Carbon Black.

Reducing Liability and Threats through Effective Cybersecurity Risk Measurement

Does Your Security Posture Stand Up to Tomorrow's New Threat?

Christopher Strand

Security Compliance and Risk Officer

The state of The industry (The Threatscape)

Statistics and Observations

Apply Security Control measurement to obtain cyber clarity.

Frameworks and Scorecards that can help reduce threats while bosting data and security accountability

ABOUT ME

Christopher Strand

Security, Risk & Compliance Officer, Carbon Black

- >20 years of IT & Compliance experience
- Certified and trained IT Auditor and Security assessor
- Oversees development of security solutions that help deploy positive security to improve compliance and risk posture
- Held leadership positions at many leading Security and compliance companies

WE HAVE TO DEFEND AGAINST…ALL OF THIS

'Darkhotel' hack targets executives using hotel Internet

Using hotel Wi-Fi networks, the hackers are able to infect corporate executives' computers with malicious software, according to security research firm Kaspersky Lab.

THE CASE FOR SPEED

MEAN TIME
TO **IDENTIFY** BREACH
BY ROOT CAUSE

+

MEAN TIME
TO **CONTAIN** BREACH
BY ROOT CAUSE

FOR A BREACH THAT IS NOT CONTAINED WITHIN 30 DAYS THE AVERAGE ESTIMATED COST INCREASES BY $1 MILLION

Ponemon Institute 2017 Cost of Data Breach Study sponsored by IBM

EXTERNAL THREAT LANDSCAPE

NY DFS ‘17
“First-in-the-nation cybersecurity regulation”

PCI DSS ‘18
Introduces 1-YR incremental changes to keep up with threats

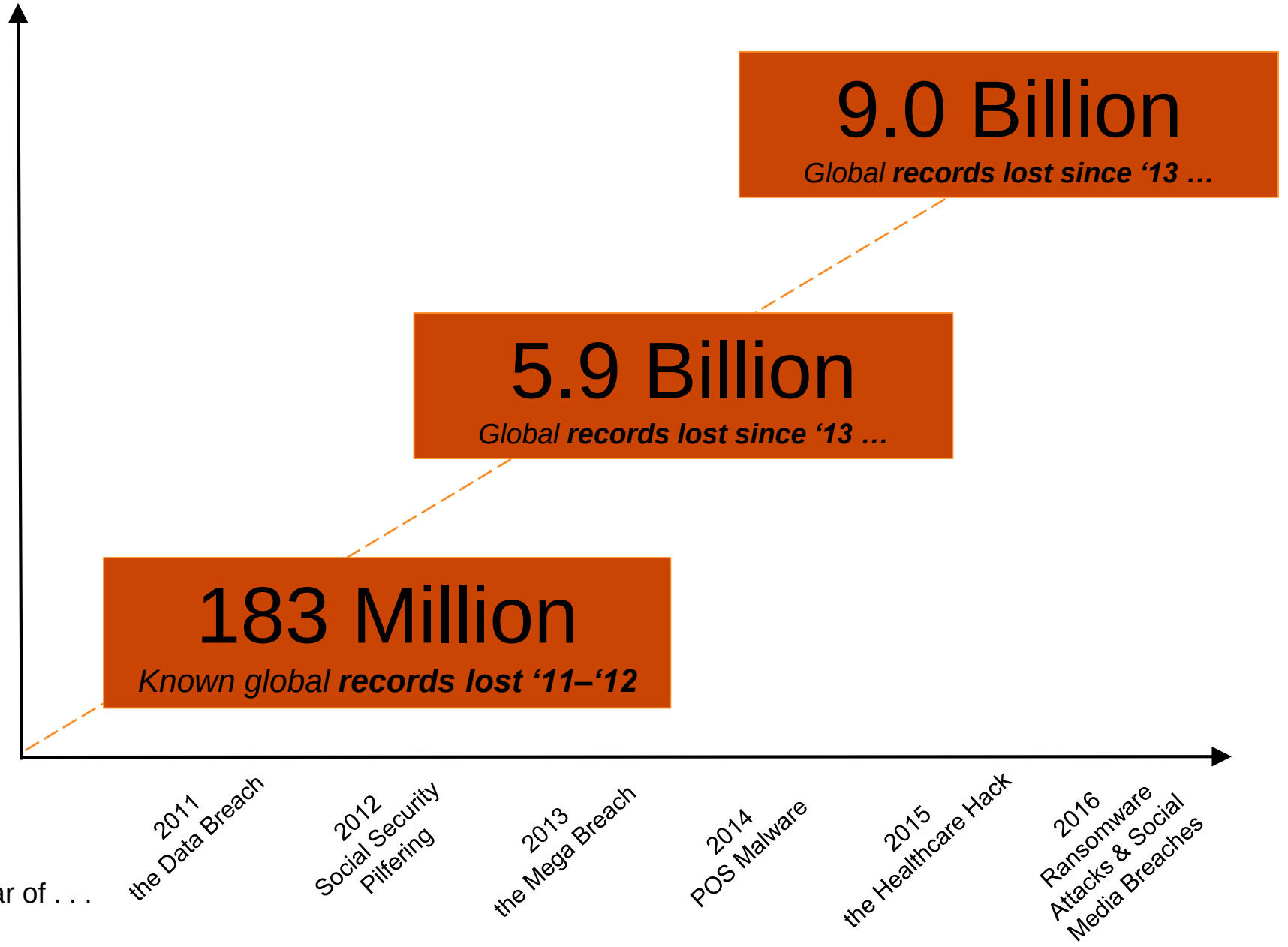
HIPAA ‘16
Stronger enforcement and oversight by OCR Phase 2 Audits

GDPR ‘18
Global implications
Strict penalties

MAS TRM ‘16
New guidelines for outsourcing risk management
Guidance on cloud services

HKMA ‘16
Introduces Cybersecurity Fortification Initiative" (CFI)

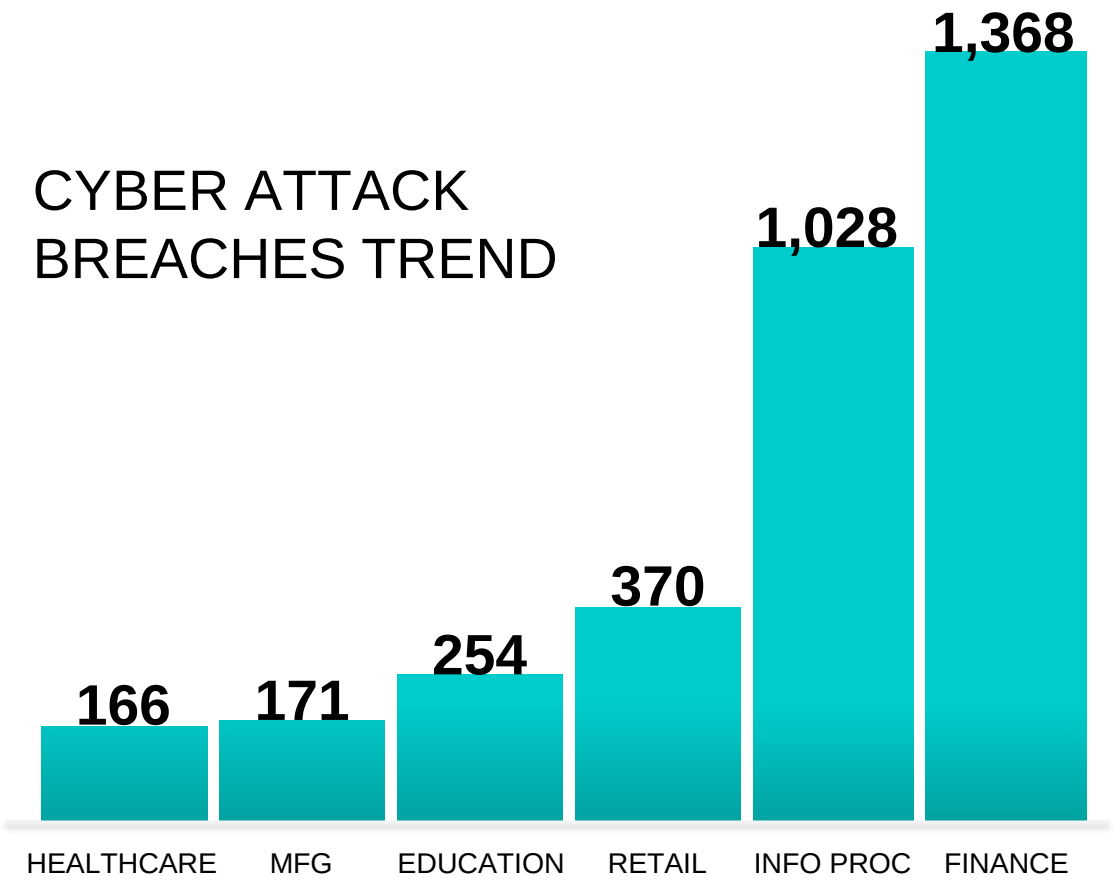
ASD ‘16
Move from Mandatory Top 4 to Essential 8



THREATS TO YOUR ENVIRONMENT

The growth of cybercrime has brought forth innovations that allow malware to rapidly change its appearance

ALL INDUSTRIES ARE UNDER ATTACK



ATTACKERS ARE RELENTLESS & OUTPACING TRADITIONAL PREVENTION

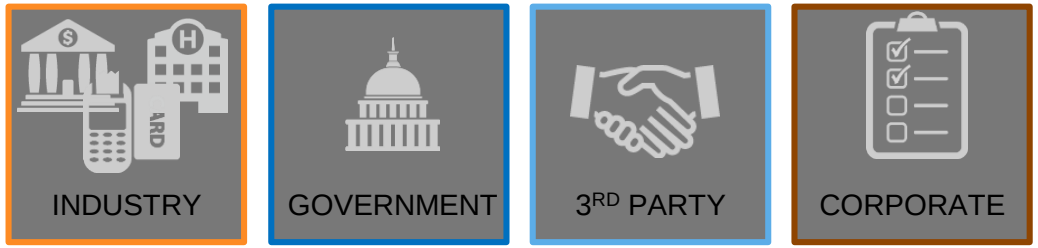
Source: 2016 Verizon Data Breach Investigations Report

CYBER SECURITY NOISE & DISTRACTIONS

External landscape

STRICTER PRIVACY LAWS

Internal mandates & policies

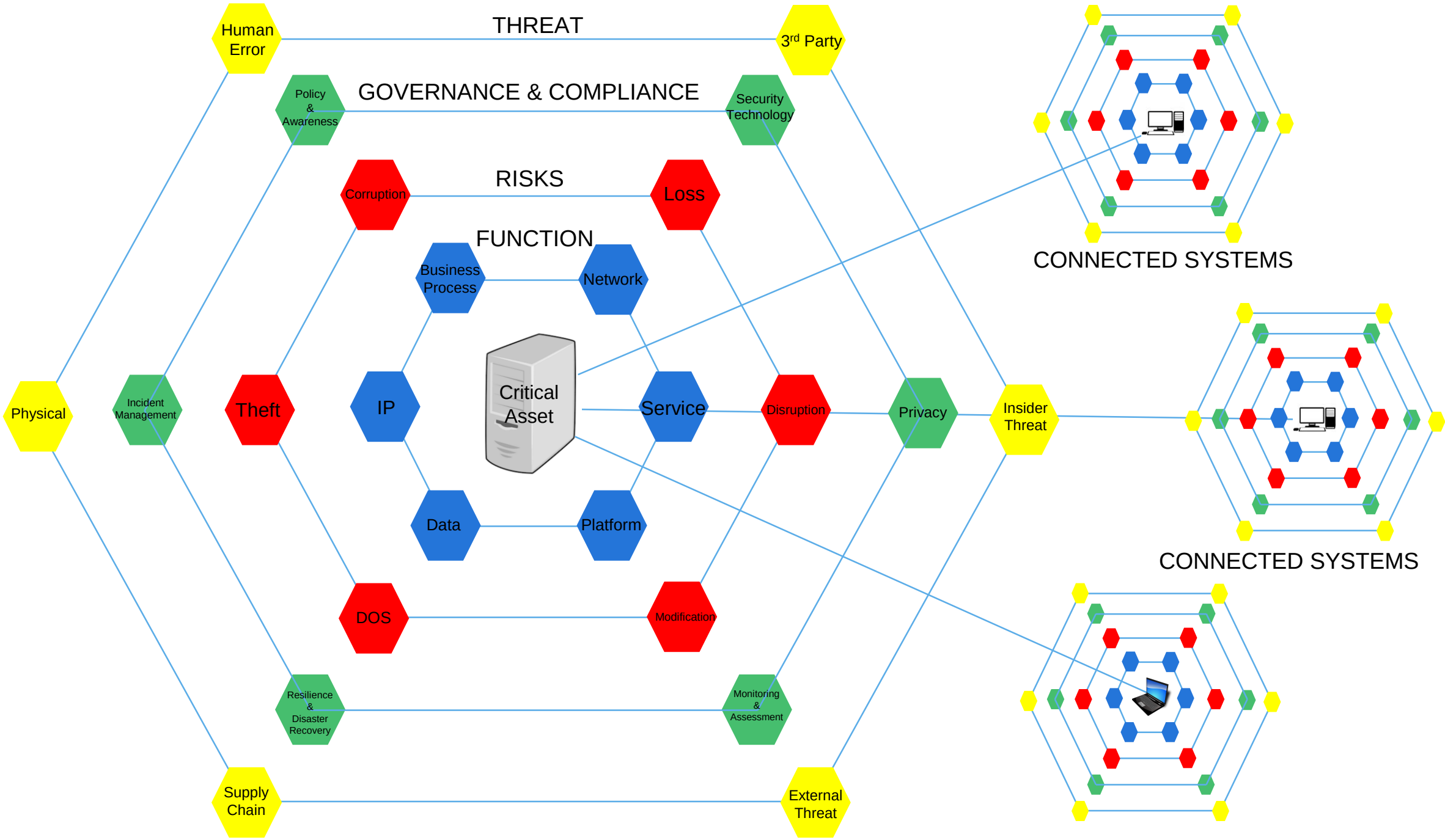


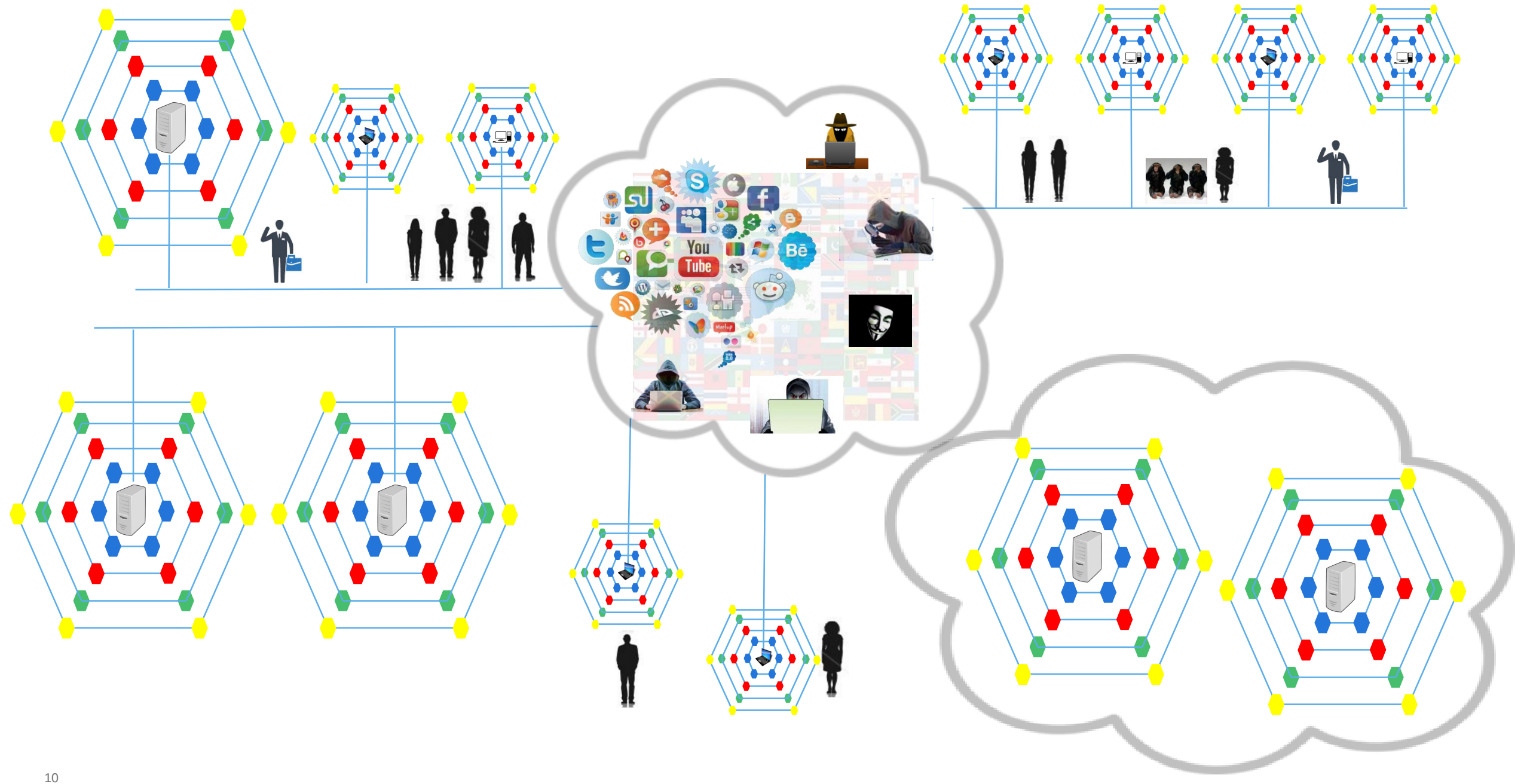
COMPLIANCE CREEP

BLACK HATS OUTPACING WHITE HATS

Threats to your environment

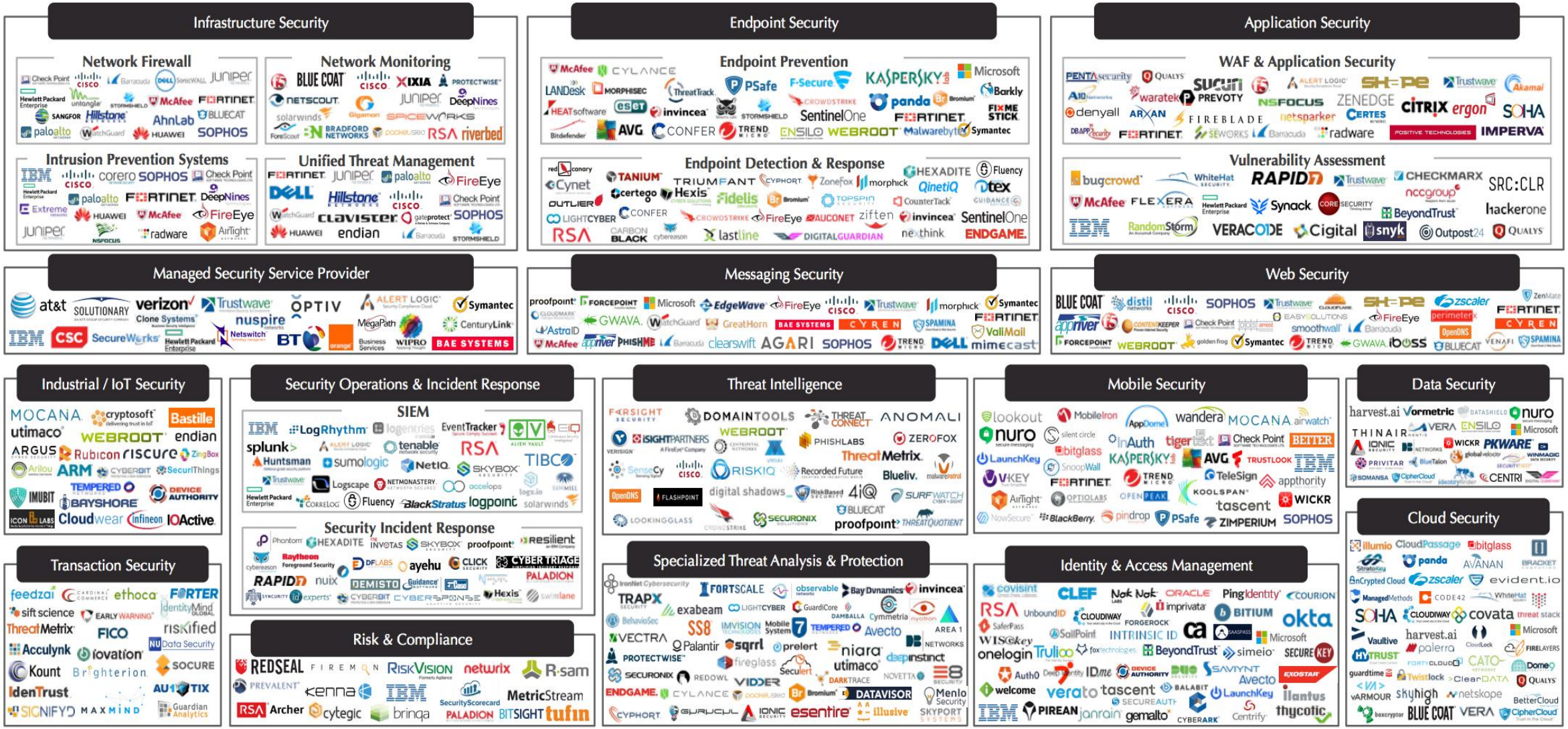
CONSEQUENCES OF NOT KEEPING UP


THREAT
Human Error
3rd Party
GOVERNANCE & COMPLIANCE
Policy & Awareness
Security Technology
RISKS
Corruption
Loss
FUNCTION
Business Process
Network
IP
Critical Asset
Service
Data
Platform
DOS
Modification
Theft
Disruption
Physical
Incident Management
Privacy
Insider Threat
Resilience & Disaster Recovery
Monitoring & Assessment
Supply Chain
External Threat
CONNECTED SYSTEMS
CONNECTED SYSTEMS


You
Tube

CYBERscape: The Cybersecurity Landscape

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



Source: Momentum Partners.

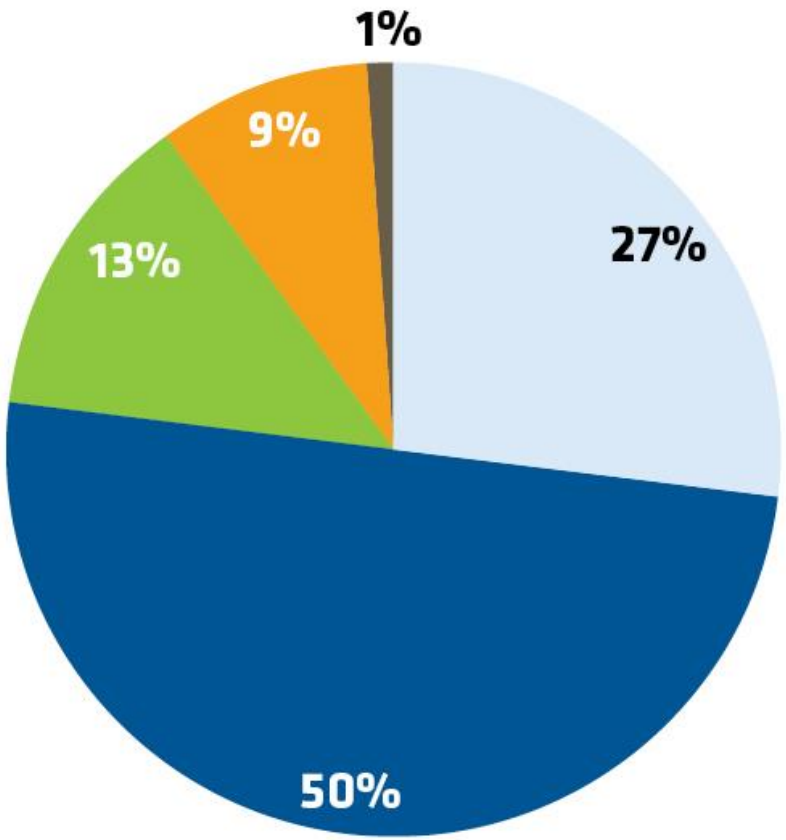
The state of The industry (The Threatscape)

Statistics and Observations

Apply Security Control measurement to obtain cyber clarity.

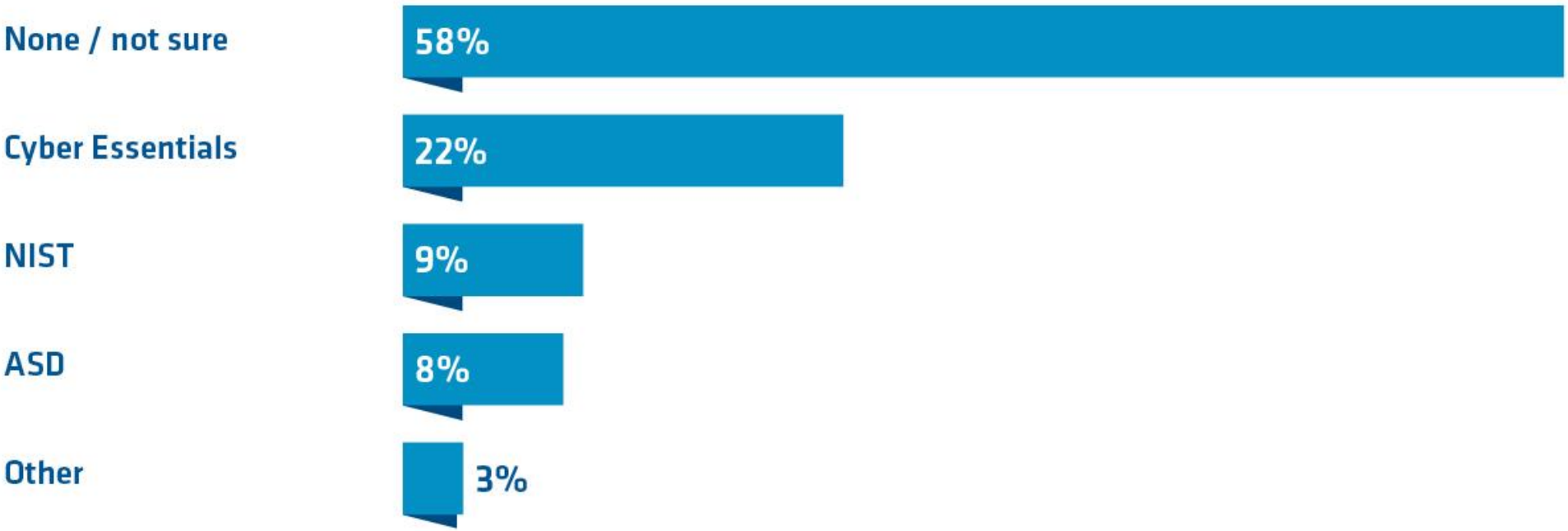
Frameworks and Scorecards that can help reduce threats while bosting data and security accountability

Which of these best matches your general view of the GDPR?

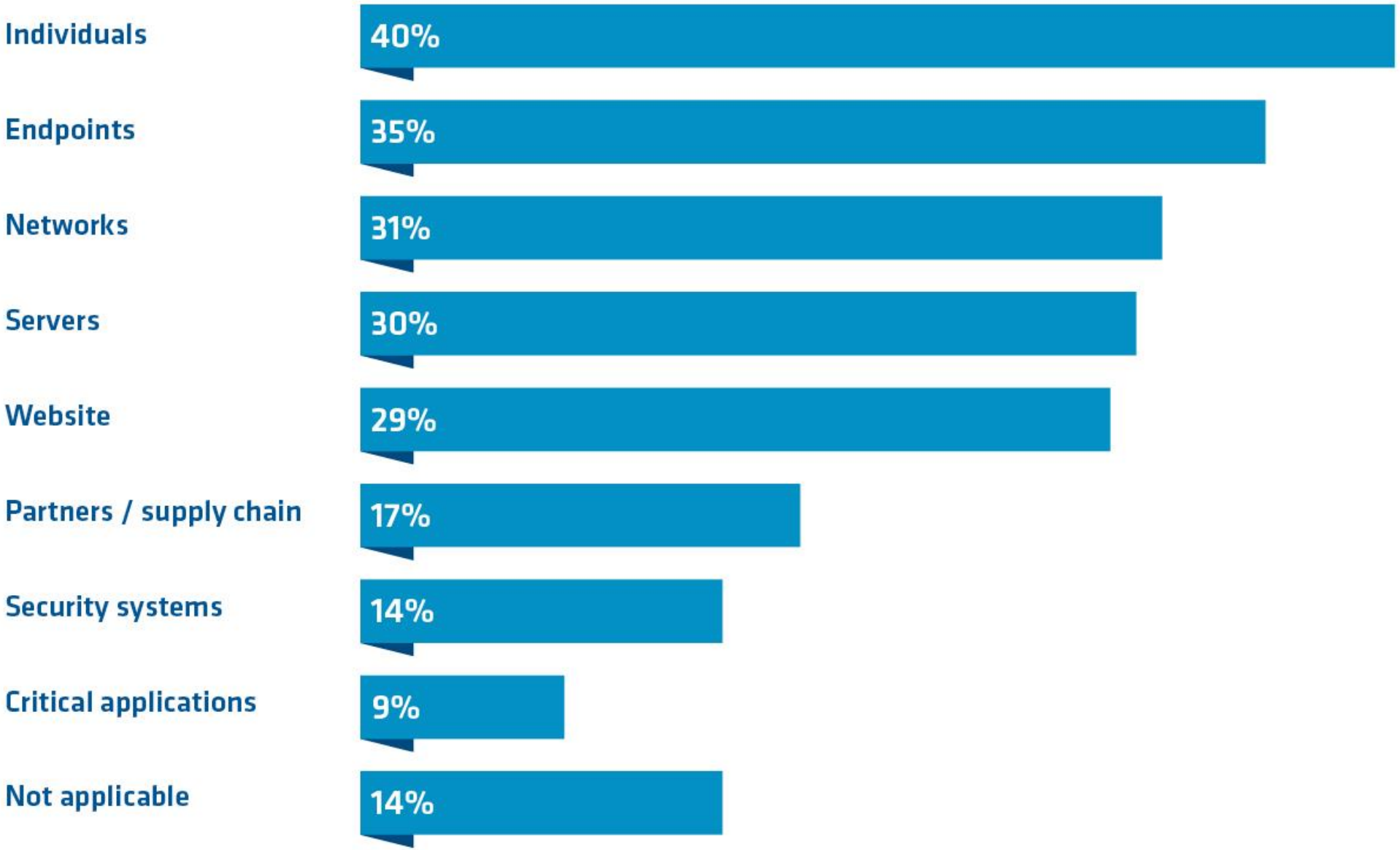


- Very much in favour – it's about time data security and privacy was taken seriously by everyone concerned
- Fairly positive – I believe the subject should be taken seriously but I'm waiting to see how the fine print plays out
- Neither for nor against
- Not 100% convinced of the need – and the penalties seem unduly harsh
- Completely against – it is too onerous to comply with relative to the problems it is designed to resolve

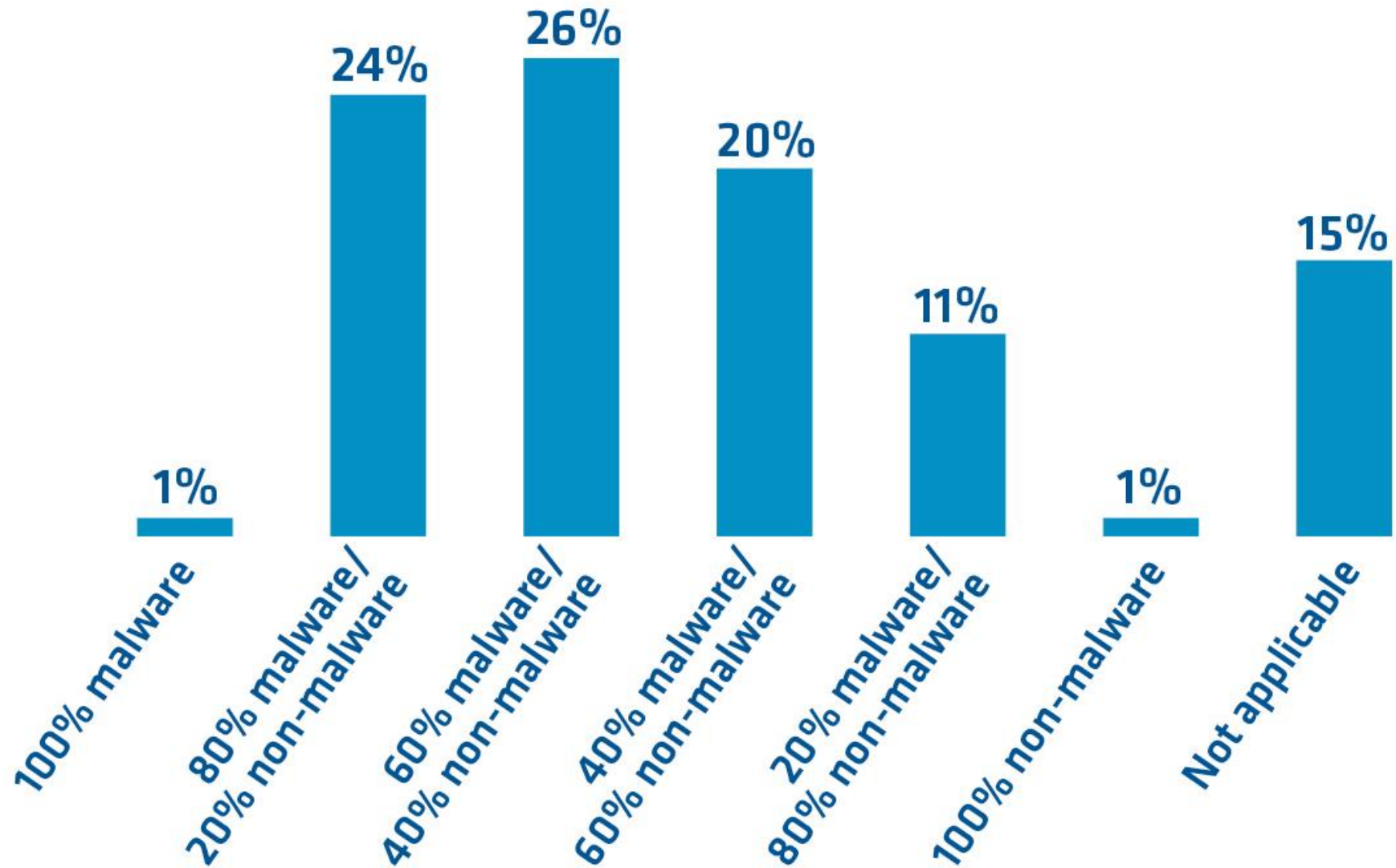
What type of frameworks or technologies are you using to identify data risk under GDPR?



Over the last two years, which parts of the enterprise were attacked by malware or other types of attack?

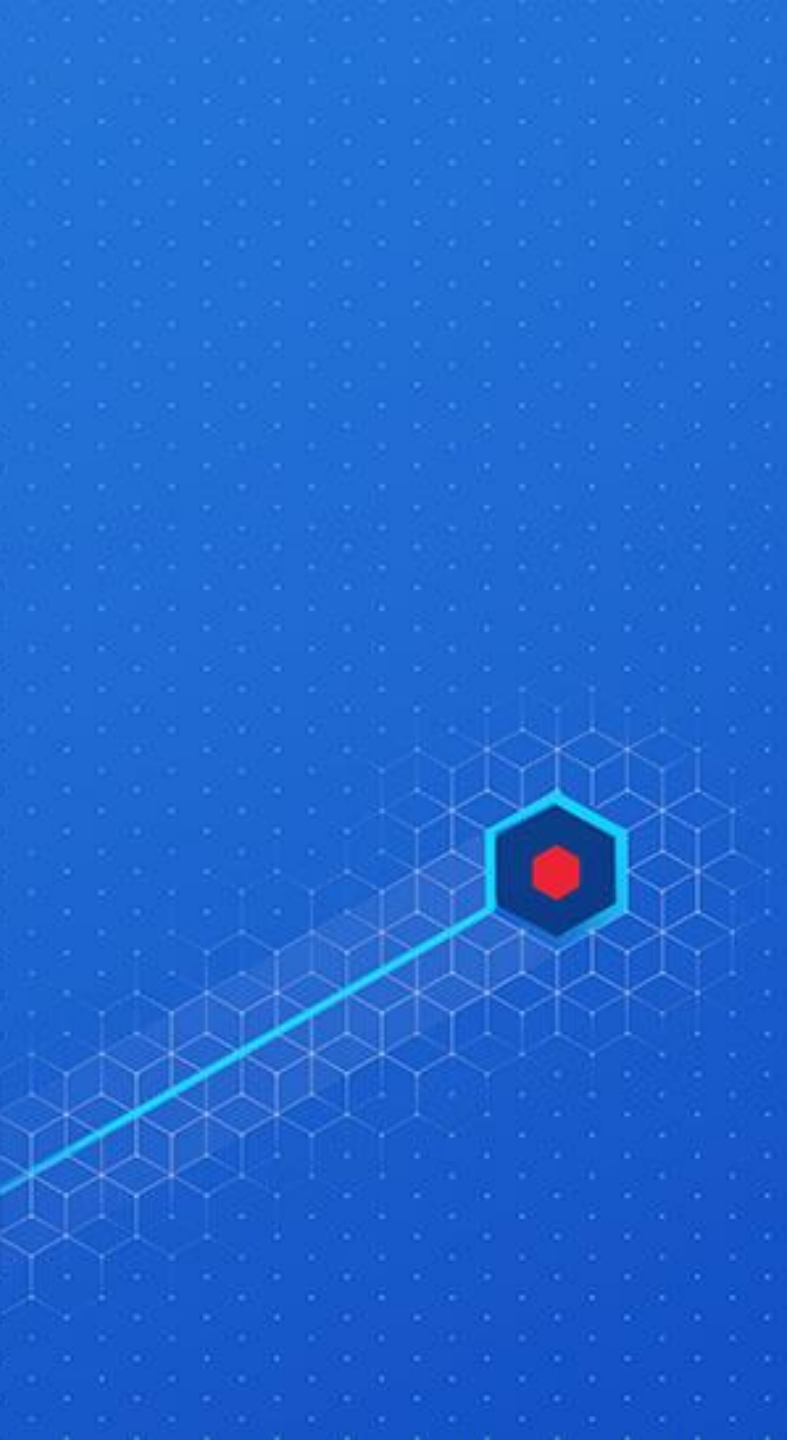


Of the attacks on your organisation in the last two years what was the split between malware based and non-malware (fileless) based attacks?



What changes are/will you be making to comply with the GDPR?

Reviewing data discovery and data deletion capabilities	61%
Providing additional data security measures	49%
Changing the way personal data is stored and/or transmitted	45%
Reviewing our business partners' uses of our data	43%
Reviewing customer-facing infrastructure	43%
Integrating Privacy Impact Assessments into our processes	39%
Reviewing our use of cloud-based applications and services	38%
Employing a Data Protection Officer	26%
Reducing the quantity of data we collect	22%
Creation of board-level team to create and execute GDPR strategy	20%
Engaging a third-party consultancy	18%



The state of The industry (The Threatscape)

Statistics and Observations

Apply Security Control measurement to obtain cyber clarity.

Frameworks and Scorecards that can help reduce threats while bosting data and security accountability

DATA SECURITY RISK MEASURE RECIPE

FRAMEWORK

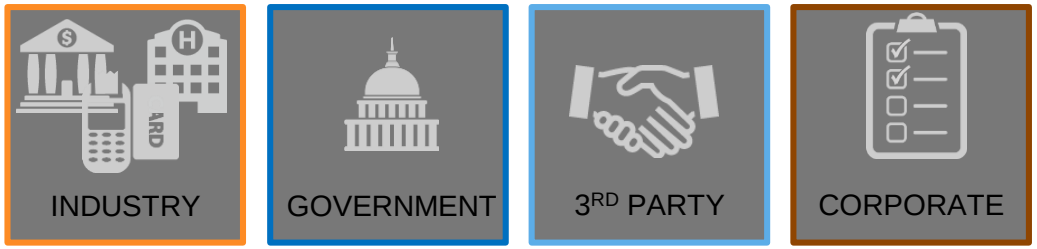
Prioritize BAU process & governance

POLICY

Focus on data residency & high-risk assets

MEASURE

Proactively assign risk & access



GET TO BASELINE

IDENTIFY CURRENT RISK TO POLICY

PRIORITIZATION VULNERABILITIES

MATURE YOUR DEFENSES

APPLY A FRAMEWORK

National Institute of Standards and Technology

EU General Data Protection Regulation

Federal Financial Institutions Examination Council

COBIT 5
An ISACA Framework

Payment Card Industry Data Security Standard

Sarbanes-Oxley
Gramm–Leach–Bliley Act

CREATE A POLICY

NIST 800 Series

CIS CSC Top 20

FFIEC Cybersecurity Assessment Tool (CAT)

SOC TYPE I & II

Payment Card Industry Data Security Standard 3.2

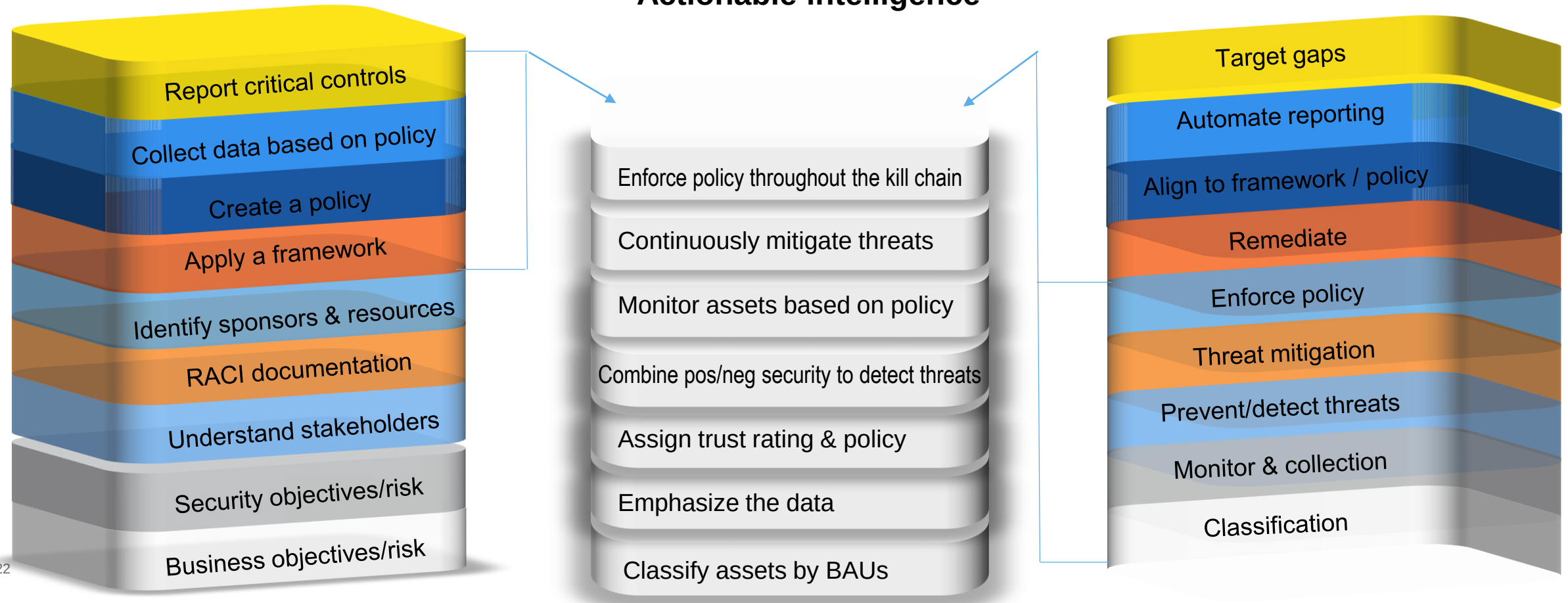
Sarbanes-Oxley Gramm–Leach–Bliley Act

PRIORITIZE BASED ON BAU PROCESS & CRITICAL DATA

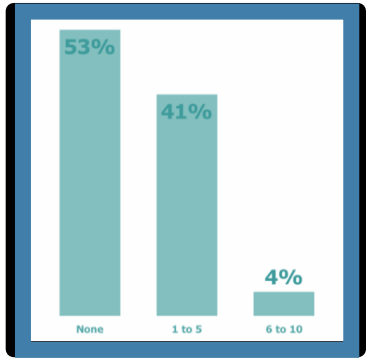
Merge Traditional IT and Cyber Risk Audit Process

Measure effectiveness and risk to critical security controls against:

Corporate policy
People, process and technology
Actionable intelligence



RANSOMWARE: A LUCRATIVE BUSINESS



12-MONTH VOLUME

SOURCE: OSTERMAN, PANDA & McAFEE

- 41% of companies hit 1 to 5x
- ’05: New strains every 12 min
- ’16: Every four sec

Bad guys:

Traditional defense strategies can’t keep up

YEARLY GROWTH

SOURCE: FBI & CSO Online

- ‘15: $325M
- ‘16: $1B
- by 2020 range up to $200B

Bad guys:

Business growth that works

SCALABLE

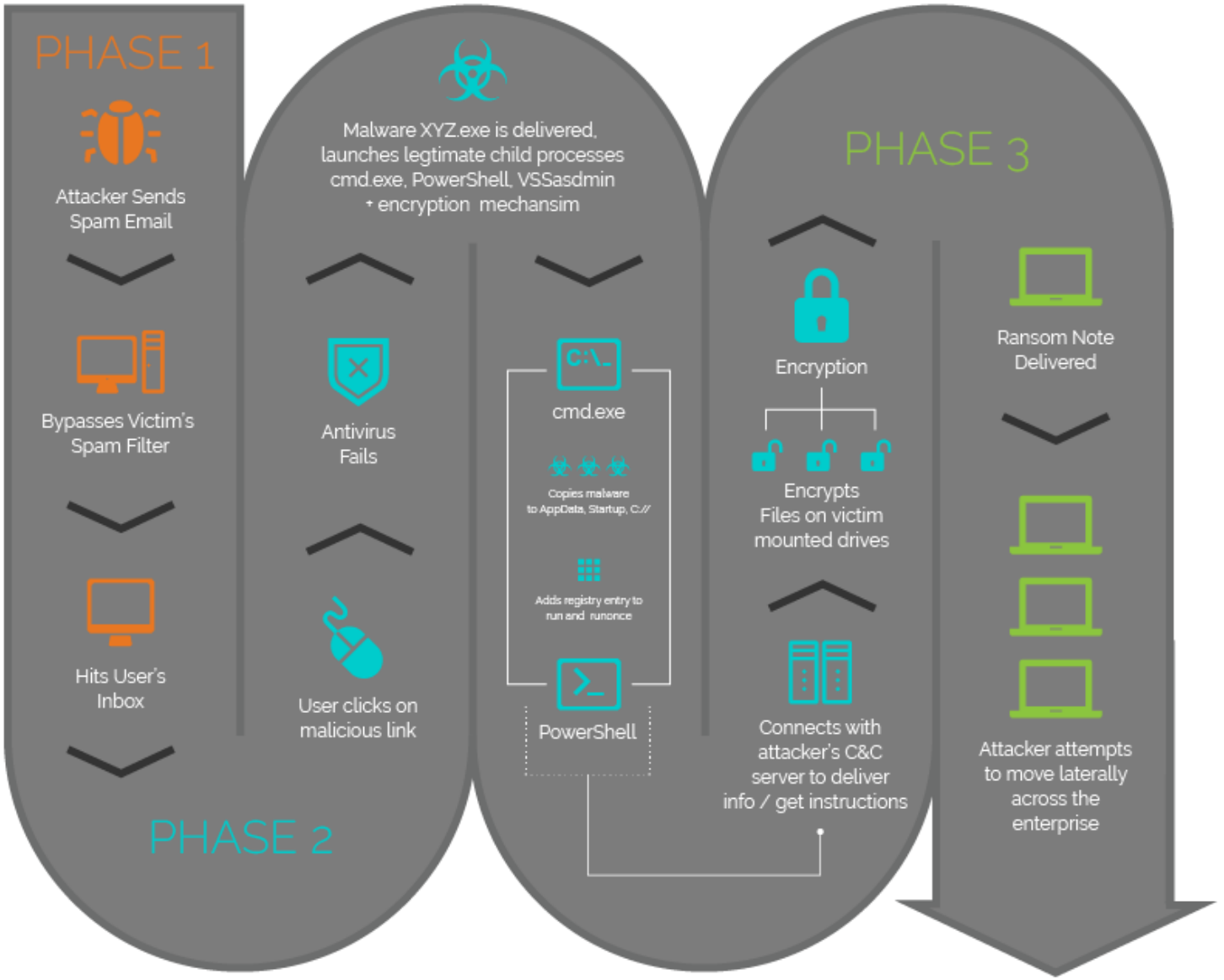
SOURCE: CERT

- ‘16: 4K daily attacks
- ↑300% from ‘15

Bad guys:

Achieve mass-scale with victim volume

Anatomy of a Ransomware Attack



RANSOMWARE: CKC & BASELINE SECURITY CONTROLS

PHASE 1
Preparation

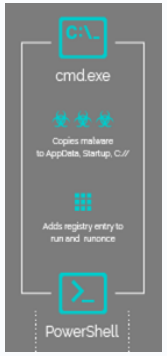
Recon

Weapon

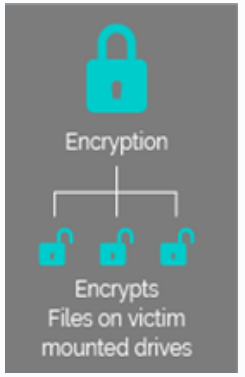
Deliver

PHASE 2
Active Breach

Exploit

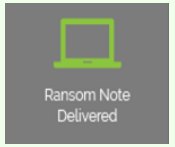


Install



Command & Control

PHASE 3
Response/Fallout



Action(s) on Target

Identify Assets → Detect → Protect → Respond → Recover

WHAT'S THE RISK?

Identify Assets	Detect	Protect	Respond	Recover
Where is data residency? Who/what has access? What are they doing with it?	Where is it vulnerable? What are we doing to fix it?	How well is it protected? What's the newest threat?	What is happening? Where did it start? How long?	How quickly was it resolved? How do I enforce it?

Identify Assets

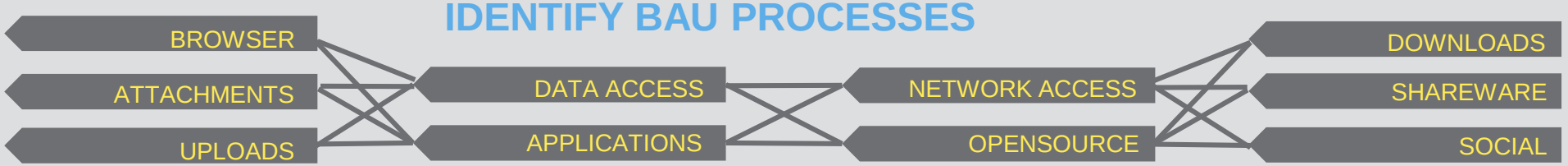
CONTROLS: UNDERSTANDING AND CATAGORIZING

COMMON SECURITY ERRORS:

Not considering Technology, Processes, and People within your BAU
Not checking Default access to sensitive data and Building Business Justification
Not mapping users to BAUs

1 PRIORITIZE HIGH-RISK AND VULNERABLE DATA AND ASSETS

2 IDENTIFY BAU PROCESSES



3 ASSIGN TRUST TO BAU PROCESSES BY BUSINESS JUSTIFICATION

IT-Driven Trust
- *Trusted* Updater (e.g., SCCM, Chrome)
- *Trusted* Directory (e.g., \\gold_dir)
- *Trusted* Publisher (e.g., Mozilla)
- *Trusted* User (e.g., help_desk)

CLOUD-Driven Trust
- Threat intelligence
- Risk ratings
- Automatically approves reputable software

Permissions
- Role-based
- User approval
- IT approval
- Do not let run

PRIORITIZE ASSETS AND PROCESSES BY RISK

Detect

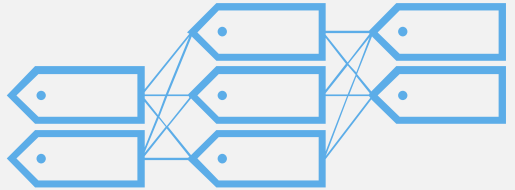
CONTROLS: MONITOR AND COLLECT INTELLIGENCE

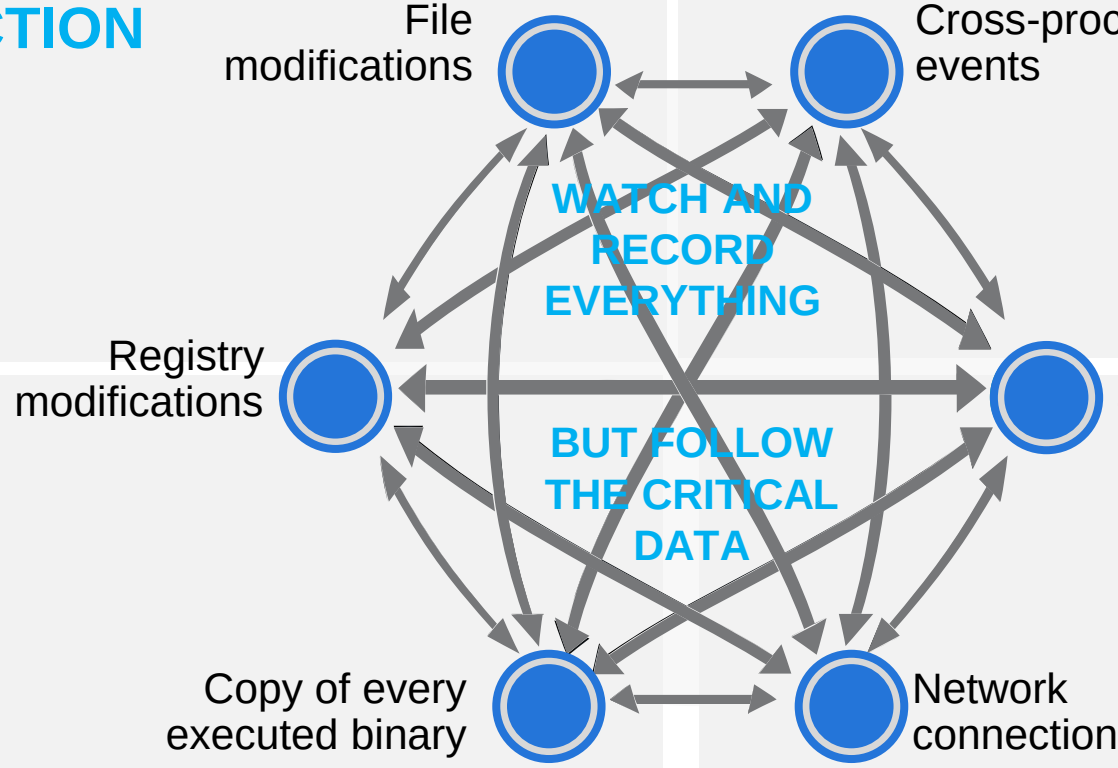
COMMON SECURITY ERRORS:

Collect without context or classification
Not focusing on high-risk assets
Not following the critical data
Not taking your BAUs and building your monitoring strategy on the front end

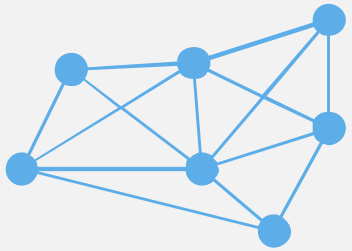
Event COLLECTION

Event BEHAVIORS





ENFORCE Policy



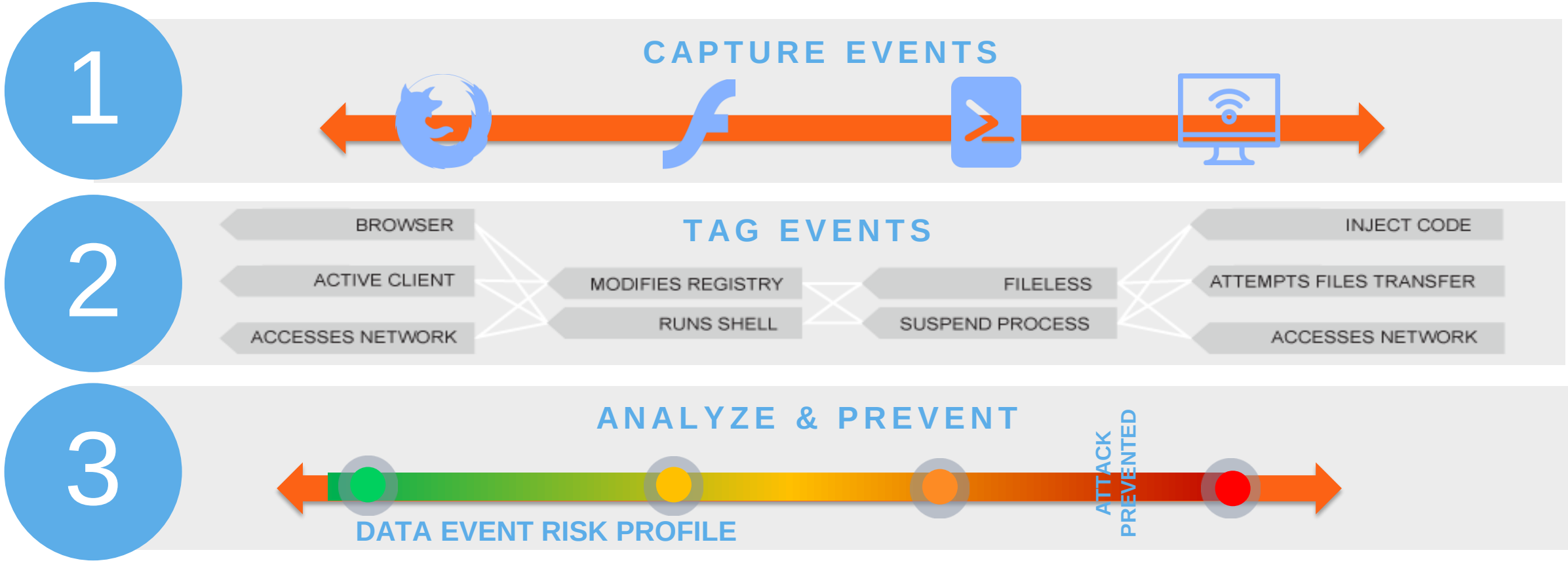
Event ANALYTICS

Protect

CONTROLS: PROTECTION AND ACCESS CONTROLS

COMMON SECURITY ERRORS:

Relying only on negative security
Point – in – Time defense strategies
Inability to get to root cause of an event



Respond

CONTROLS: THREAT MITIGATION AND REMEDIATION

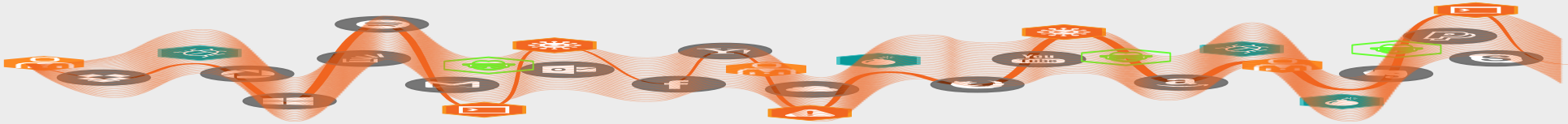
COMMON SECURITY ERRORS:

Sifting through large amounts of data to gather in-scope information
Not assigning alerts to change-detection events
Analyzing all change

1

2

USER BEHAVIOR, IOC'S, UNWANTED CHANGES



3

CONTROL AND PROVE ENFORCEMENT

Filter out irrelevant changes on the front end
Focus on authorized critical changes
Scope out large amounts of data on in-scope
Monitor log files for better audit and chain of custody

CONTROL
- Change
- Access
- Privilege

Create a scorecard with a prioritized approach to close gaps in your data security policy

Recover

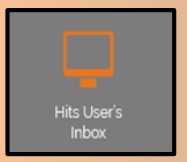
CONTROLS: ASSESS RISK AND CLOSE GAPS

PHASE 1

Preparation

Recon

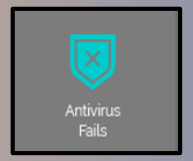
Weapon



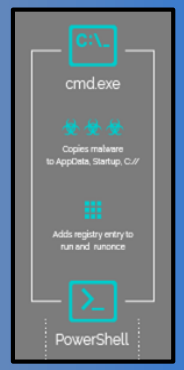
Deliver

PHASE 2

Active Breach

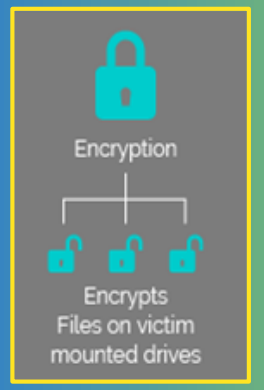


Exploit



Install

Command & Control



PHASE 3

Response/Fallout

Action(s) on Target

Conform assets

Protect data integrity

Proactively monitor critical systems

Threat mitigation

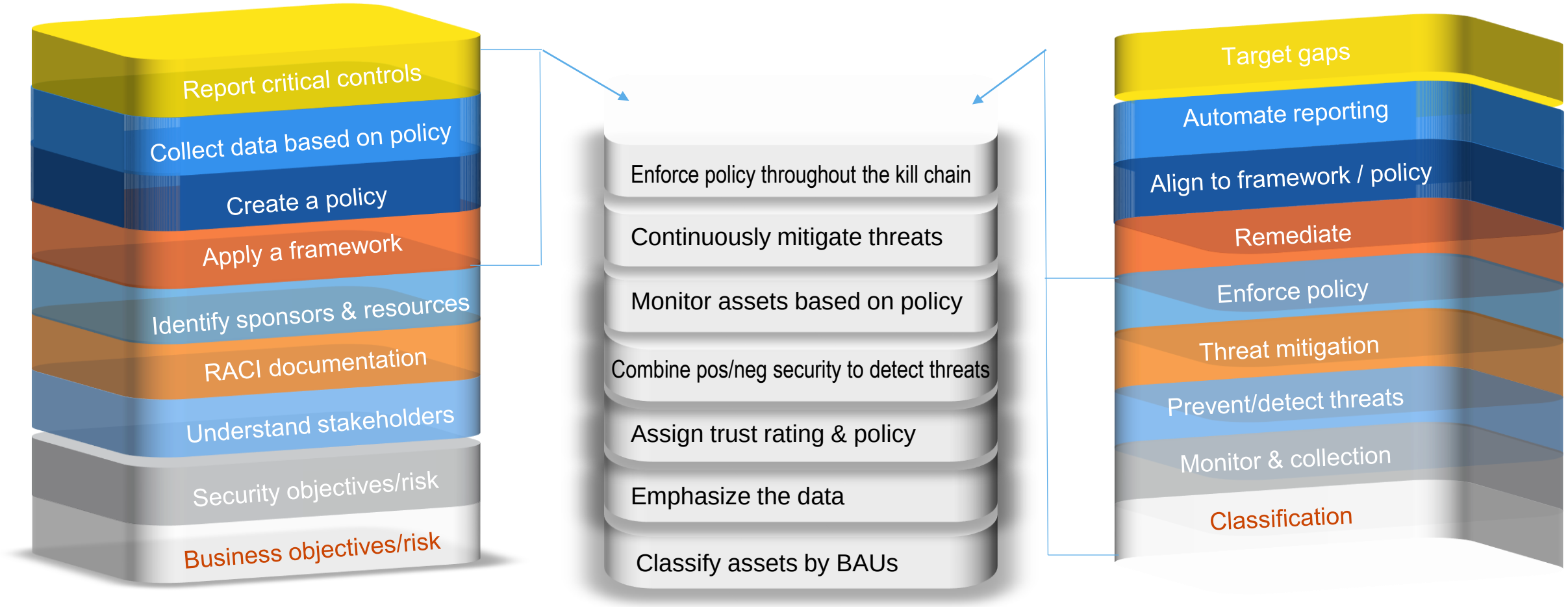
Enforce security and compliance policy

CLOSE THE GAPS

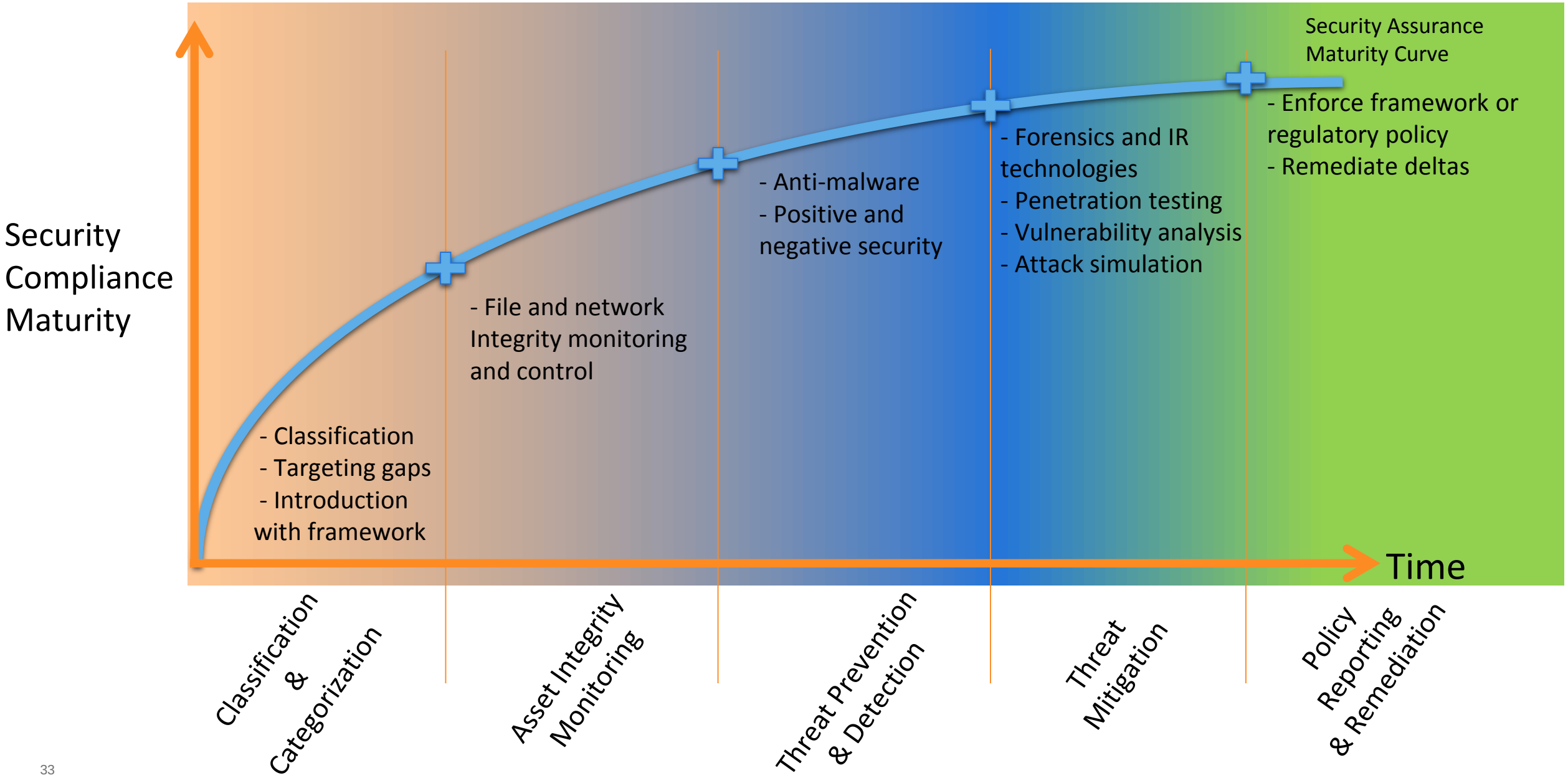
- *The state of The industry (The Threatscape)*
- *Statistics and Observations*
- *Apply Security Control measurement to obtain cyber clarity.*
- *Frameworks and Scorecards that can help reduce threats while bosting data and security accountability*

CYBER SECURITY SCORECARD

Paradigm shift to close the SECURITY gap across the CYBER KILL CHAIN



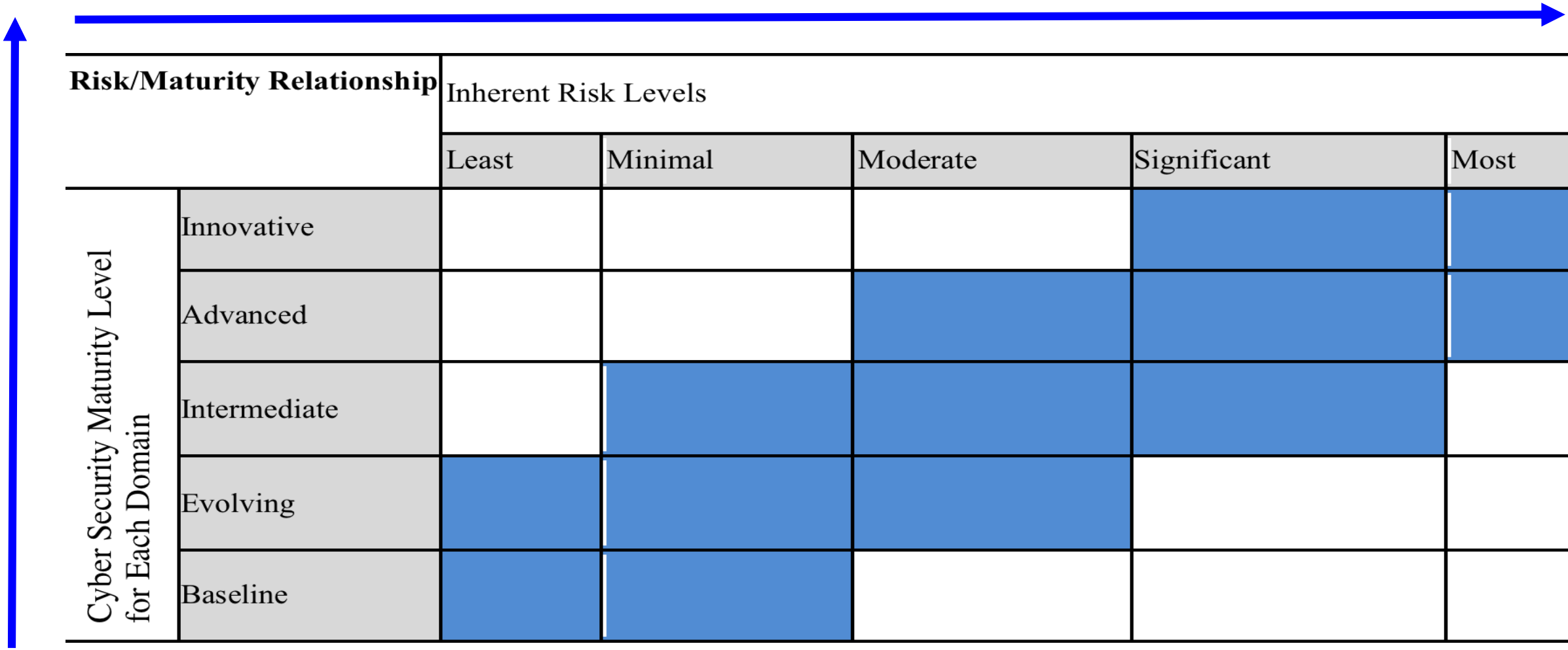
TECHNICAL CONTROL SOLUTION FRAMEWORK



DOCUMENTING YOU CYBER RISK TOLERANCE

Cyber Risk	Impact	Tolerance	Action
Loss of customer data	Business reputation	Very low	Prioritize and fix
Loss of IP	Competitive edge	None	Fix immediately
Loss of business continuity	Profitability targets	Very low	Prioritize and fix
Web defacement / denial of service	Customer experience	Acceptable w/ sr. mgmt. approval	Review and prioritize
Loss of data integrity	Internal apps and data	None	Fix immediately

RISK MATURITY MATRIX



Risk/Maturity Relationship		Inherent Risk Levels				
		Least	Minimal	Moderate	Significant	Most
Cyber Security Maturity Level for Each Domain	Innovative					
	Advanced					
	Intermediate					
	Evolving					
	Baseline					

IT OPERATIONS AND SECURITY MATURITY SCORECARD EXAMPLE - ISO

ISO Control	0	1	2	3	4	5
Risk Management						
Policy						
Organization						
Asset Management						
Communications / Operations						
Access Control						
Threat Protection and Development						
Incident Management						
Business Continuity						

Legend:

0 - Non Existent
1 - Initial
2 - Repeatable
3 - Defined
4 - Managed
5 - Optimized

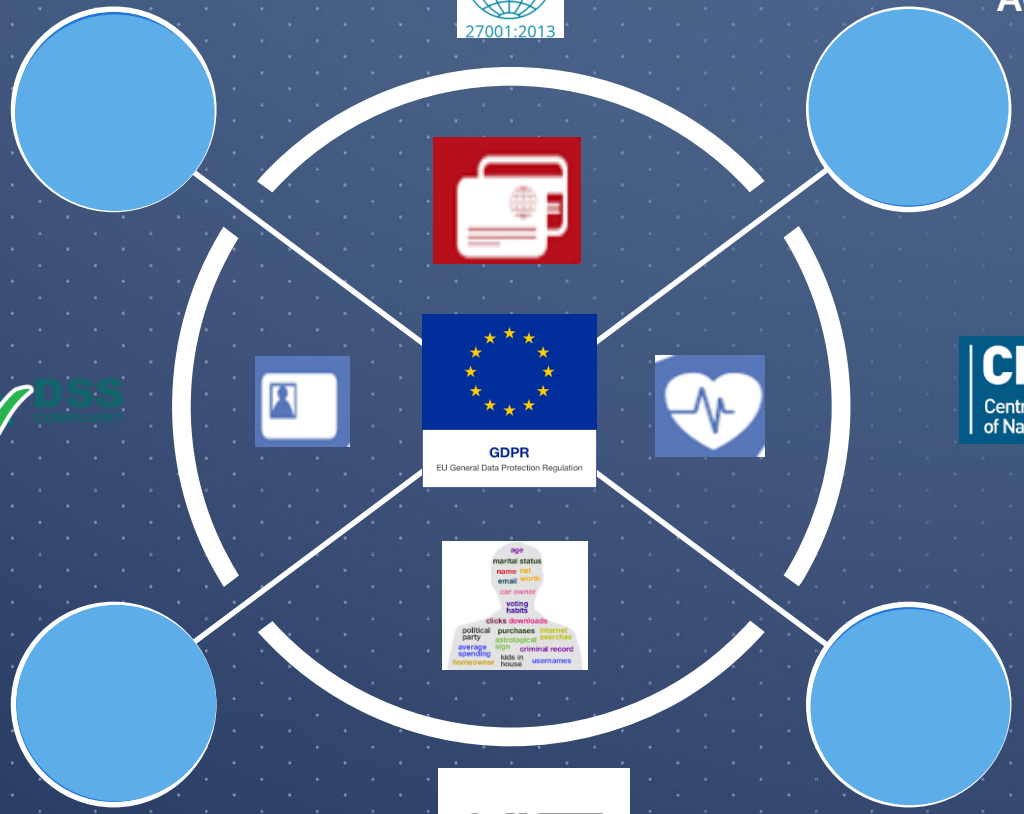
MINIMIZE GDPR RISK: FOCUS ON QUICK WINS

GDPR CONCENTRATION AREAS

PURPOSE

UNDERSTAND YOUR DATA

MONITOR AND CONTROL DATA ACCESS



ASSESS DATA SECURITY CONTROLS

IMPLEMENT DATA PROTECTION IMPACT ASSESSMENTS

Data Process Clarity

Continuous Assessment and audit of data and systems

Detection, reporting, and investigation of a personal or corporate data incident

Enact Privacy Impact Assessments guided against policy

- *The state of The industry (The Threatscape)*
- *Statistics and Observations*
- *Apply Security Control measurement to obtain cyber clarity.*
- *Frameworks and Scorecards that can help reduce threats while bosting data and security accountability*

Carbon Black.

Thanks!

www.CarbonBlack.com