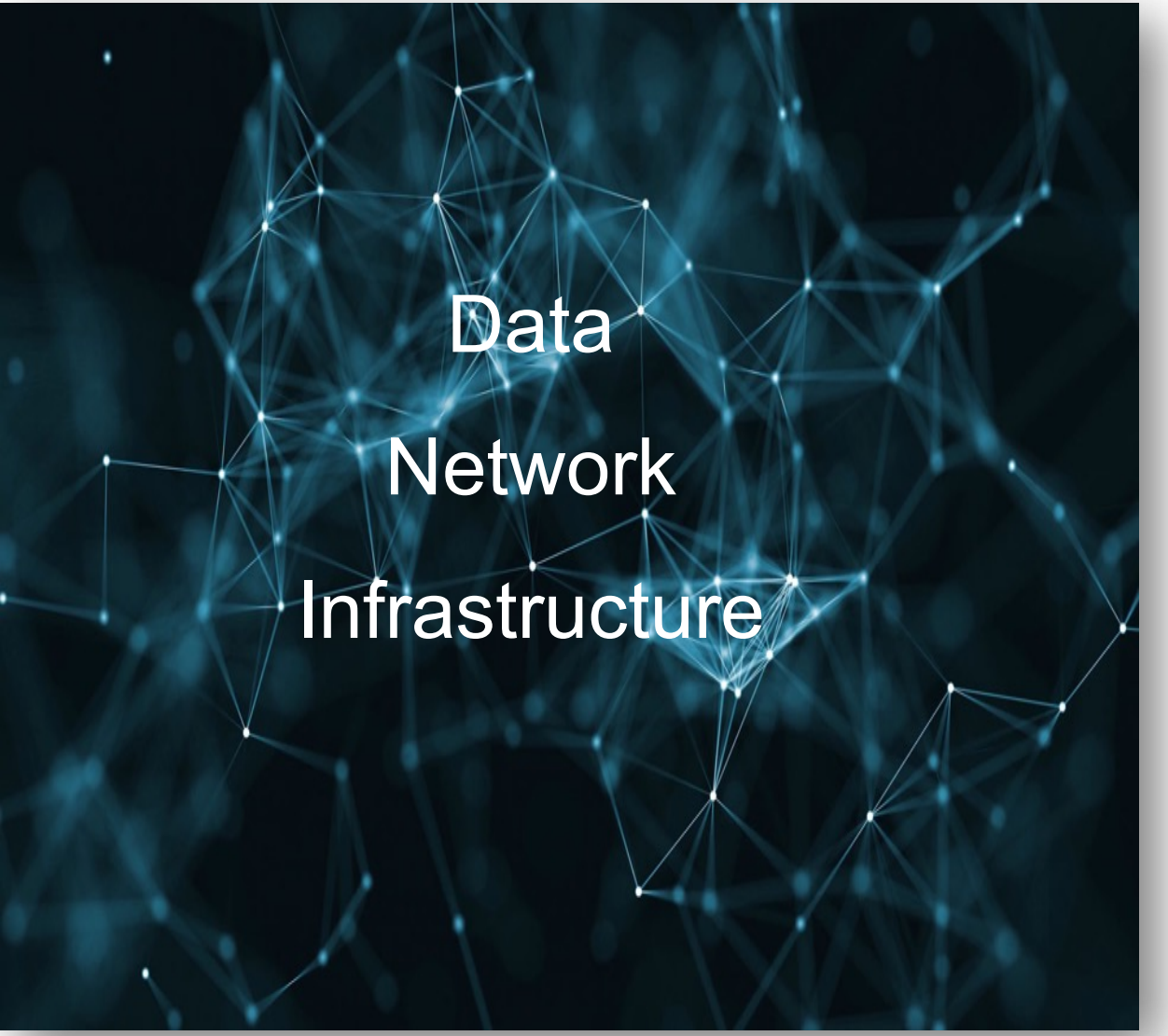
A Bold Vision

A world where DIGITAL RESILIENCE delivers
CONFIDENCE in the face of cyber attack.

It is a Business Strategy…and it is not Just About Technology



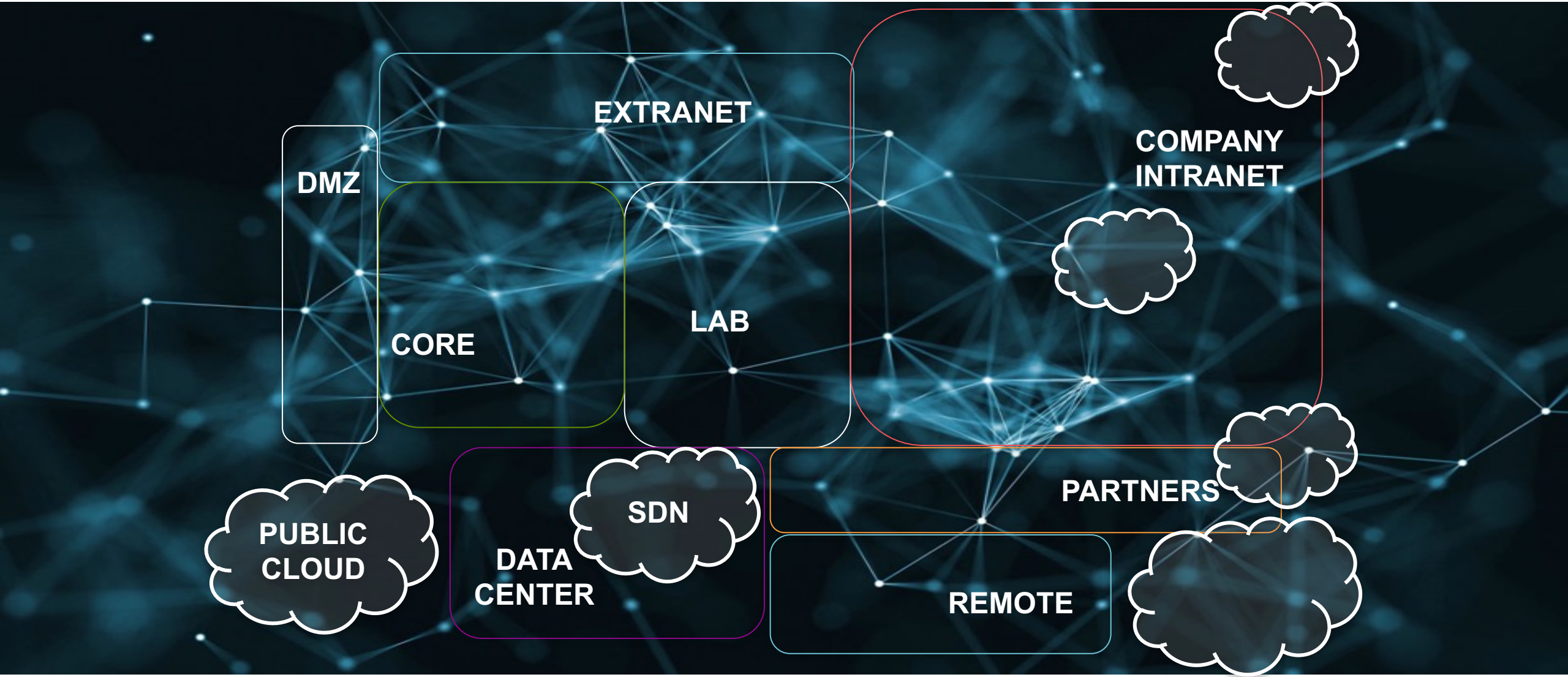
Technology



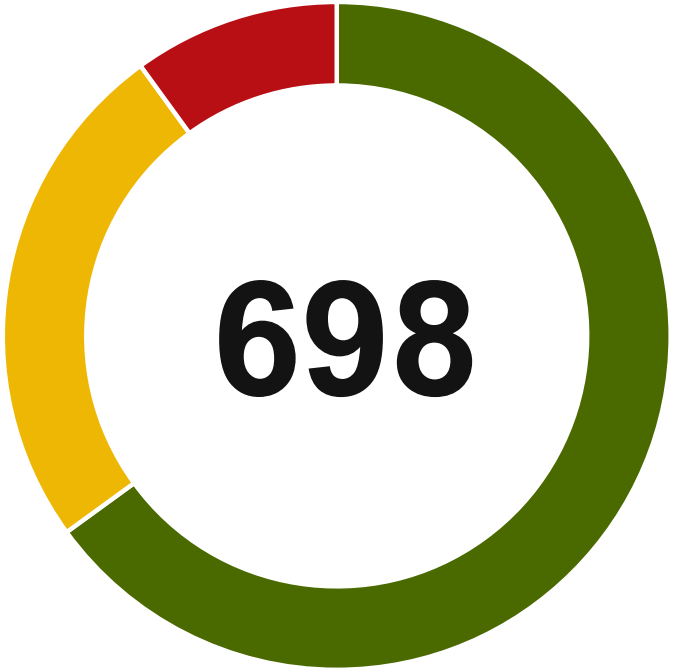
Most systems were not built with *resilience* in mind

Getting to Resilience

Know your Infrastructure Better than the Hacker Does

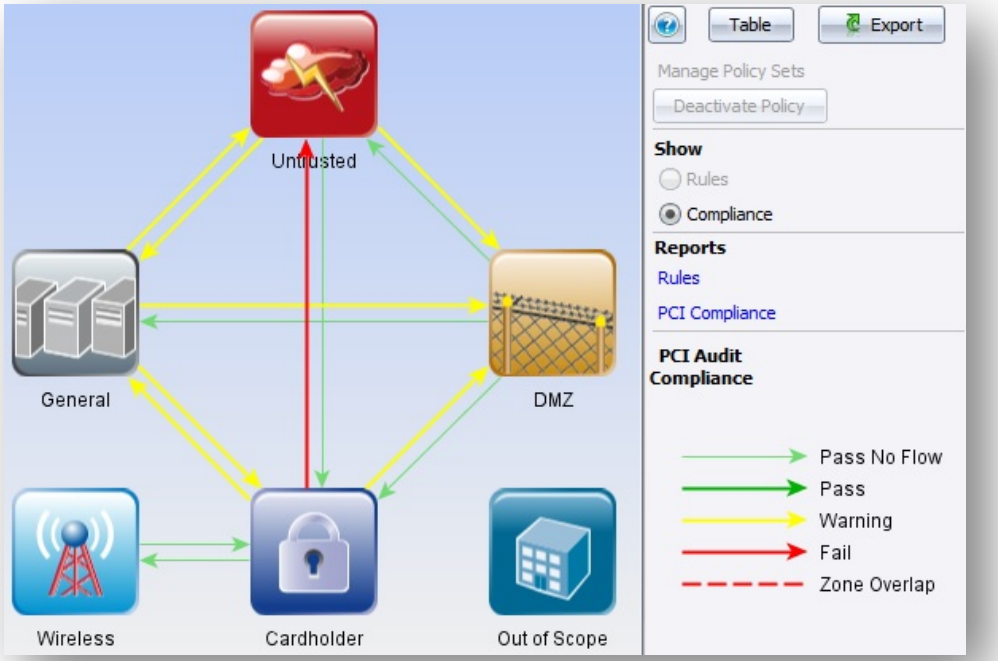


Measure And Improve Security Posture - Continuously



- Vulnerabilities in Network Context
- Configurations - Secure and Proper
- Knowledge of your Network - Inventory & Known, Unknown or Inapproriate Pathways

Policies & Compliance



Improve Responsiveness

40% rank detection as their strongest cyber capability

PERCEPTION	REALITY	
It takes an average of	Studies reveal very different answers	
6 HOURS to detect an incident	24 HOURS	2017 SANS Incident Response Survey
	49 DAYS	2017 Trustwave Report
	99 DAYS	The 2017 Mandiant M-Trends Report

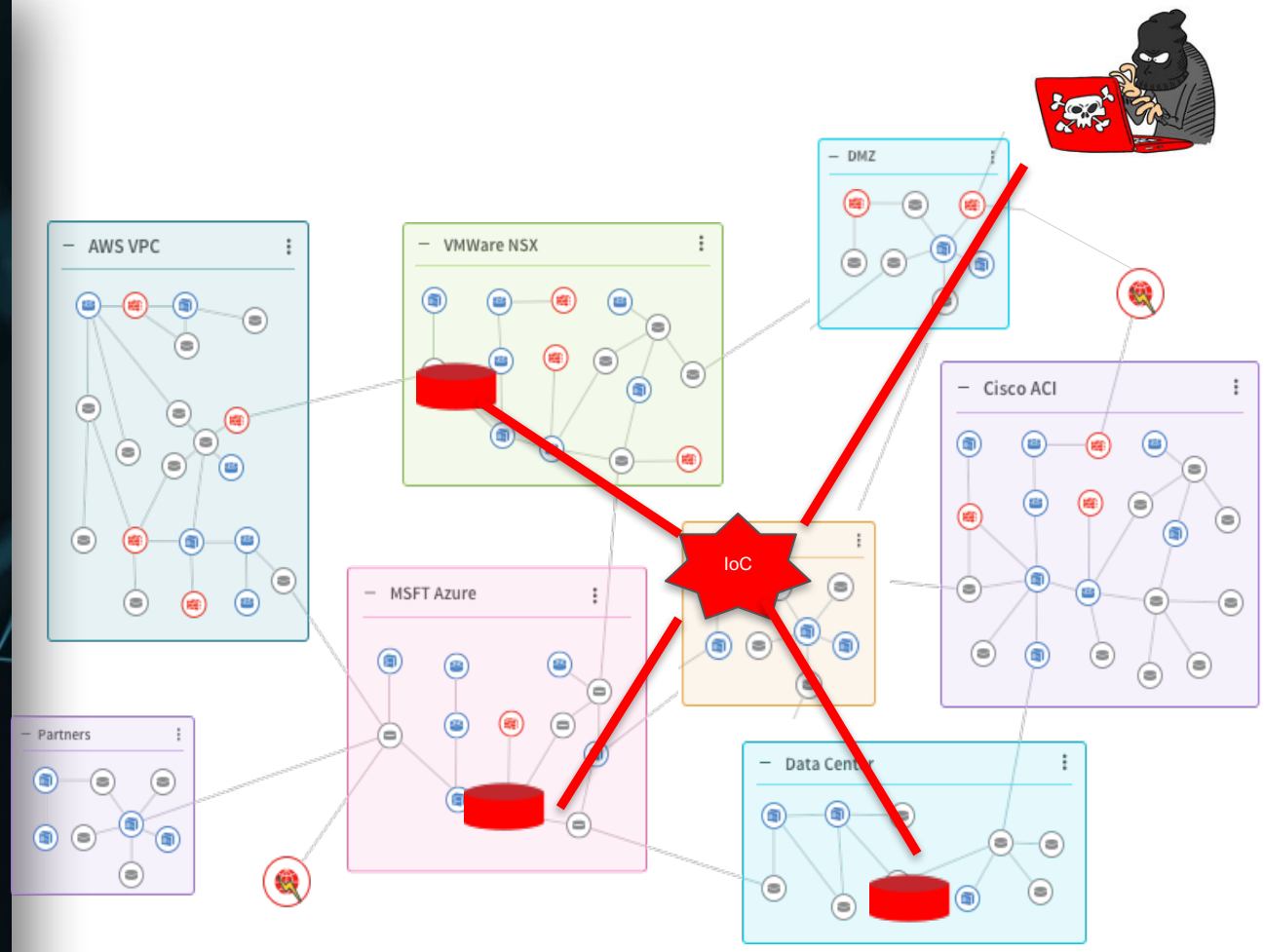
Source: RedSeal Resilience Report

WHAT IS THE BIGGEST COST OF THE DELAY?

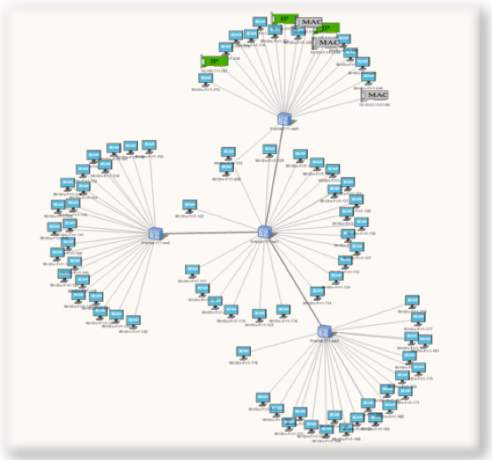
TRUST & CONFIDENCE

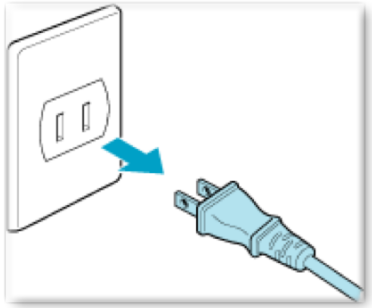
Rapid Response Requires Network Context

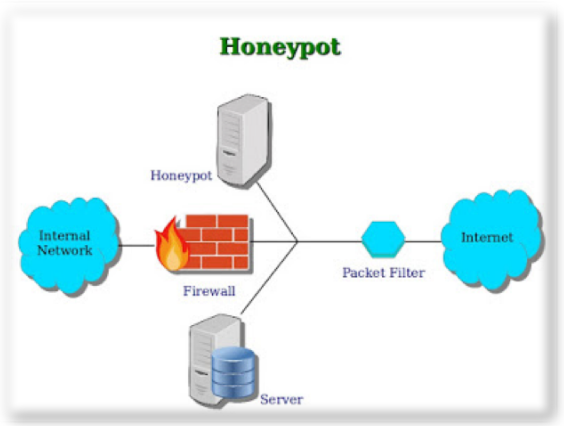
- What is the device with IoC?
- Where is the device?
- Where can the attacker traverse to?
- How can they get there?
- What containment options are available?



Rapid Response Requires Network Context







- Network Context Speeds Response
- Pull Plug- Need L2 information
- Kill Switch- L2 information
- Honeypot- Path and L2
- Deploy IDS- L3 Path
- Change ACL- L3 Path & FW

Resilience In Action | WannaCry Example

What if you had 10,000 wannacry violations?

*Resilience knowing **asap** which ones will take you down, knowing exactly how to fix them, staying in business*

Or you could pull all the plugs and be headline news

Resilience In Action | Table Top Exercise

Build Confidence

- Cross Functional
- 3 to 4 hours
- Various Scenarios
- Accelerate Time
- After Action/Lessons Learned

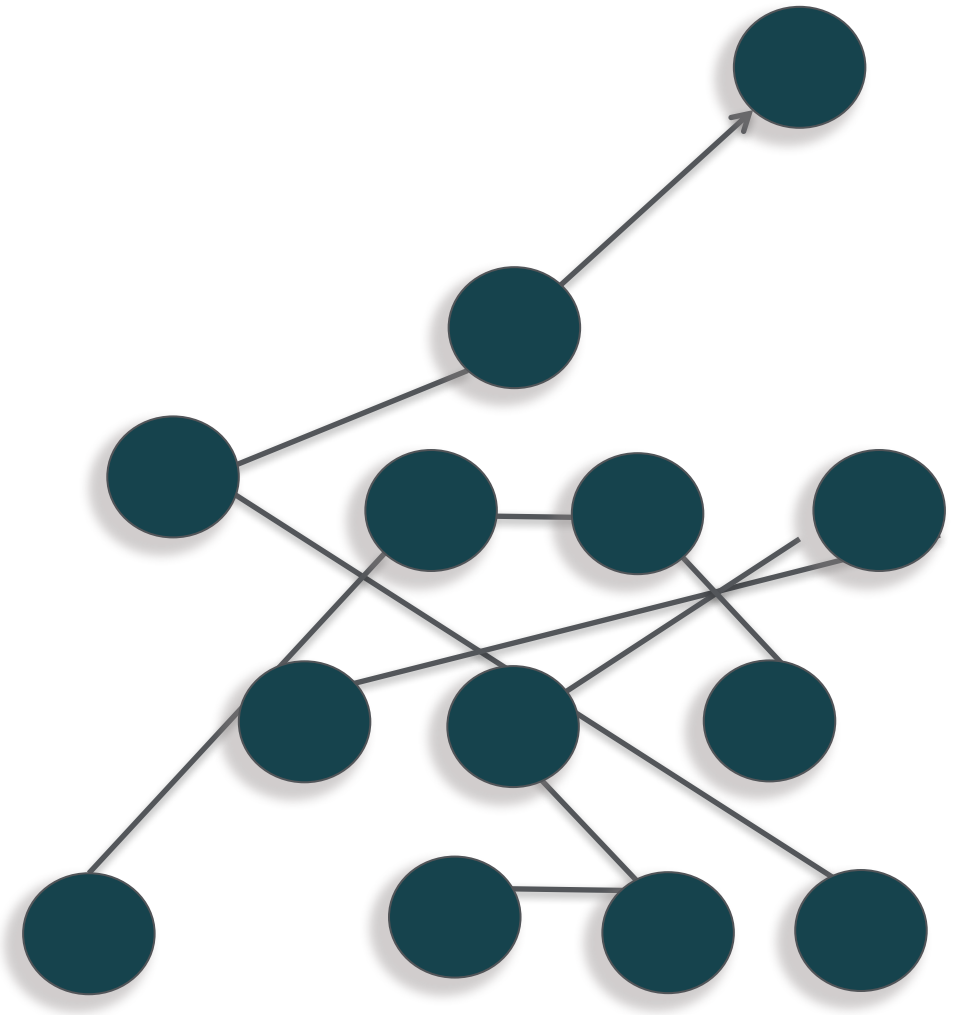
People and Process

Skilled People

Defined and Rehearsed Processes

And

Technology Are Involved



Recommendations

- Understand Network & Access Paths
- Establish Actionable, Executive Level Metrics
- Establish & Test Controls Continuously
- Rehearse Process with Cross Functional Team

The Bottom Line

YOUR JOB RESPONSIBILITY HAS CHANGED

Hackers Are In.
Protection and detection are necessary, but clearly not sufficient.

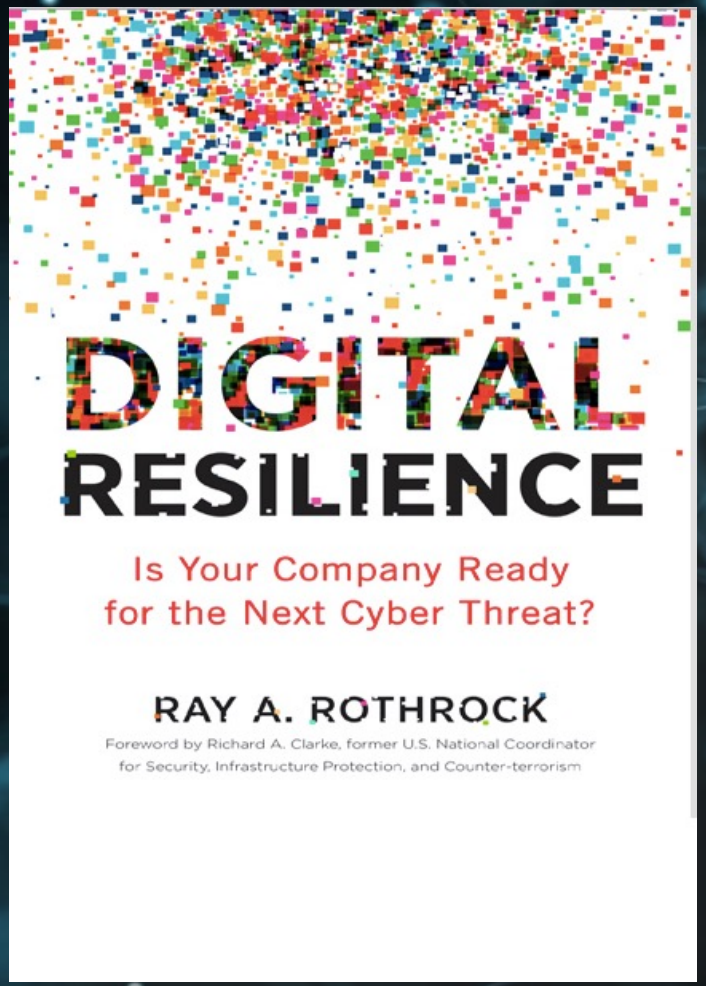
THE REQUIREMENT HAS ELEVATED

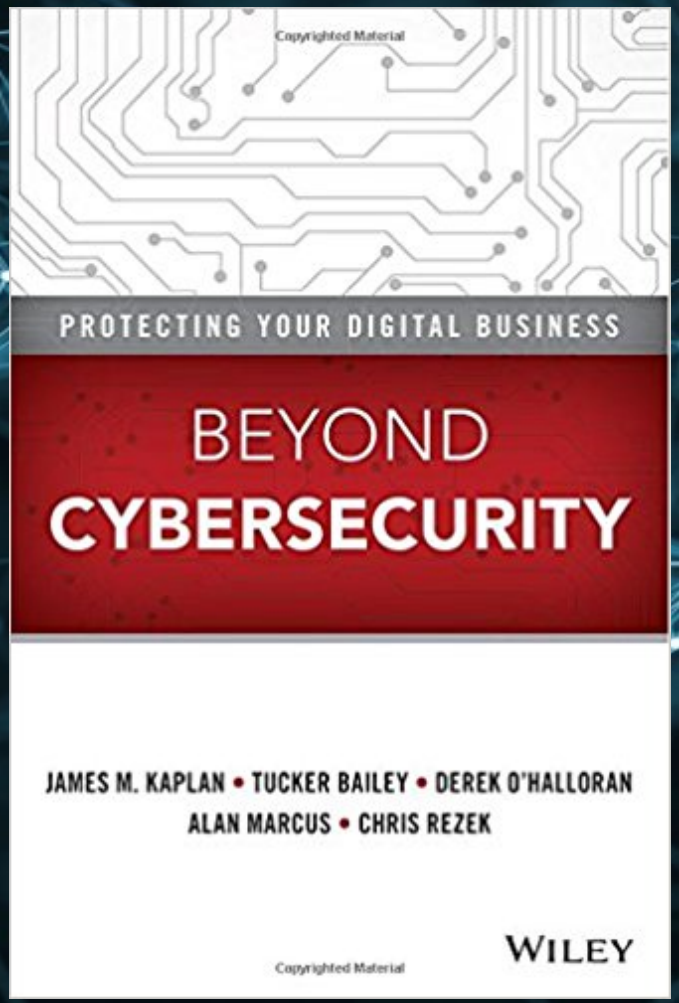
Resilience.
Must be built into the infrastructure to speed investigation and mitigate damage.

FOUNDATIONAL KNOWLEDGE CRITICAL

Network Context.
Is everything. You need to know your infrastructure better than your attacker, before they attack.

Industry Reading





MITRE

FCA
FINANCIAL CONDUCT AUTHORITY

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

SEE IT, MODEL IT, SCORE IT.
IN THE CLOUD.
ACROSS YOUR HYBRID DATA CENTER.

Thank You

Don't forget to rate this session
in the .conf18 mobile app