Governance and Assurance for Emerging Technologies

Steven Myers (AIA CISO)

Agenda

- Threat Landscape & Threat Defence
- Threat Visibility
- New Technology and Cyber Assurance
- Cyber Detection & Response
- Governance
- Q&A

A Myriad of Different New Technologies

Design
Assessment

Threat Visibility

Assurance
Methodology

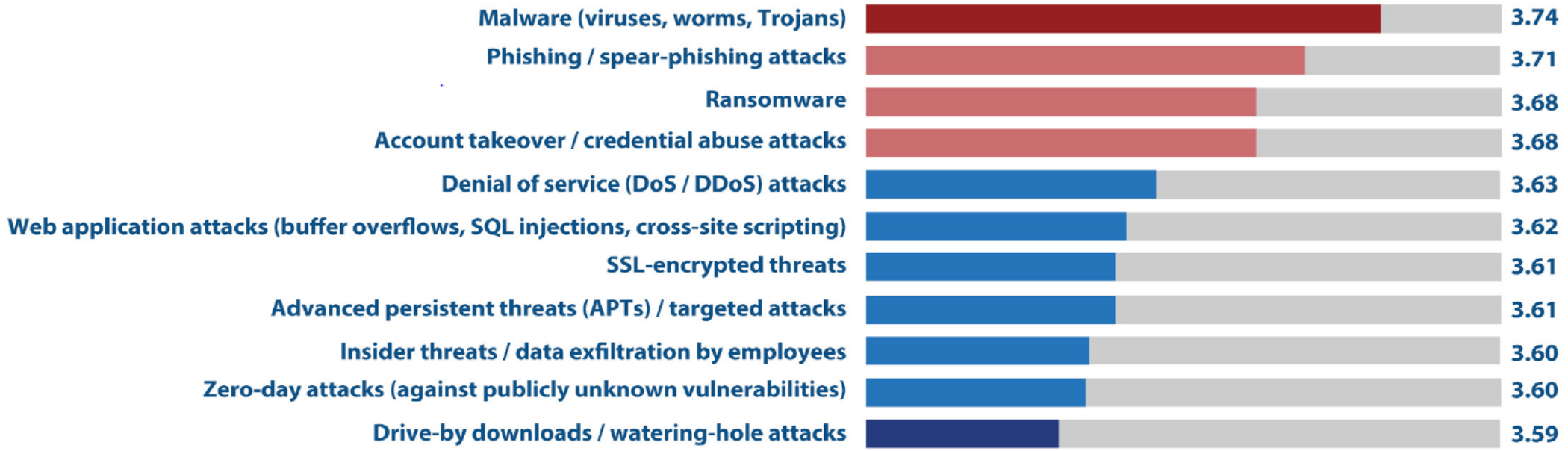
Oversight

Cyber Response

Cyber Threat Landscape

Concern for Cyberthreats

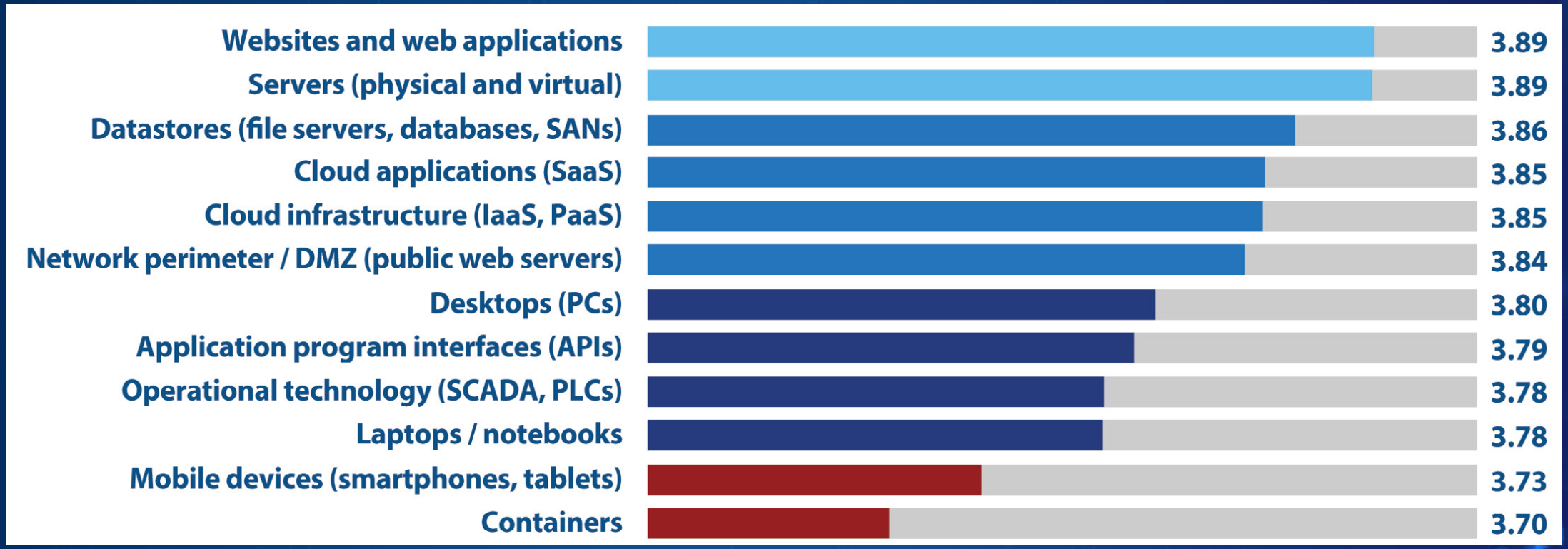
On a scale of 1 to 5, with 5 being highest, rate your overall concern for each of the following types of cyberthreats targeting your organization. (n=1,193)



2019 Cyberthreat Defense Report (cyber-edge.com)

Cyber Threat Defence

On a scale of 1 to 5, with 5 being highest, rate your organization's overall security posture (ability to defend against cyberthreats) in each of the following IT components: (n=1,191)



2019 Cyberthreat Defense Report (cyber-edge.com)

Threat Visibility

- How do you know what the threats are?
- Threat Intelligence - TIP
- What Intel feeds do you process?
- What quality of data are you consuming?
- Do you follow a standard framework?

MITRE ATT&ACK https://attack.mitre.org

Cyber Security & Assurance – Key Methodologies

Digital Web Apps

BlockChain

IOT

Cloud SAAS

STRIDE threat modelling

Security Design reviews

Security Certifications - Cloud Security Alliance (STAR)

Vulnerability Assessments – Static, Dynamic

Pen Testing – CREST, Bug Bounty

Red Team – CBEST

Managed Threat Hunting

General Considerations

- People

Do we have the right skills to assess the threats & risks correctly?

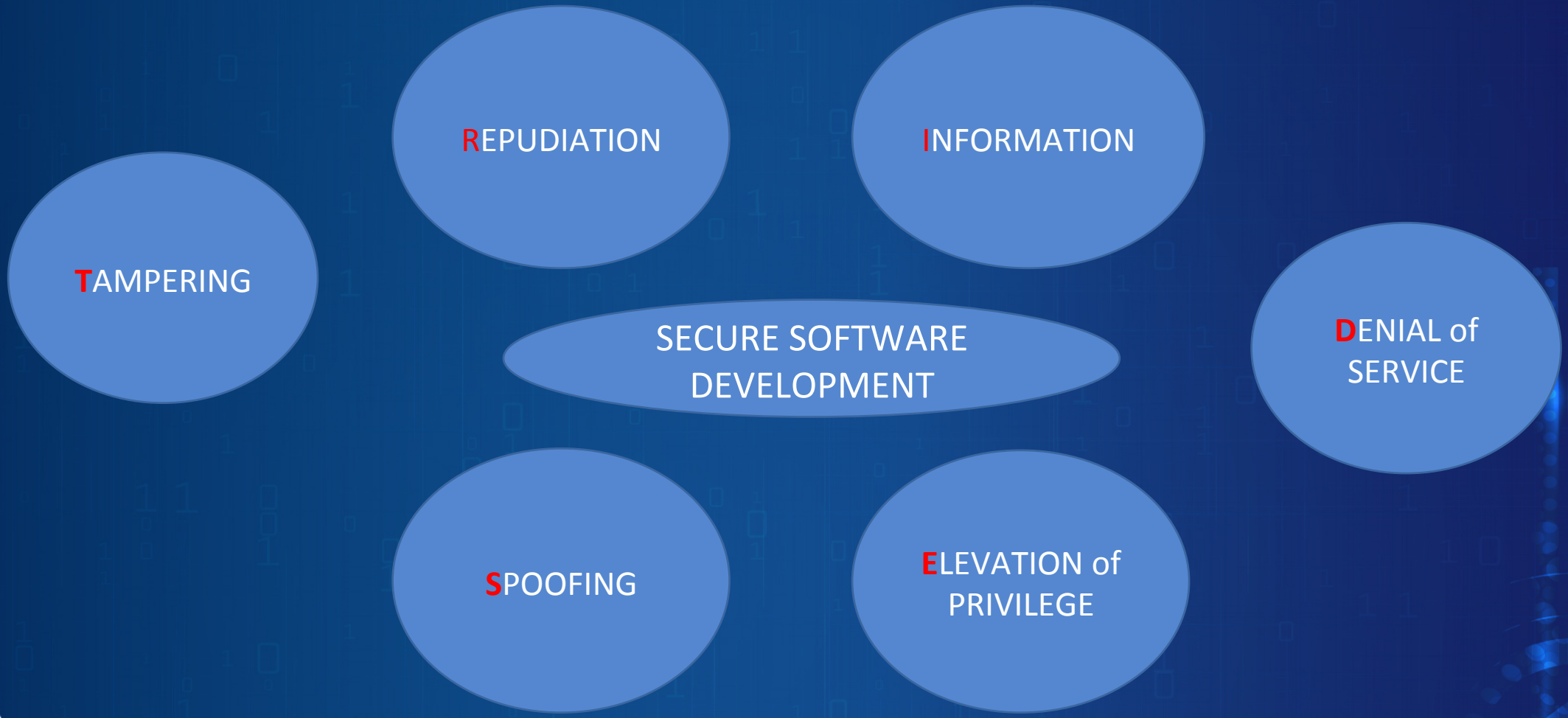
- Process

Are we following the best industry assessment standards?

- Technology

Does the new technology integrate into the ‘Security Ecosystem’

Example - Digital Web App Attacks ? STRIDE



Example: Cloud Security Assurance

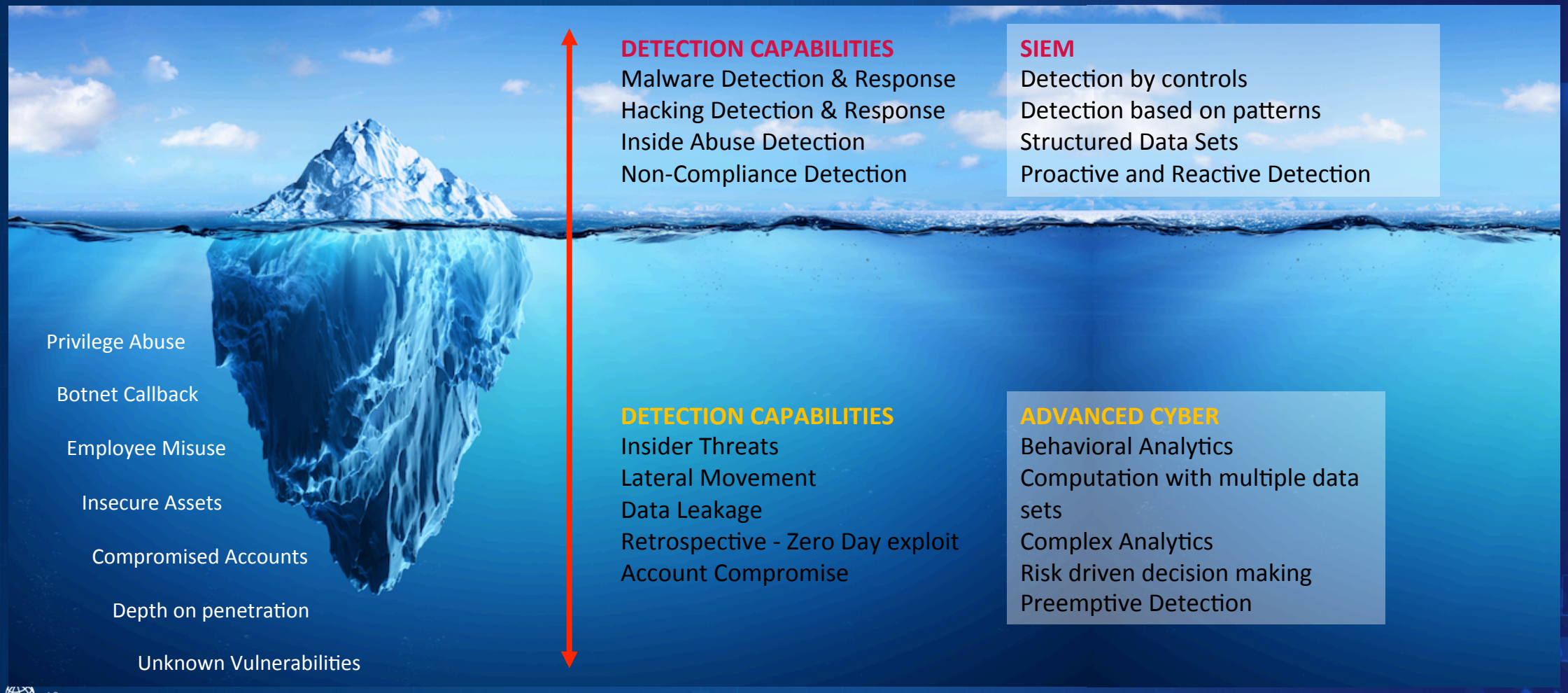
What are some of the key new risks?

- Container images and serverless functions may contain hidden Vulnerabilities
- Containers with Embedded Secrets
- Configuration and Access issues e.g. Open APIs
- Malware

How can I manage those risks?

- Visibility – Container Inspection, Scanning, Lifetime – Refresh and Rebuild
- Orchestration – Automate security controls real-time upon deployment
- Cloud Access Security – CASB
- Cloud Posture Management

Cyber Detection



DETECTION CAPABILITIES
Malware Detection & Response
Hacking Detection & Response
Inside Abuse Detection
Non-Compliance Detection

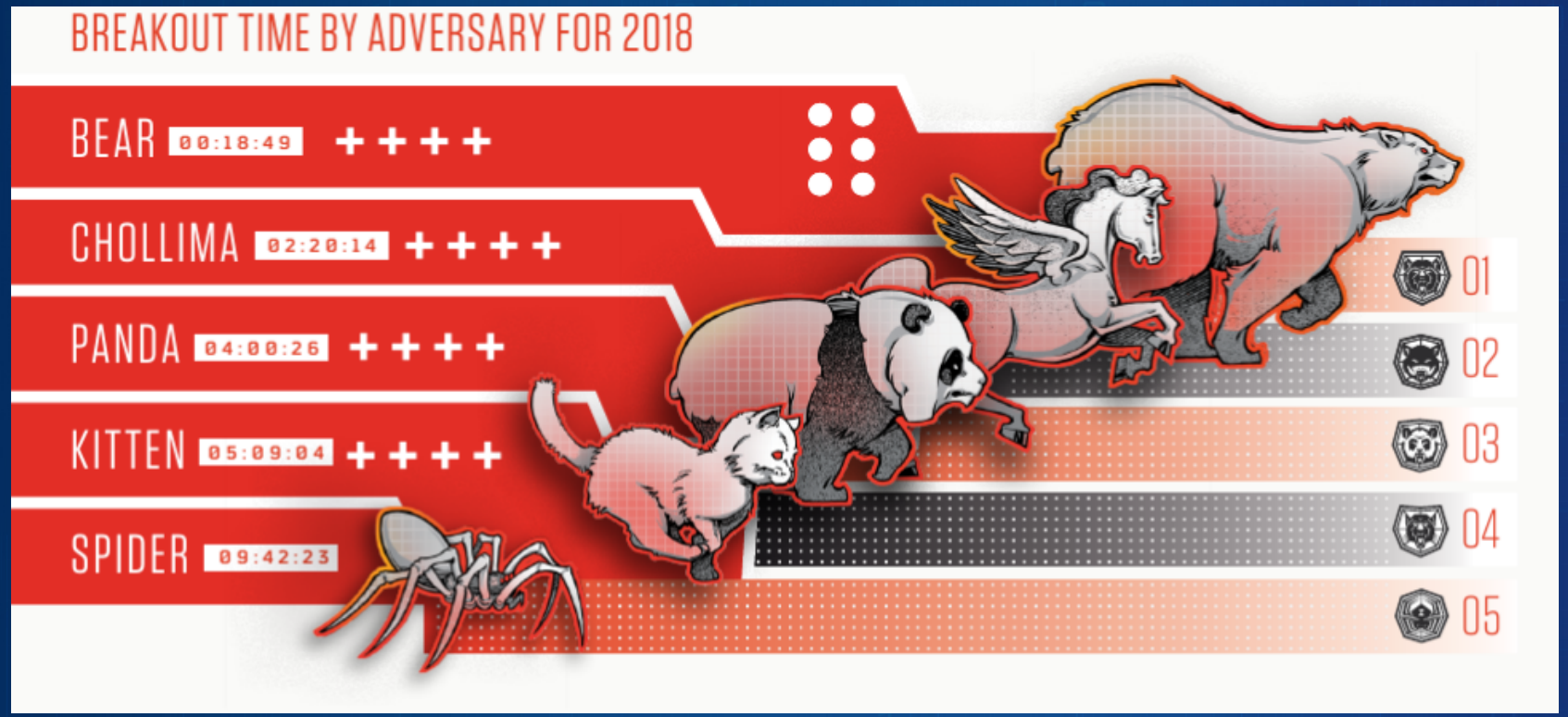
SIEM
Detection by controls
Detection based on patterns
Structured Data Sets
Proactive and Reactive Detection

DETECTION CAPABILITIES
Insider Threats
Lateral Movement
Data Leakage
Retrospective - Zero Day exploit
Account Compromise

ADVANCED CYBER
Behavioral Analytics
Computation with multiple data sets
Complex Analytics
Risk driven decision making
Preemptive Detection

Cyber Response

Why do we need to build automated response?



The *2019 CrowdStrike® Global Threat Report*

Governance

- Define standards for emerging technologies
- Integrate KRIs
- Use Automated dashboards
- Continuous Anomaly Detection

Cyber Hygien

- Keep systems up to date
- Use Strong Authentication
- Encrypt your sensitive data
- Advanced Security Monitoring
- Automated Response

Thank You ☺

Questions?