I don’t know much about cyber, but I’m in charge.

Being a fiduciary in a regulated world.

Your speakers today

Mike Lefebvre

Director of Cybersecurity
SEI Sphere

mlefebvre@seic.com

Mark Norcini

IT Platform Director
SEI Sphere

mnorcini@seic.com

Agenda

- Introduction
- Defining fiduciary responsibility
- Cyber as a business risk
- A process for addressing the fiduciary standard

Where we are going today?

Scenario One

Last month:

- 3 million firewall hits,
- 700 email quarantines for malicious signatures
- 150 download blocks

We researched 47 alerts, 5 of which were high severity

The team remediated all 5 and restored functionality

Scenario Two

Here is a battle map for the top 50 active threats in our industry, **today**, and the controls we have in place for each one.

In a recent incident, a phishing email successfully bypassed security;

an employee clicked it, but the attack was stopped.

Had it been able to continue, there were 4 more protections in place across our infrastructure, **specific for this attack**, that would have seen it before the attack was successful.

The attack has been confirmed clear after a regression test.

What is a fiduciary?

- One who stands in a special relation of trust, confidence, or responsibility in his or her obligation to others as a company director or an agent of the principal.
- Duty of care
- Obligation to be informed
- Example: 401k committee

BOTTOM LINE

Leadership with ultimate responsibility over the ongoing nature of the business

Who is a fiduciary?

CEO: “How are we looking around the corner so we don’t end up in the newspaper?”

CFO: “How much is this going to cost to comply with or mitigate?”

CRO: “What kind of data do we have to prove it?”

Board: “What are our peers doing? Is our process defensible?”

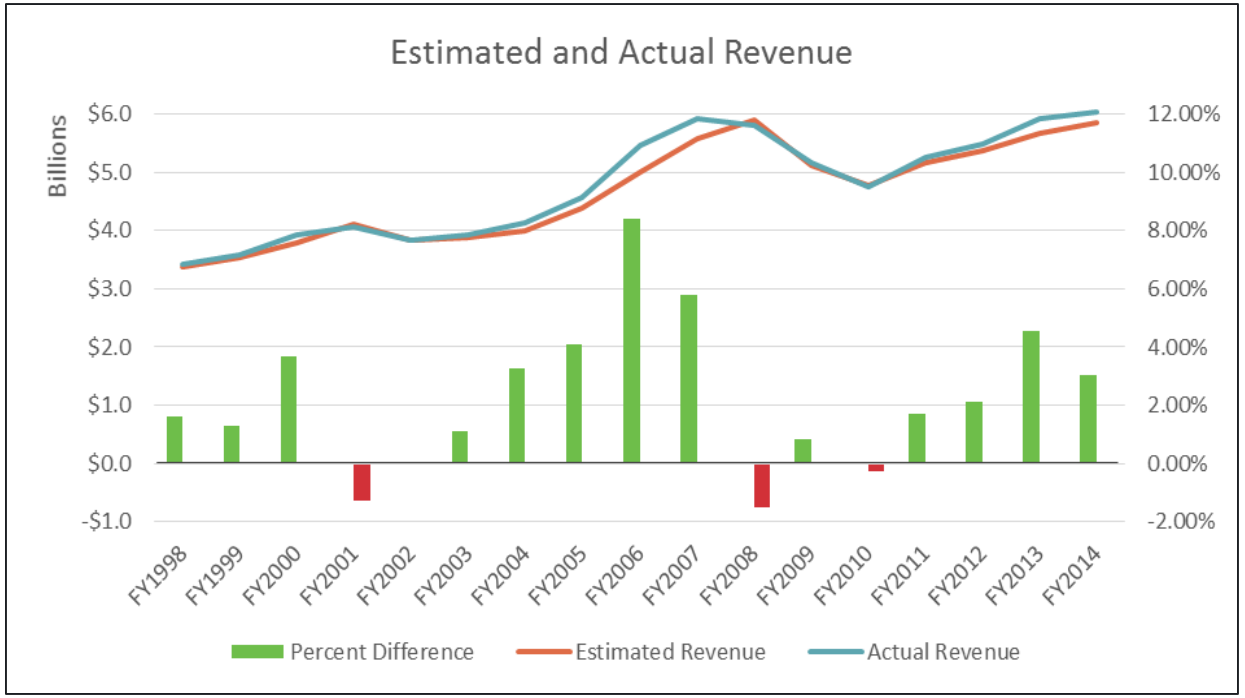
What do fiduciary business leaders care about re: IT?

Trust.

- System availability
- Protection of company & customer data
- Intellectual property
- Compliance
- Staying out of the headlines
- Thinking ahead: future-proofing the organization

Banks: Great at quantifying financial risk

- VaR: Value at Risk
- CECL: Current expected credit loss
- Duration: Interest rate risk
- LCR: Liquidity coverage ratio



Also … Banks: What is our cyber risk?

Current cybersecurity risk: _____

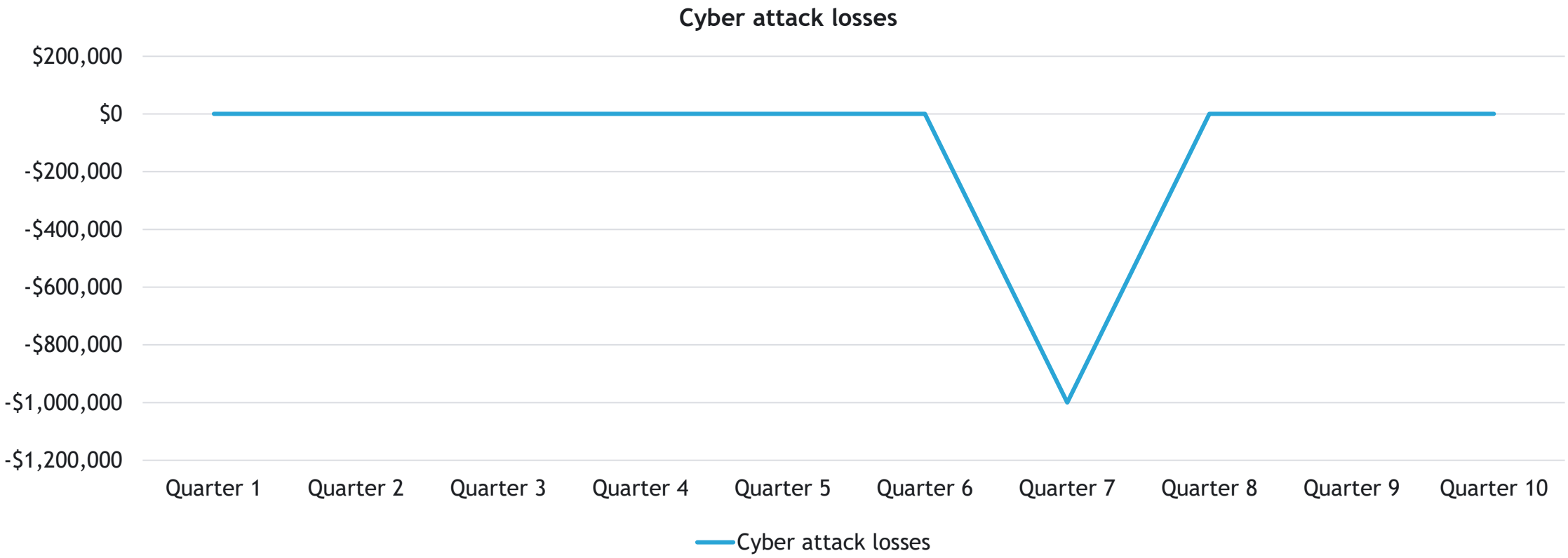
A "We passed our audit"

B "We patch critical infrastructure every 30 days"

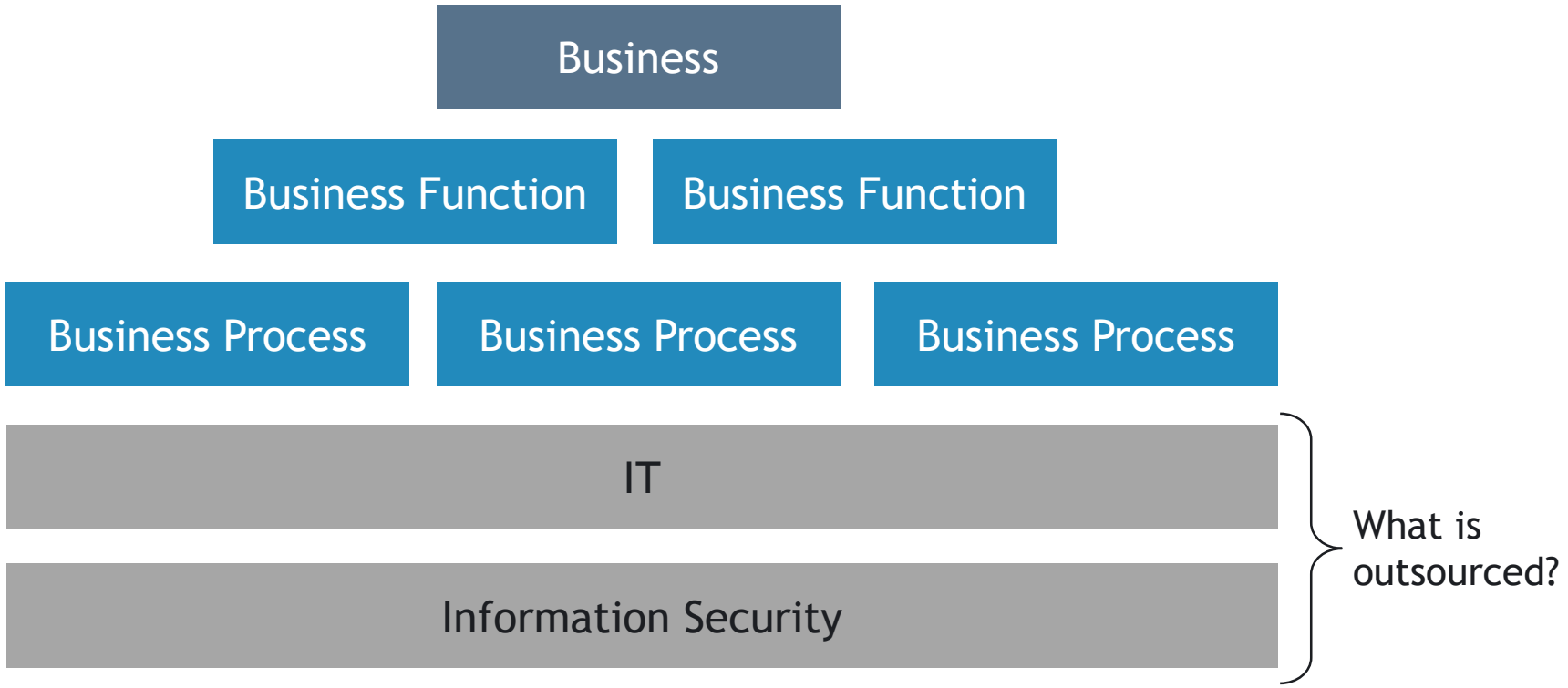
C "7,982 firewall blocks"

D "We're in the middle of a core conversion"

Cybersecurity: A lopsided risk



Where is Cyber in an Organization?



A history of being set up to fail

Tell you there's a problem, do not fix the problem

"I'm not a dentist. I'm a dental monitor - I just tell you when you have a cavity."

*LifeLock television advertisement

What's your job today, IT?

What's changing?

"By 2026, at least 50% of C-Level executives will have performance requirements related to cybersecurity risk built into their employment contracts."

"Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem," Gartner, gartner.com (login required).

"Over the years, our disclosure regime has evolved to reflect evolving risks and investor needs … Today, cybersecurity is an emerging risk with which public issuers increasingly must contend. Investors want to know more about how issuers are managing those growing risks."

— SEC Chair Gary Gensler

"SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," Securities and Exchange Commission, sec.gov.

Why increasing cyber regulation?

Expect cyber to become as regulated as finance

Banks

The Consumer Financial Protection Bureau (CFPB) labeled cyber protection of consumer data as a “liability” area that it intends to enforce in an August 2022 circular issued on data security.

Digital Assets

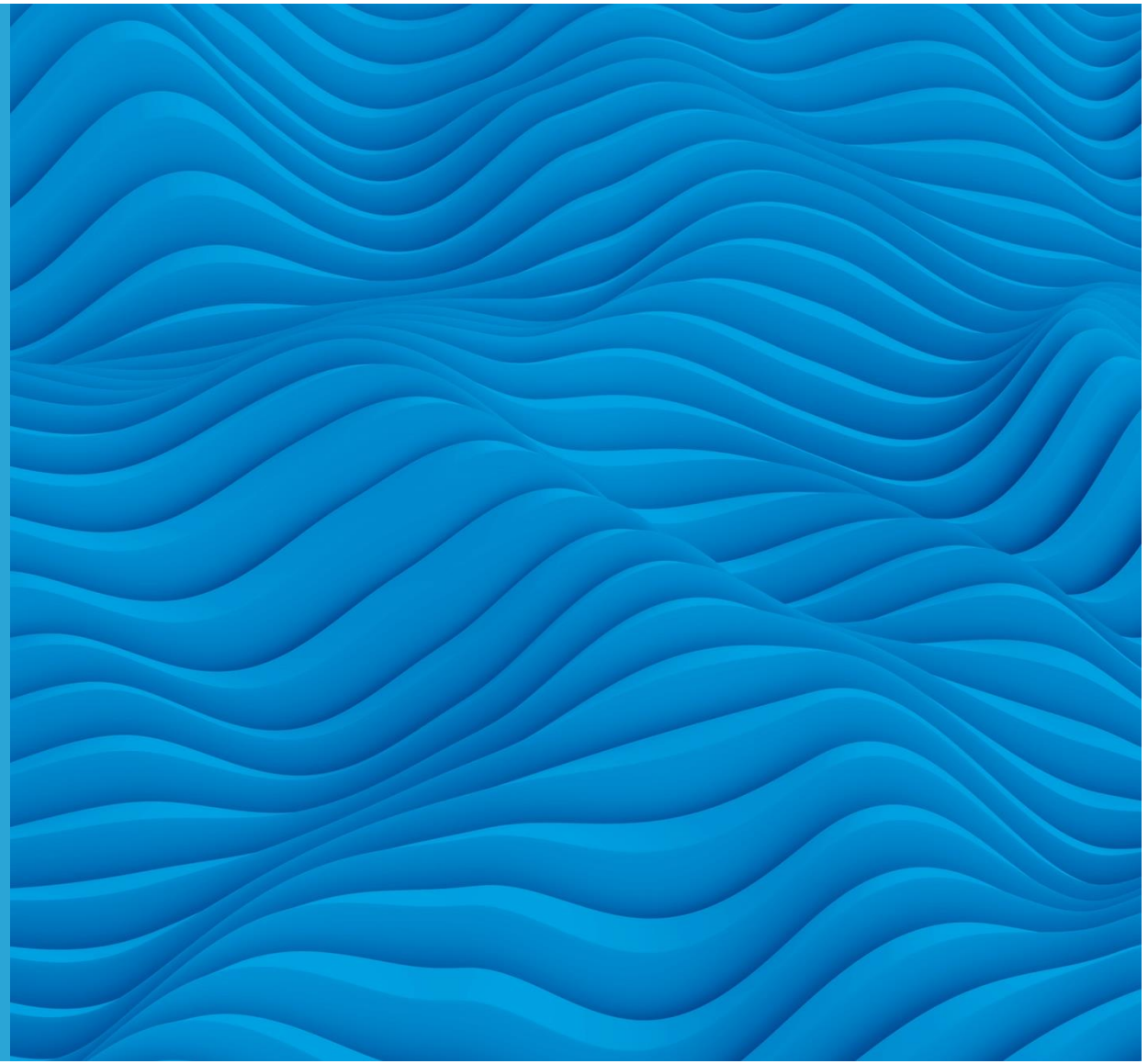
There have been 64 bills introduced in the current session of Congress dealing directly or indirectly with cyber security.

National Security

34 amendments to the National Defense Authorization Act directly or indirectly dealing with cyber security.

Moving security forward

Thinking like a cyber fiduciary.



Prepare and Maintain = “Mandatory Essentials”

- Patching critical infrastructure every 30 days, everything else every 60
  - Cost to do it more often is X, but outweighs the perceived risk
- Phishing testing twice a year - quarterly for those who fail - with a goal of 10% open rate
  - Cost to get to 5% is X, but outweighs perceived risk due to these compensating controls
- Vulnerability scans on endpoints and network devices every X weeks
- Annual penetration test

Detect and Respond

- Email security tool, intrusion protection, endpoint protection, web filtering, etc.
- SIEM to correlate activity
  - SIEM is actively managed by IT or vendor
- Vendor or IT manages system alerts

Forecasting the threats we are likely to see

Fiduciary Detect and Respond

What is active in our industry, amongst peers? What threats should we expect to see?

- What is the process for choosing these?
  - How regularly are we updating this forecast?
    - If they show up, what protections are in place? How do we know we will be alerted?
      - What happens if we fail?

Fiduciary Detect and Respond

Attack Stage

Threat	Delivery	Exploitation	Installation	C2/2dary	Exfiltration
Agent Tesla	✓	✓	✓	✓	✓
Adwind	✓	✓	✓	✓	✓
Avemaria	✓	✓	✓	✓	✓
Bazar	✓	✓	✓	✓	✓
IcedID	✓	✓	✓	✓	✓
CobInt	✓	✓	✓	✓	✓

Case Study: Fiduciary Detect & Respond

Stage 1

Phishing Email hits employee inbox.

<<Click>>

Stage 2

Network detects potential malicious download.

- Security mitigates and **remediates** the issue.

Stage 3

Security confirms, using threat traits, the malicious zip file download would have been seen by the endpoint detection tool.

Stage 4

The file required a manual password by the employee.

Stages 5 & 6

Had the employee failed to identify this as suspicious, additional controls in the network tools would have seen it for the secondary call out and the C2.

Post Incident

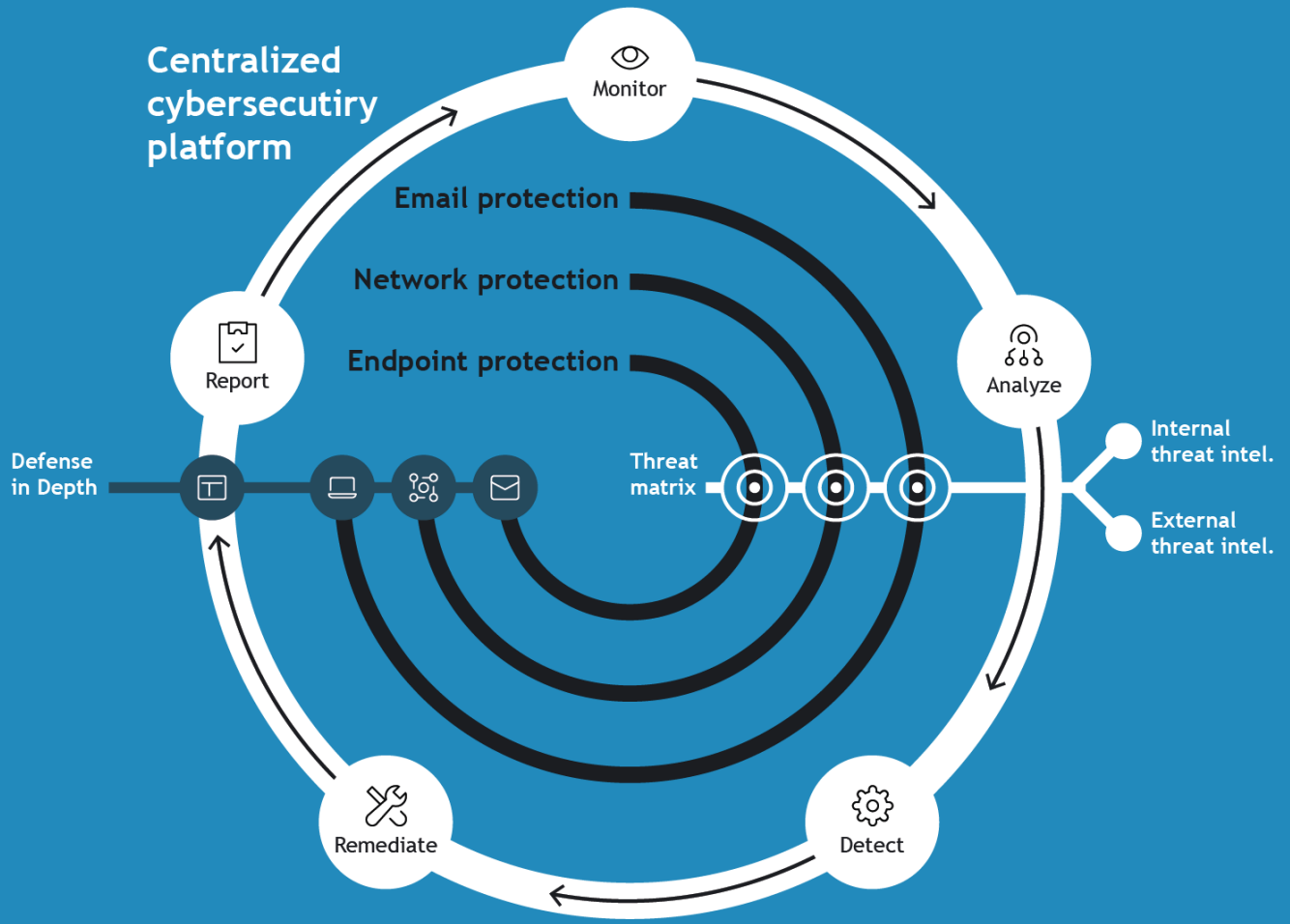
A regression test of IOCs confirms the environment clear; email intelligence has been updated if attack returns

CONCLUSION

‘Security’ is confident there is no further compromise

A comprehensive cybersecurity solution

- Holistic view of infrastructure
- Integration of tools
- Layered resiliency
- Single point of execution



Summary

- Regulatory push for greater fiduciary standards in the C-Suite over cyber
- Moving from reactive to future proofing
- Mapping active threats to compensating controls
- Defensible process, sleep well at night, facilitate budget discussions

Questions? Let’s get in touch.

SEIC.com/Sphere
sphere@seic.com