Incident Response – Now and Then

16th Workshop – January 7th, 2017

Mohammed Almozaiyn,

CISM, CISSP, CISA, CRISC, GCIH, GREM, CICA, ACE

Sponsored By

"If you're going to invest in one thing, it should be incident response"

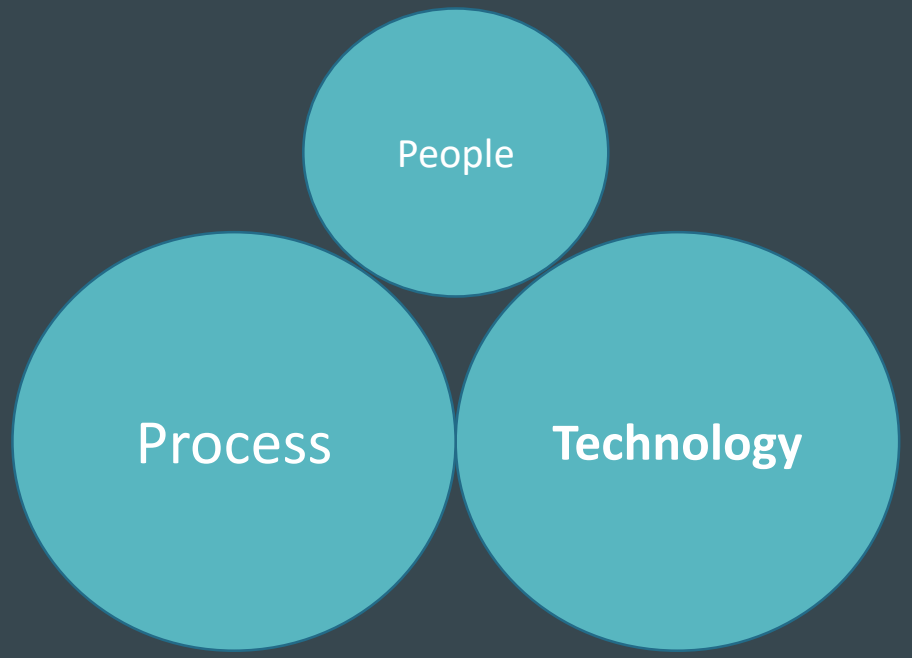
Gartner®

Agenda

- Background
- Need and Origins
- Current Practices
- Future of IR
- Success Factors

infosec elites

IM Curriculums



infosec elites

IM Curriculums

People

Incident Response

Incident Management

Threat Intelligence

Forensics Analysis

Emerging Vulnerability Analysis

Imminent Threat Analysis

Process

Log Management

Knowledge Management

Technology

infosec elites

PREPARATION

Before sailing, put all plans ready for action.

IDENTIFICATION

Get to correctly know what's happening, or about to happen.

CONTAINMENT

Stop the bleeding, effectively.

ERADICATION

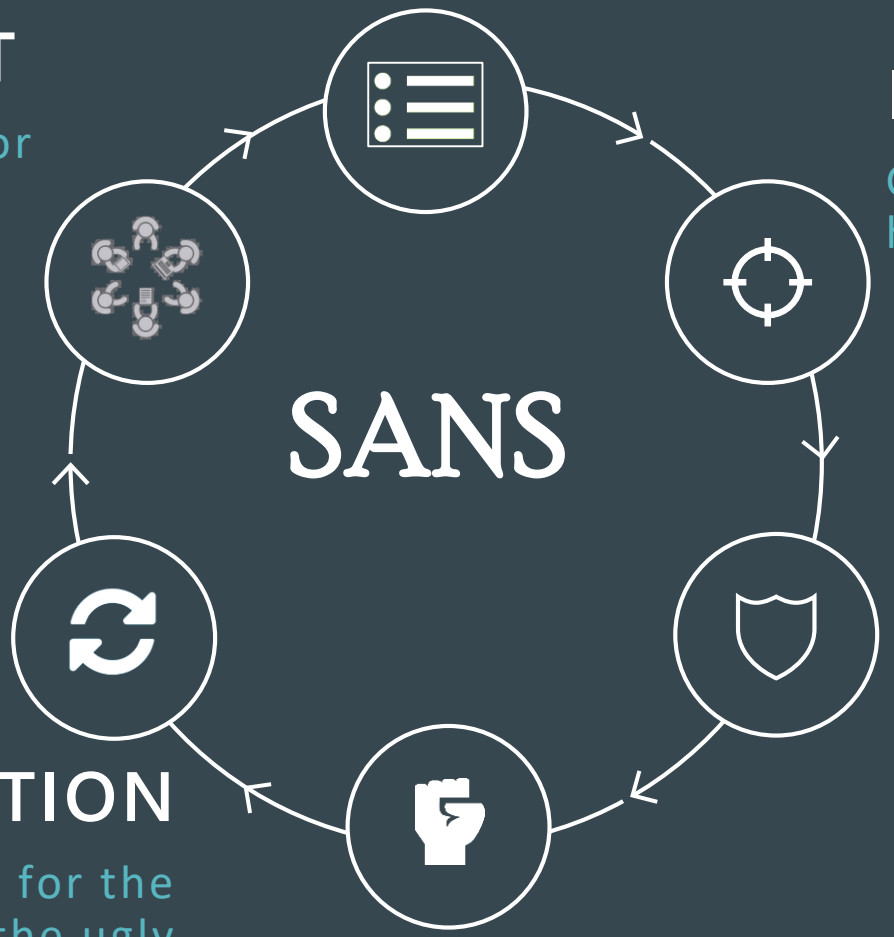
Eliminate the bad and prepare for the worst by extracting the ugly

RECOVERY

Back to normal or so

LESSONS-LEARNT

What have we done right or wrong.



infosec elites

Why IR?

Current State of the World IR - 2015

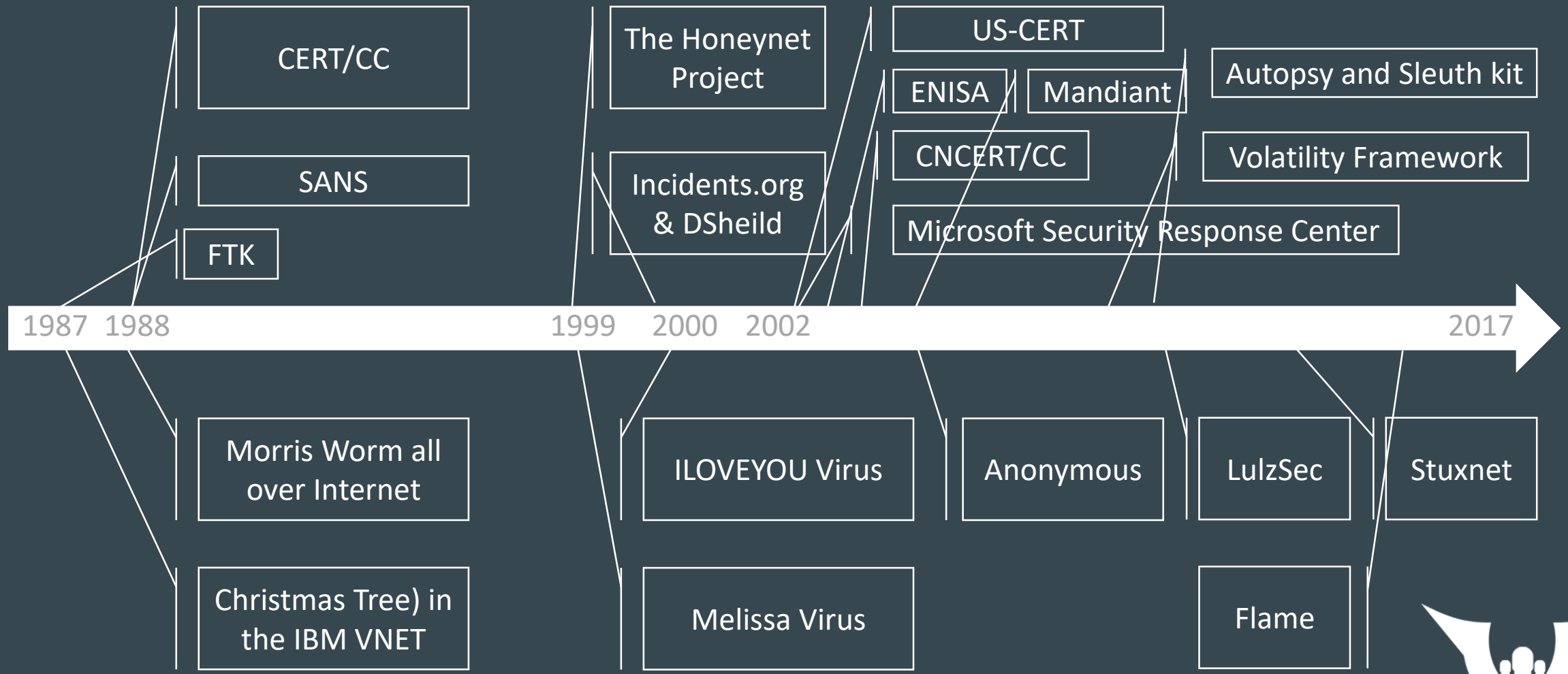
Most organizations suffered a breach last year	• 67% of organizations reported a cyber breach in the last 12 months • 100% of firms surveyed reported a cyber breach at some point in the past • A breach is - to all intents and purposes - inevitable.
Security spend is shifting towards Incident Response	• Traditionally, cyber security focuses on Prevent & Protect approaches • Firms are migrating spend to Detect a breach quickly… • … and Respond to minimize the impact of that breach.
Are firms really ready for cyber breaches?	• **86%** of firms claim a high state of readiness for cyber breaches • Yet **39%** do not have a cyber readiness plan • And only **30%** of firms that have a plan test it regularly.

http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/MCS_Incident_Response__Execsum_Resilient_2016.pdf?submissionGuid=e4205681-7292-45cd-a6f1-d2adaea252c0

infosec elites

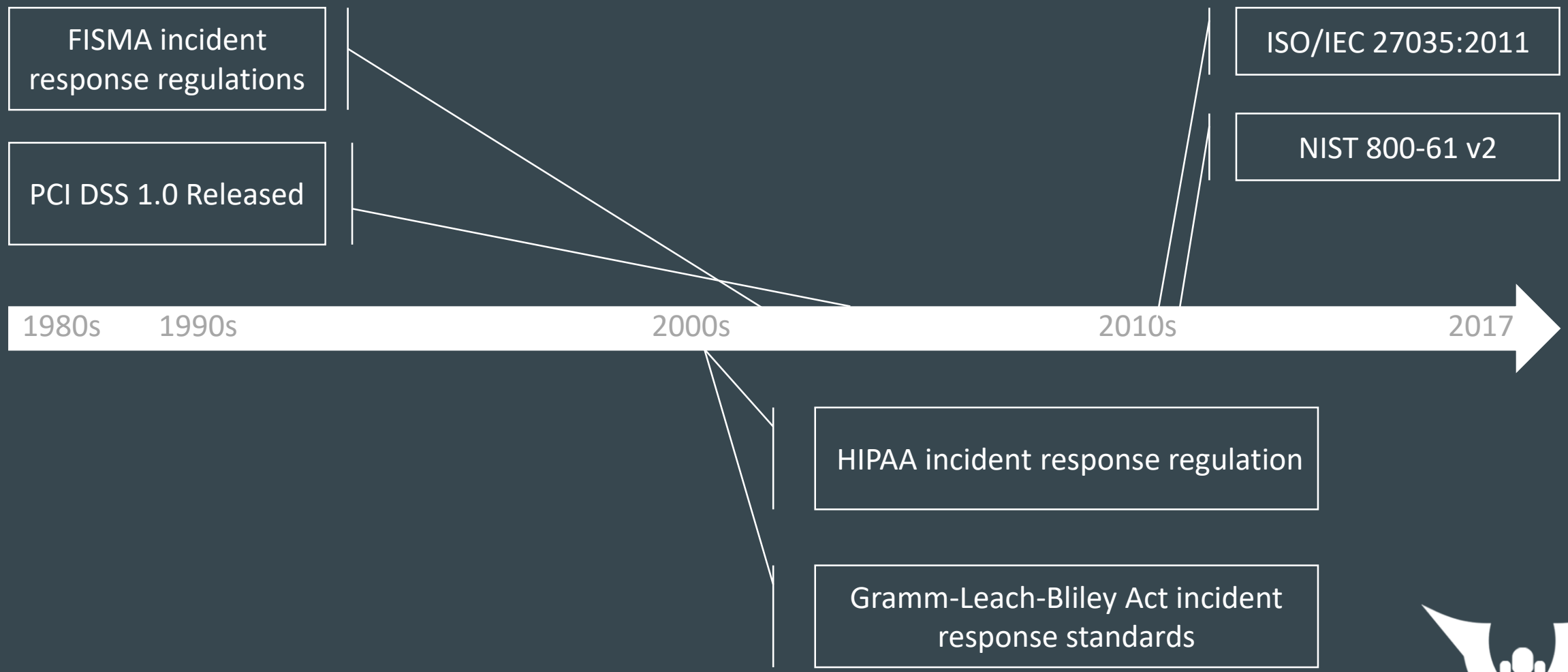
Yesterday

History of Response – Major Events and Response Bodies



infosec elites

History of Response – Standards and Regulations

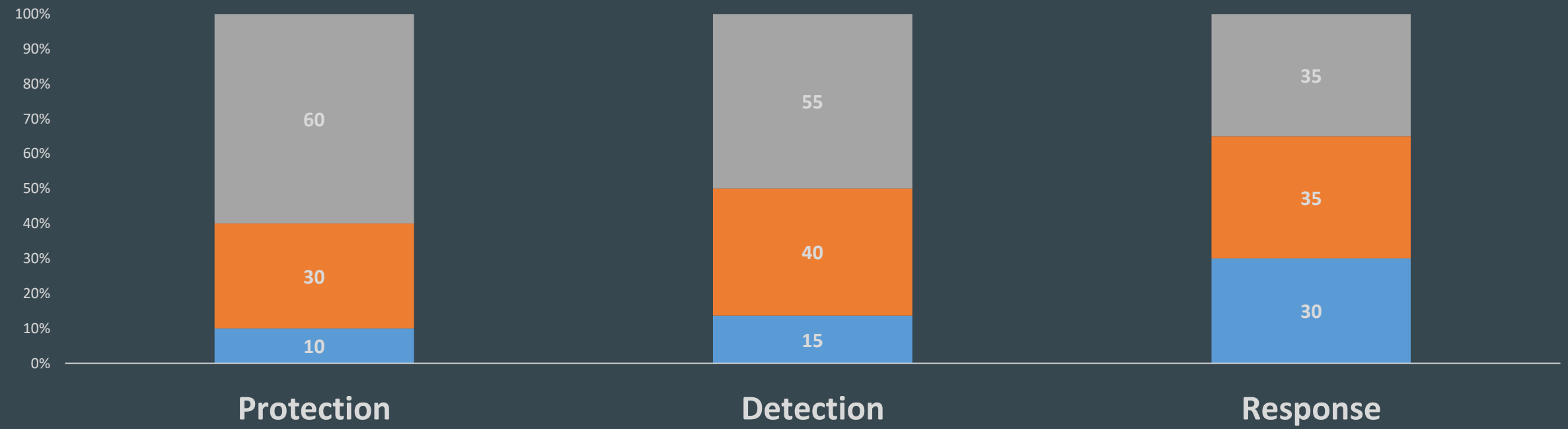


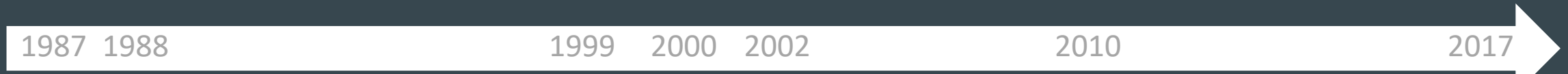
infosec elites

History of Response – The Hidden Change

infosec elites

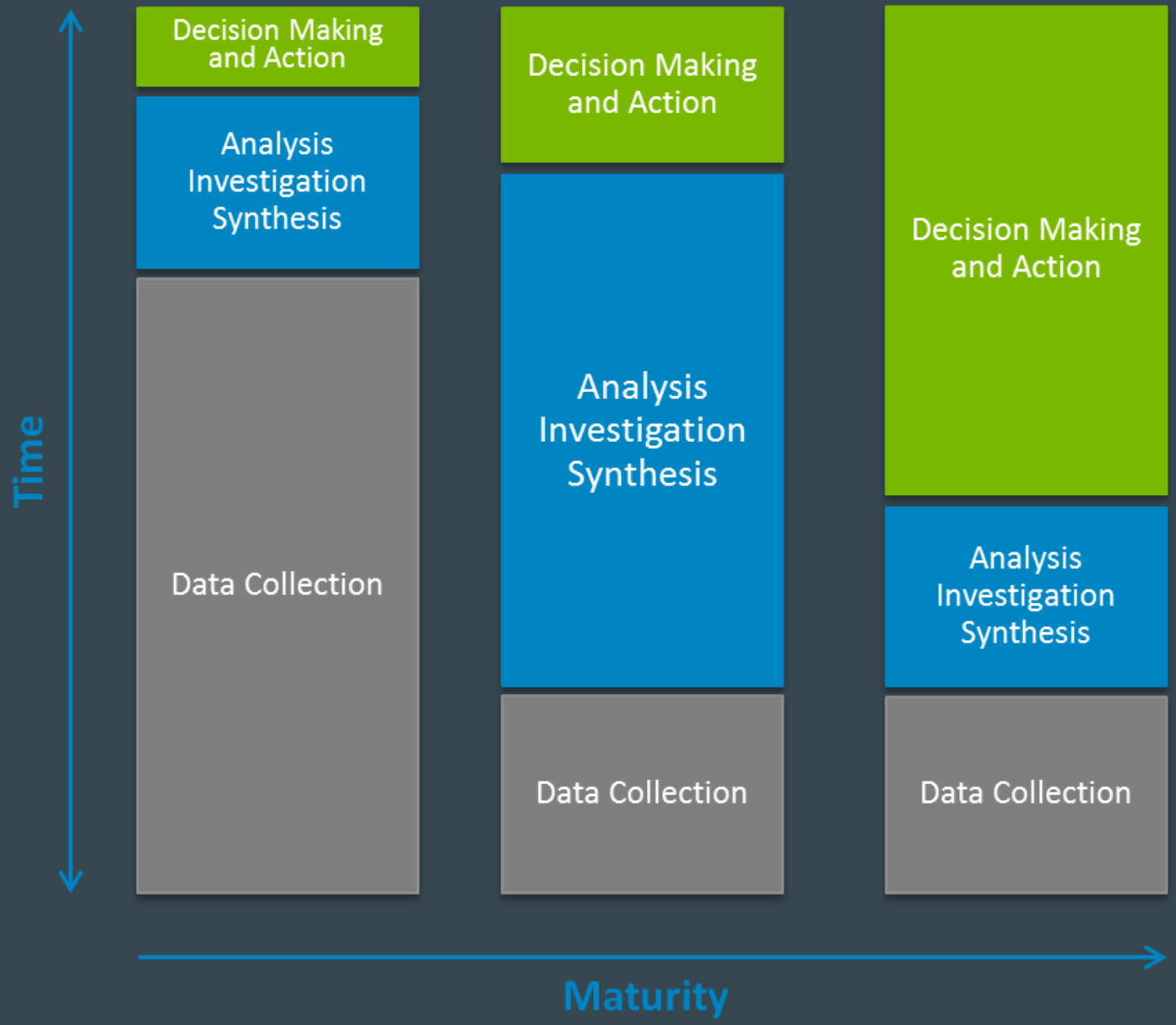
History of Response – The Hidden Change





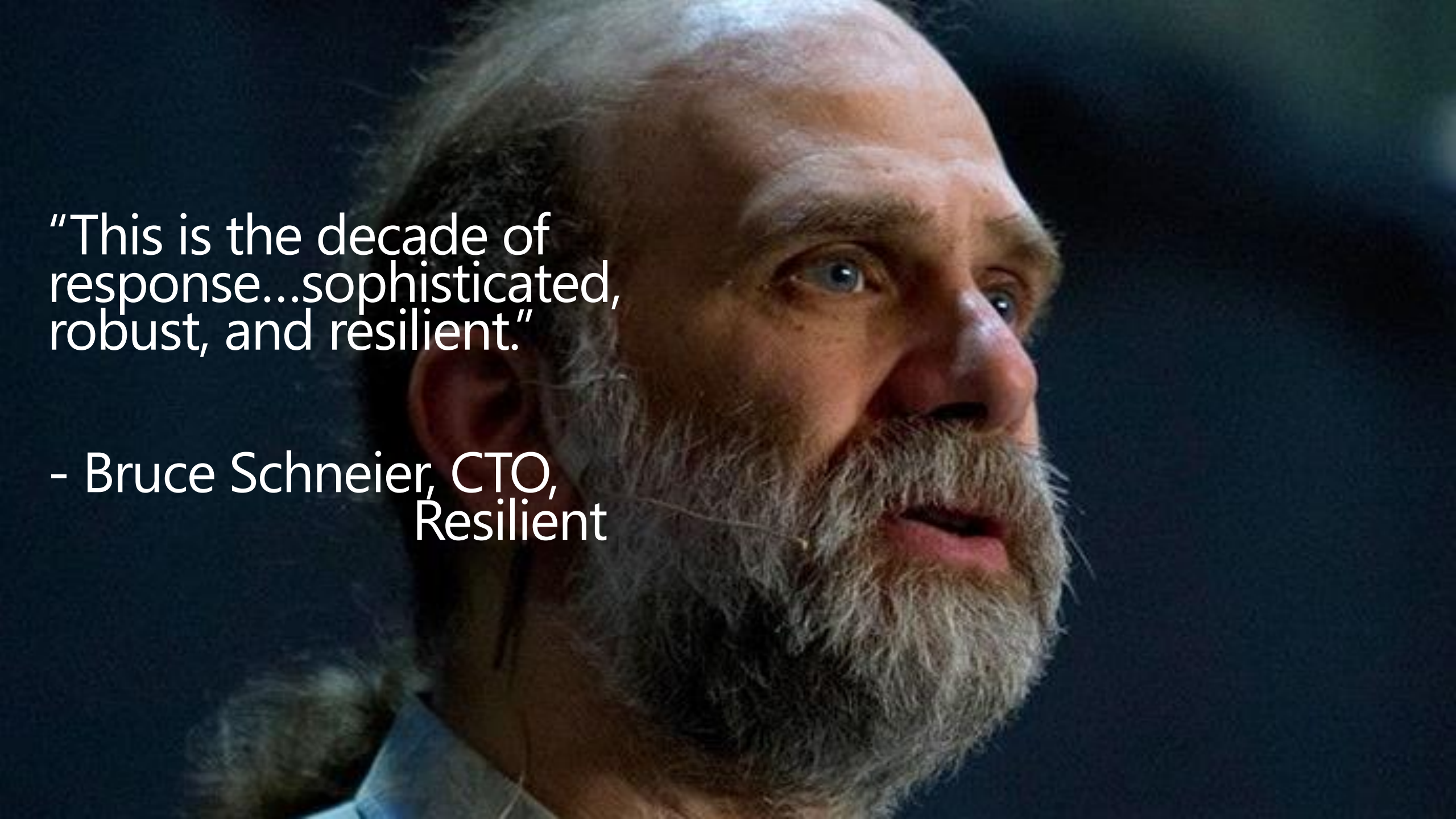
infosec elites

Threat Intelligence Maturity Model



Enhanced from "BI Capability Maturity Model"

infosec elites


“This is the decade of response…sophisticated, robust, and resilient.”
- Bruce Schneier, CTO, Resilient

Need for Maturity Model

Self-Awareness

Objective Assessment

Program Benchmarking

Standardization

Targets Prioritization

IM Maturity Model

1- Ad Hoc	2- Repeatable	3- Defined	4- Managed	5-Optimizing
No IM Process Ad Hoc Procedures Lack or unenforced IM Policy Arbitrary prioritization No incident ownership Limited sources of incidents	Published and enforced policy Established and followed processes Defined sole practice owner Hierarchical and functional escalation matrix Incident response progress is closely monitored Basic automation of IM recording (inventory)	Tailored, updated and followed procedures Defined Roles and Responsibilities Defined and tracked basic KPIs IM Process is aligned with ITIL Clear liaising with internal and external stakeholders KPIs for all incident lifecycle Clear IM and Threat Analytics Metrics generated and tailored-dashboarded Defined collaboration with internal and external bodies Regularly audited and reviewed by internal and external independent bodies Incidents with unknown root cause is escalated	All documentation is reviewed regularly for applicability Cost per incident is calculated and well-known, and continuously tracked. Trend analysis for all KPIs and process parameters Mature and flexible platform for IR with solid integration with Change Management Workflows, Threat Intelligence and SEIM Regular Threat Hunting and Incident Scenarios stress-testing	Regular drills and stress tests for IM procedures, process, and other parameters Automated responses for security controls and network services (as applicable) Business (risk) owners directly involved in integrated-response BIA with most sufficient roles Solid culture of continuous improvements, especially in process optimization and people training

infosec elites

What’s wrong?

What's wrong? (1)

Gap between stakeholders, especially lower levels of detection and analysis

Lack of sufficient decision making power

Organizational politics causes latency and drifts efforts aside

Rapidly growing sources of incidents

People, Process, and Technology not maturing at same pace

Firefighting Mode

Premature IR programs are killers.

infosec elites

What's wrong? (2)

Organizations may not have a response plan but upon an incident, will try to make one.

An incident happened. Weaknesses may be identified. No fix is attempted.

Responders tell intruders what they know.

An incident happened, and management will know about it from news (or may never know).

Responders may not show due diligence with the sensitivity of the handled incident.

Unintentional (incautious) delay in response.

Pulling the plug.

Losing logs (or other evidences)

Organizations purchase and have deployed response (forensics tools) but have not acquired the skill sets to manage and use them.

No eye on the end-point.

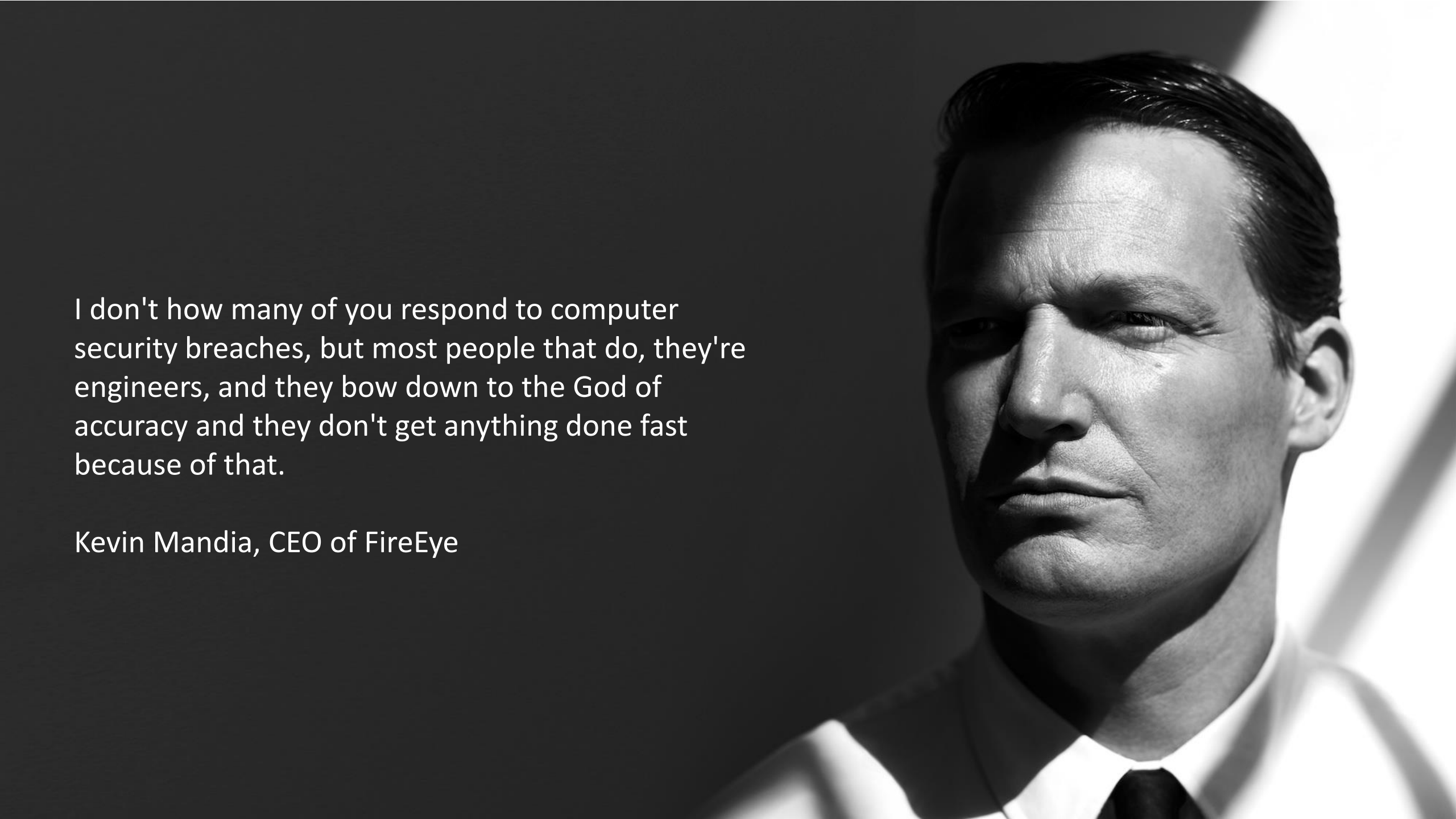
Focusing on the documented procedure and not looking at the overall picture

infosec elites

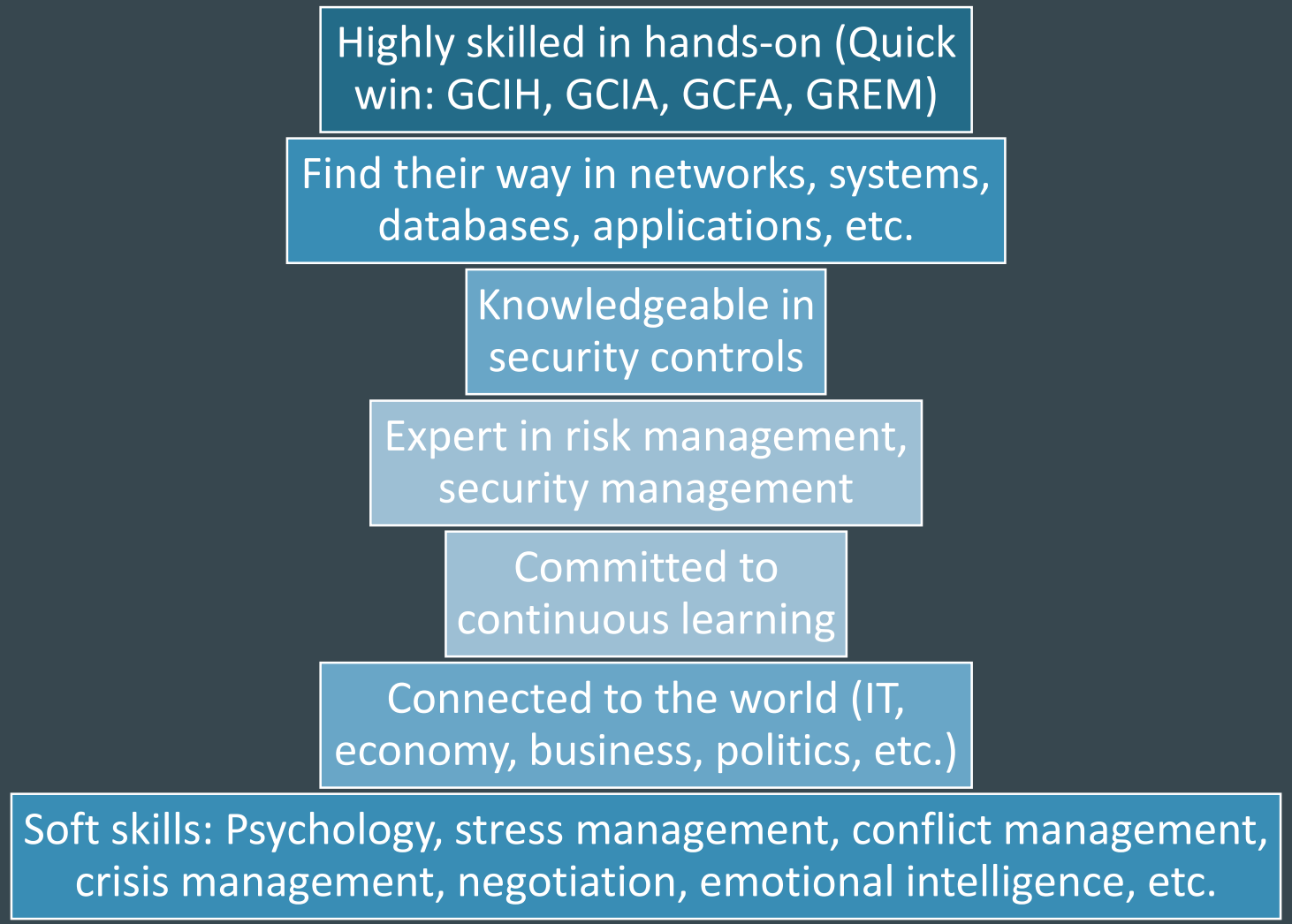
Making it better?

I don't how many of you respond to computer security breaches, but most people that do, they're engineers, and they bow down to the God of accuracy and they don't get anything done fast because of that.

Kevin Mandia, CEO of FireEye



Fit Responders should be:

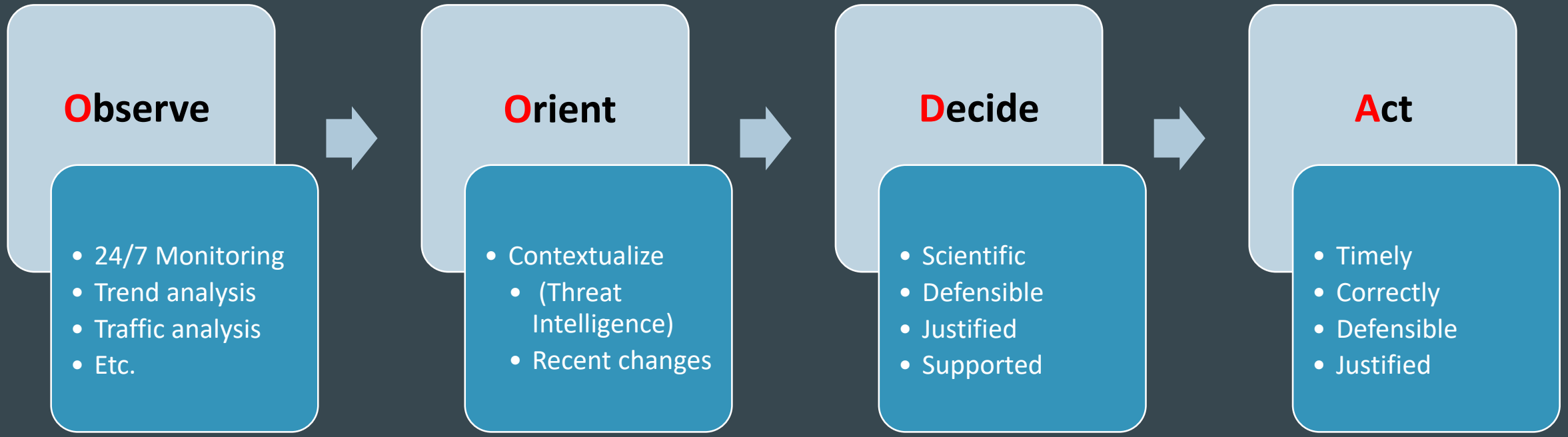


infosec elites

After all, the OODA

Military's OODA

See: John Boyd



TI Model

infosec elites

Change your mindset

Conclusion

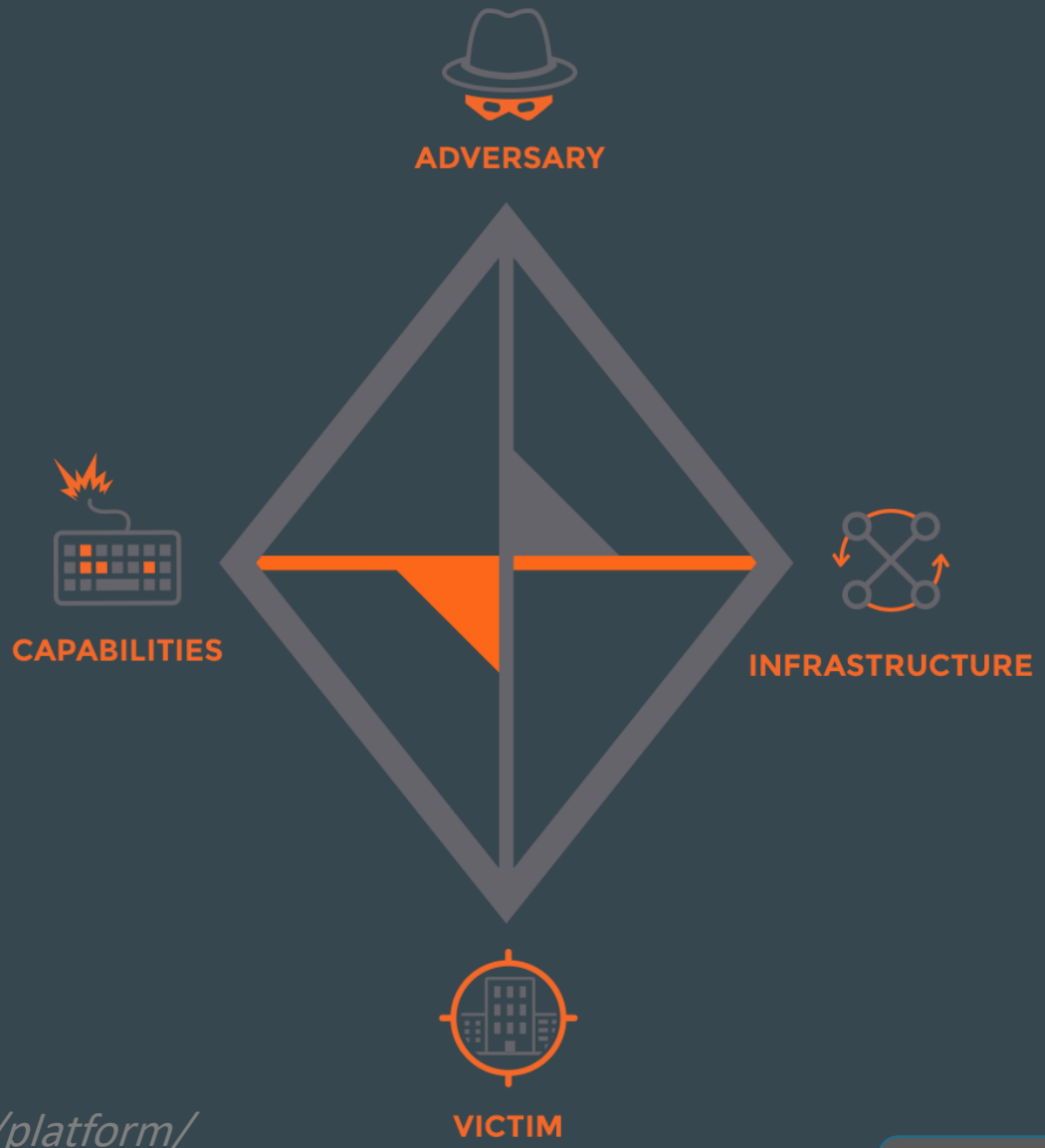
- It’s time of IR.
- Threats (and motives behind them) are becoming more sophisticated and so should IR be.
- You won’t control your data. How would you control your IR?
- More of Process and Technology over People. However, People are controlling the pace and other parameters, because they are the runners as well as the targets.

Any Questions, Comments or Concerns?

Thank you!

Meetup: InfoSec Elites (official website temporary)
http://www.meetup.com/infosecelites/
LinkedIn: https://www.linkedin.com/groups/10321393
Website: infosecelites.com (work on progress)
Twitter: @InfoSecElites
Email: Infosecelites@gmail.com

Threat Context



https://www.threatconnect.com/platform/methodology/

Back

infosec elites

Incident Management vs. Incident Response

- Incident Management is the capability to effectively manage unexpected disruptive events with the objective of minimizing impacts and maintaining to restoring normal operations within defined time limits.

- Incident response is the operational capability of incident management that identifies, prepares for, and responds incidents to control and limit damage, provide forensic and investigative capabilities, and maintain, recover, and restore normal operations as defined in SLAs.

infosec elites

IM Stakeholders' Roles

- Information Security Manager (CISO, CSO)
- Information Services Manager (CIO)
- Chief Operation Officer (COO)
- Incident Response Manager
- Incident Handler
- Investigator
- Forensics Analyst
- Threat Intelligence Analyst
- Security Monitoring Analyst
- IT Security Specialist
- Business Manager (Liaison)
- IT Specialist
- Legal Representative
- HR Representative
- Fraud Investigator
- Public Relations Representative
- Risk Management Specialist

Back

IM Competencies

Network Security	Traffic Analysis	Incident Response	Malware Analysis	Security Architecture
Threat Analysis	Risk Management	Security Management	Data Analysis	Web Security
Data Security	Privacy	Cyber Law	Security Controls	Forensics Analysis
Vulnerability Management	System Security	IS Audit	Access Management	Log Analysis

Back