*Reassuringly dull cyber security

The key for 2023:
Cybersecurity trends and the necessary defensive blends

Chris Roberts – Fortinet BDM, Security Operations
Paul Cragg – norm. CTO

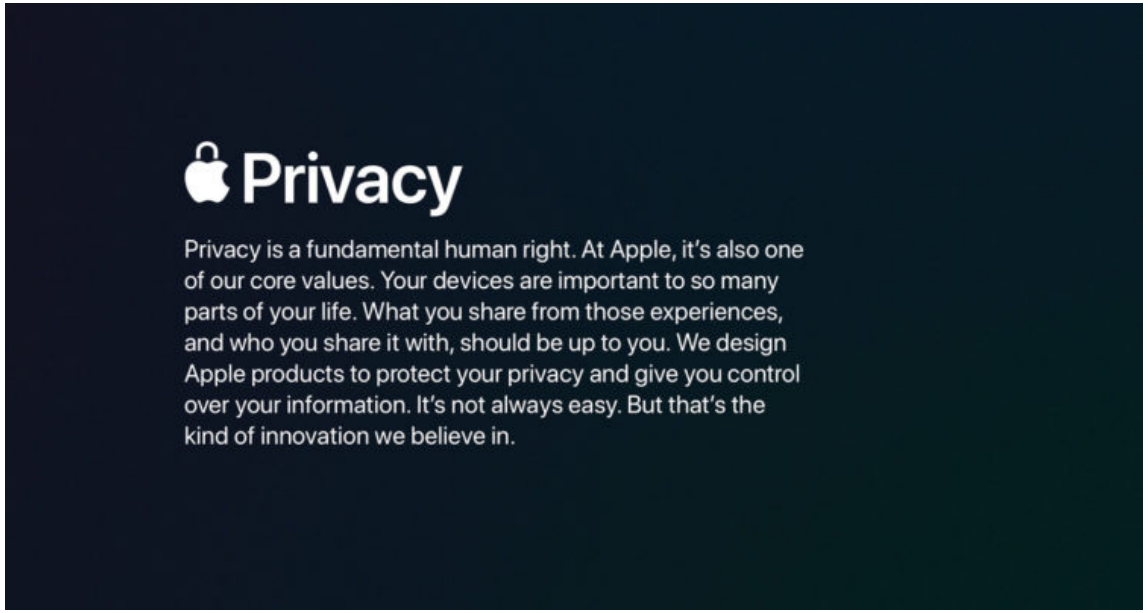
Six Cybersecurity Trends you can expect in 2023…

- **A ‘Privacy-First’ Approach to Information Security**
  - Growing amount of privacy legislation, globally
  - Multiple countries adopting stricter data privacy regulations
  - Effort towards harmonisation of Information, Privacy and Data Regulations
- **More organisations will outsource Cybersecurity Operations**
  - Increasing complexity
  - Skills shortage
  - Constantly evolving treat landscape
- **Ransomware**
  - Shift to ‘simple extortion’
  - Cybercrime as a Service – accelerate the volume and effectiveness of cyberattacks
- **Enterprise misinformation attacks – social engineering**
  - Deepfakes
- **Zero Trust**
  - Evolving remote working trends
  - Never trust, always verify
- **Cyber Insurance**
  - Rocketing insurance premiums
  - Reduced coverage
  - Becoming more difficult to obtain / afford

Only the resilient survive…

A Privacy First Approach…

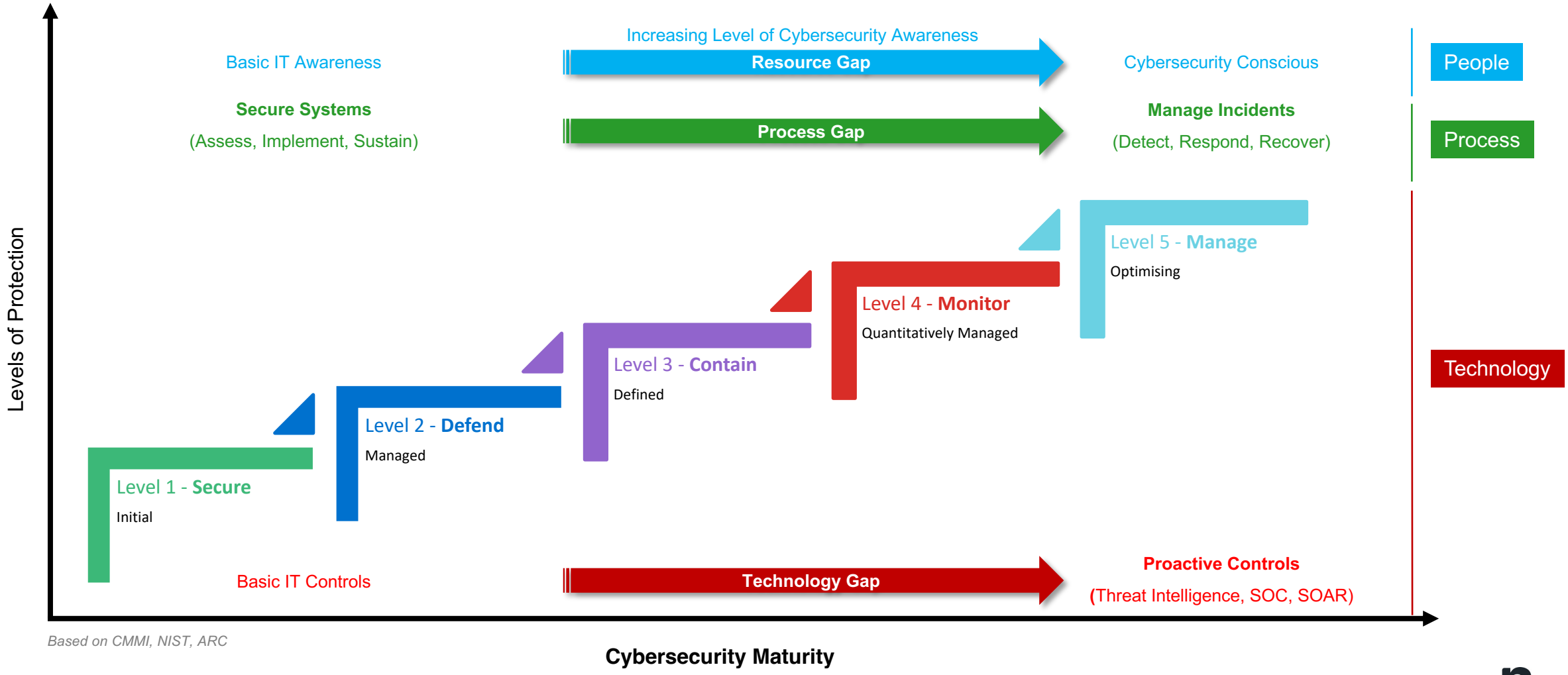
- **Privacy begins at home**
  - Where is your data ?
  - Employee data
- **Earning your Customers' Trust**
  - Far from just a regulatory obligation
  - Customer Relationship
- **Securing Executive Support**
  - Focus on both the qualitative and quantitative benefits
  - Competitive advantage
- **Adoption of internationally recognised frameworks**
  - ISO27001 (Information Security Management)
  - ISO27701 (Privacy Information Management)
- **Prepare for tomorrow's regulatory environment**
  - Rapidly changing dynamic environment
  - Work with our Privacy experts to help build a robust 'Privacy First' strategy



Outsourcing Cybersecurity Operations…

- **24 / 7 year-round coverage**
  - The bad guys don't sleep…
  - Respond to threats as and when they happen
- **Quicker path to Cybersecurity Maturity**
  - A well-defined route to success
- **Cost effective**
  - Predicable opex costs
  - A fraction of the costs of an in-house solution
- **Broader experience**
  - Aggregate knowledge across diverse customers and verticals
  - Threat Intelligence led
  - Breadth and depth of technical and subject domain knowledge
- **Advanced Technology**
  - Quicker adoption of emerging technologies
  - Fully integrated into service proposition
  - SOAR built-in
  - Outcome focused
- **Focus**
  - Allows the business to focus on its core business

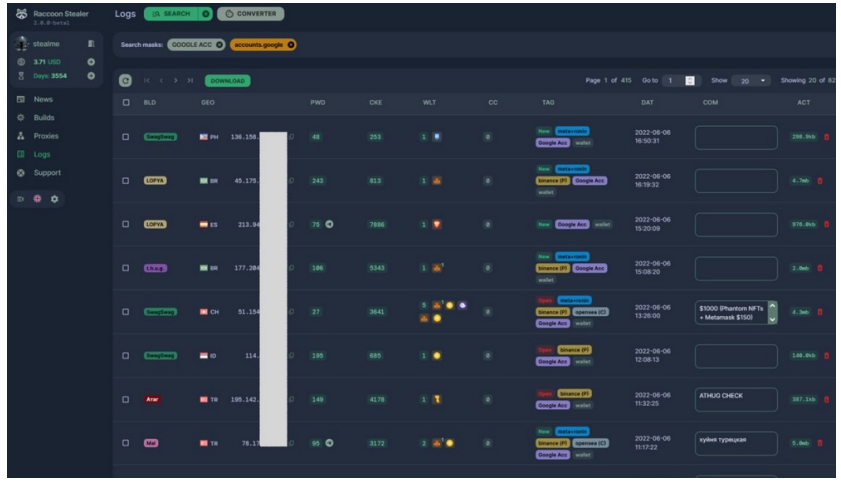
Cybersecurity Maturity Levels



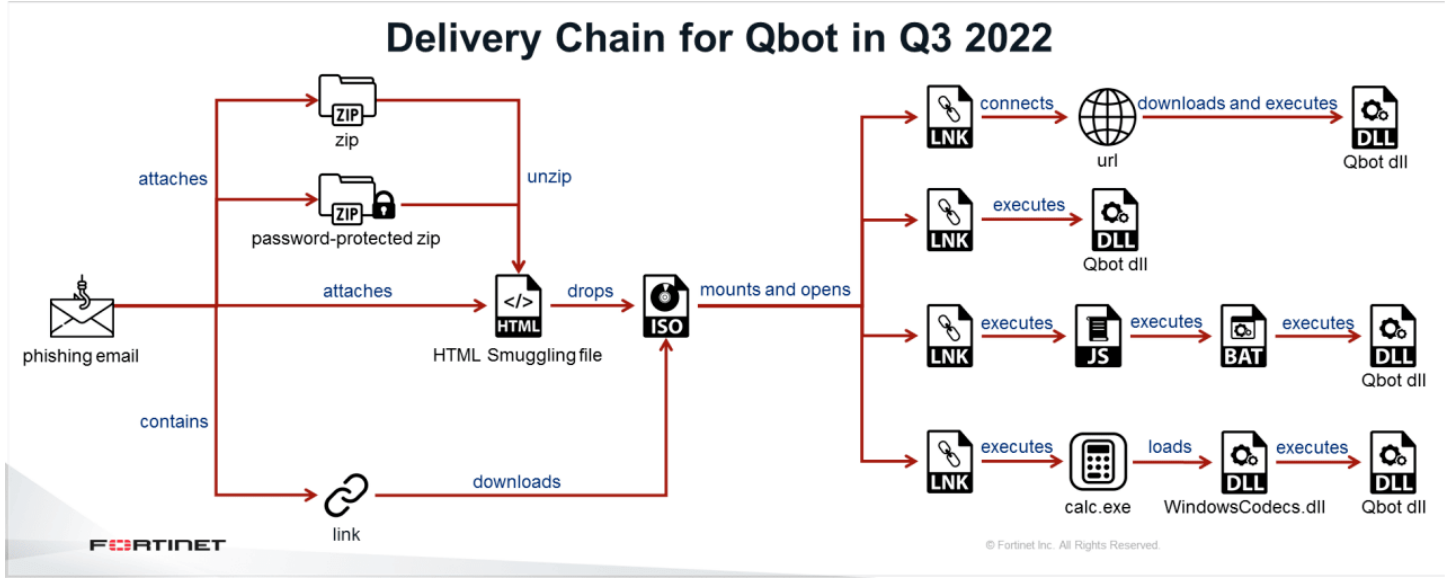
Based on CMMI, NIST, ARC

State of the Nation

- **Netgear VPN Routers**
  - 'Multiple security vulnerabilities in its business grade….can't be fixed….replacement router'
- **Realtek SOC Vulnerabilities**
  - Zero touch exploit – millions of devices
  - Execute code, intercept traffic
  - ASUSTek, Belkin, Buffalo, D-Link, Edimax, TRENDnet, Zyxel, etc
- **DDoS botnet 'Enemybot'**
  - Uses TOR for C2C
  - Targets routers, IoT and IT devices
- **Lightning Stealer**
  - Targets 30 browsers
  - Steals bookmarks, browser history, cookies, crypto wallets, Telegram data, Discord tokens, and Steam user's data
- **Nokoyawa Ransomware**
  - Unique encryption keys
  - Contact through TOR browser



Racoon Stealer dashboard



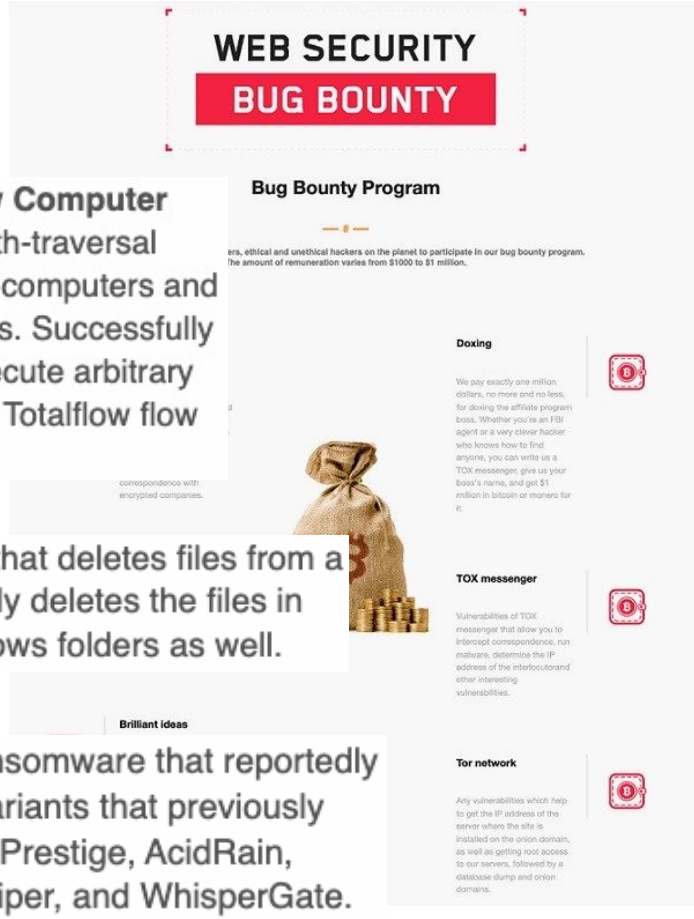
Ransomware Evolves

Ransomware Gangs are Increasingly Confident

- **LockBit**
  - In wild since 2019
  - Targets Windows and Linux
  - Version 3.0 debuted in March 2022
  - RaaS model
  - Support services – negotiation, etc
  - 20% fee for use of RaaS platform
  - Critical Infrastructure off limits for encryption only
  - Former Soviet countries also off limits
  - Bug Bounty ($1k - $1m)

- **RedAlert**
  - Targets Windows and ESXi
  - Multiple threats including DDoS and employee calls

- **Dark Web Hacker**
  - $3k ransom demand
  - Desktop wallpaper with QR code
  - Deletes shadow copies



Path Traversal Vulnerability (CVE-2022-0902) in ABB Flow Computer and Remote Controllers – FortiGuard Labs is aware of a path-traversal vulnerability (CVE-2022-0902) that affects ABB Totalflow flow computers and remote controllers widely used by oil and gas utility companies. Successfully exploiting the vulnerability allows an attacker to inject and execute arbitrary code. The vulnerability is a path-traversal vulnerability in ABB Totalflow flow computers and remote controllers.

The Wise Guys ransomware is a destructive malware that deletes files from a victim's machine. Once the ransomware runs, it not only deletes the files in specific special folders, it then tries to delete the Windows folders as well.

This is significant because Somnia is the latest ransomware that reportedly targeted Ukrainian interests. Other ransomware variants that previously targeted Ukraine include, but are not restricted to, Prestige, AcidRain, DoubleZero, CaddyWiper, IssacWiper, HermeticWiper, and WhisperGate.

Outbreak Alert: Hive Ransomware - The Hive ransomware gang has received up to $100M+ in ransom payments from over 1,300 victims, according to a joint advisory released by the FBI, the U.S. Cybersecurity and Infrastructure Security Agency, and the Department of Health and Human Services.

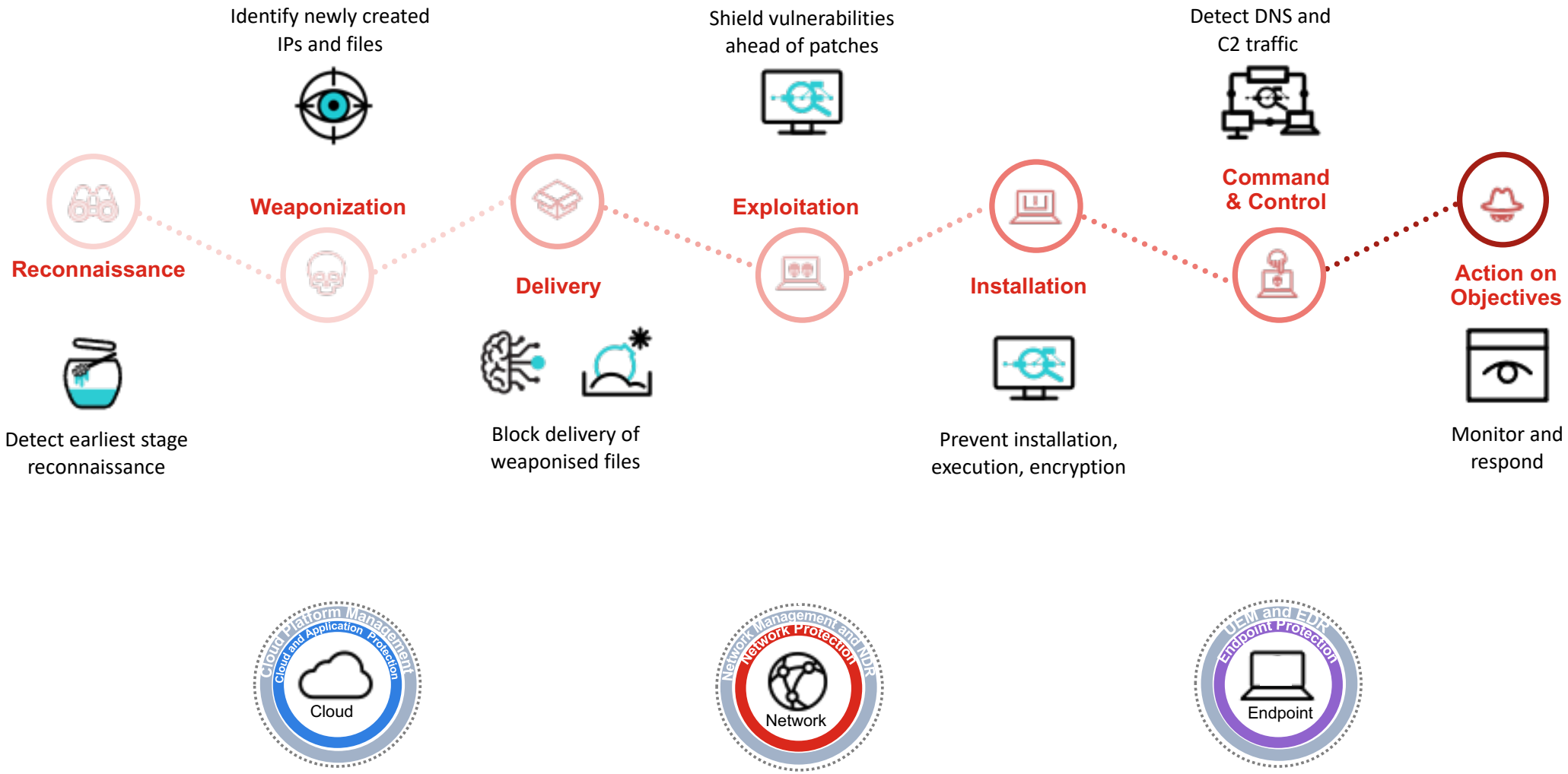
FortiGuard Labs

- **Summary**
  - 10,666 in 1H 2022 vs 5,400 in 2H 2021
  - $600m ransoms paid in H1 2021
  - More than the combined previous decade
  - 49% of respondents have pay policy in place
  - Ukraine based wiper malware – 25 countries
  - Numbers rising due to RaaS –bad coding/wipers
- **2023 and Beyond**
  - More wiper based malware, worms & subscriptions
  - More CaaS options – quicker paydays
  - Satellite attacks – turbines, shipping, airlines, etc
  - Deepfake use on the rise
  - Reconnaissance as a Service
  - ML for money mule recruitment & MLaaS
  - Quantum computing to discover zero days

https://www.fortinet.com/demand/gated/wp-threat-prediction-2023

Understanding the Journey

Across the attack surface and along the cyber kill chain



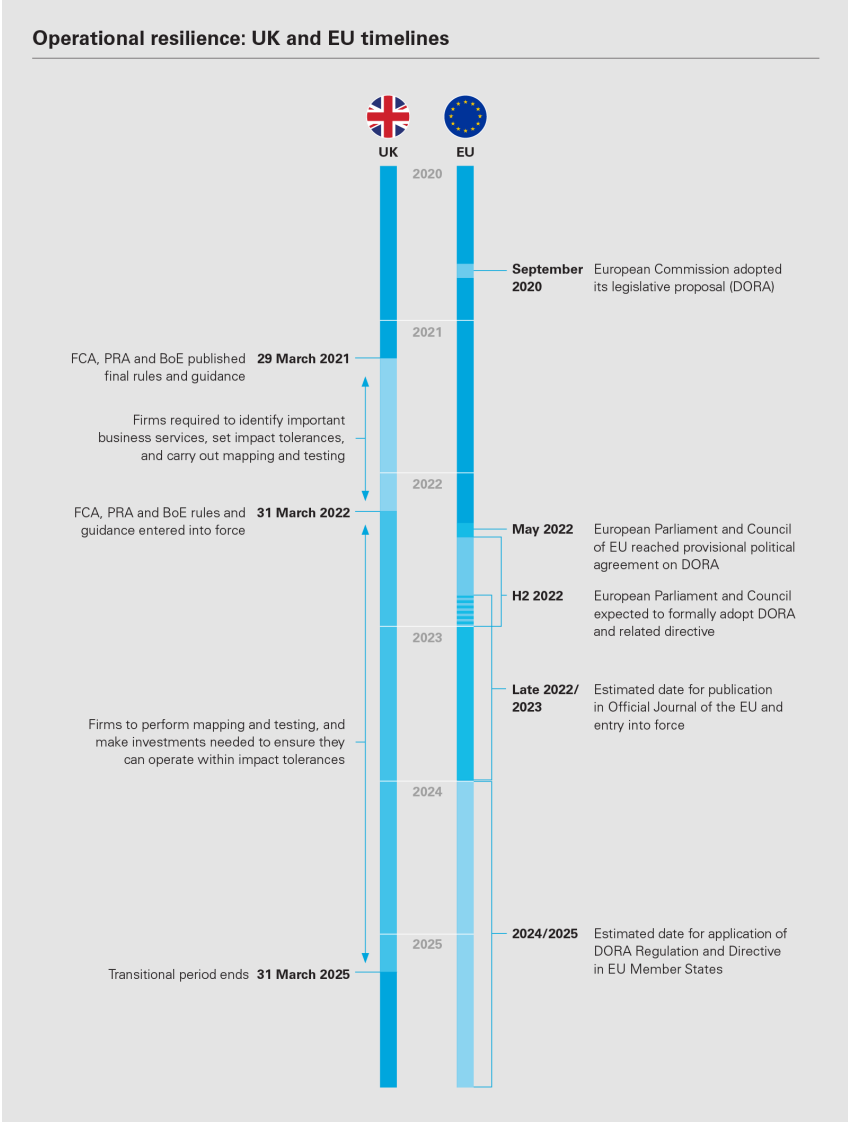
Digital Operations Resilience Act Thoughts

an assessment of basic requirements (e.g. vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where

financial entities should regularly test their ICT systems and staff with regard to t effectiveness of their preventive, detection, response and recovery capabilities,

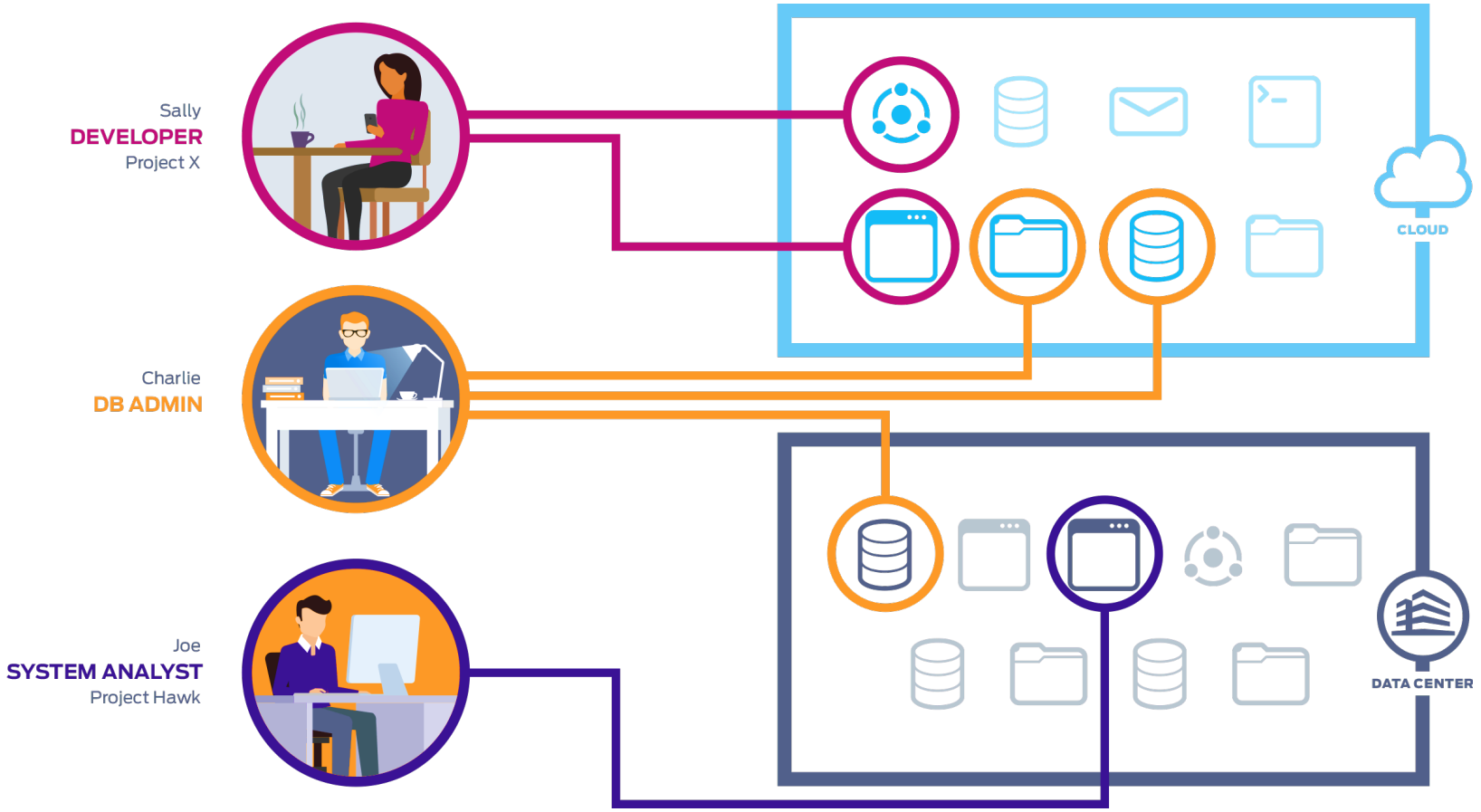
periodically tested for preparedness and identification of weaknesses, deficiencies or gaps, well as the prompt implementation of corrective measures. This regulation allows for

Finally, in terms of environmental impacts, the policy option chosen would encourage an enhanced use of the latest generation of ICT infrastructures and services, which are expected to become environmentally more sustainable.



Zero Trust Network Architecture…

- Users in or out of the Office
- Automatic Secure connection to applications
- Application located anywhere
- SSO Supported
- MFA provided when necessary



Cybersecurity Insurance…

- **Premium costs are increasing**
  - Trend expected to continue for the next two years
  - Loss ratios range from 67% - greater than 100%
- **Premium cover is contracting**
  - Level of cover available (£)
  - Exclusion list growing
- **Securing cover is challenging**
  - Fragmented approach to quantifying risk across the industry
  - Inconsistent / ever-changing question sets
  - Mandating the implementation of certain technical controls
- **Affordability / Value**
  - Customers are questioning the value of cybersecurity insurance
  - Growth in ‘Self Insure’ trend
- **Predicted to grow from £9.9 Billion in 2022 to £24.3 Billion by 2027**
- **Clearly demonstrate you’re a safe bet for cyber insurers**
  - Provide regular employee awareness training on phishing and social engineering
  - Constant management of your attack surface
  - Proactive and preventative monitoring in place, 24x7

Behavioural Protection at the Client…

Detect, defuse, respond and remote remediation

Pre-infection/Pre-execution

Discover

Proactive Risk Mitigation

- Discover rogue devices and IoT
- Vulnerabilities
- Virtual patching

Prevent

Pre-execution Protection

- ML AV
- FortiGuard Threat Intelligence
- Sandbox Integration
- Desktop firewall
- Web filtering

Post-infection/Post-execution

Detect

File-less and Advanced Threats

- Behavioural based
- Detect memory-based attacks
- Threat classification

Defuse

Stop Breach and Ransomware

- Block malicious actions
- Prevent data loss
- Zero Dwell time

Respond & Investigate

Full attack visibility

- Playbook automation
- Cross platform response
- Forensic data
- Behavioral-based threat hunting
- Built-in MITRE tags

Remediate & Roll Back

Automated Dis-infection

- Clean up/roll back
- Eliminate re-image/ rebuild
- Minimize business disruption

Automation | Cloud • Hybrid • Air-gap Deployment | OS Coverage

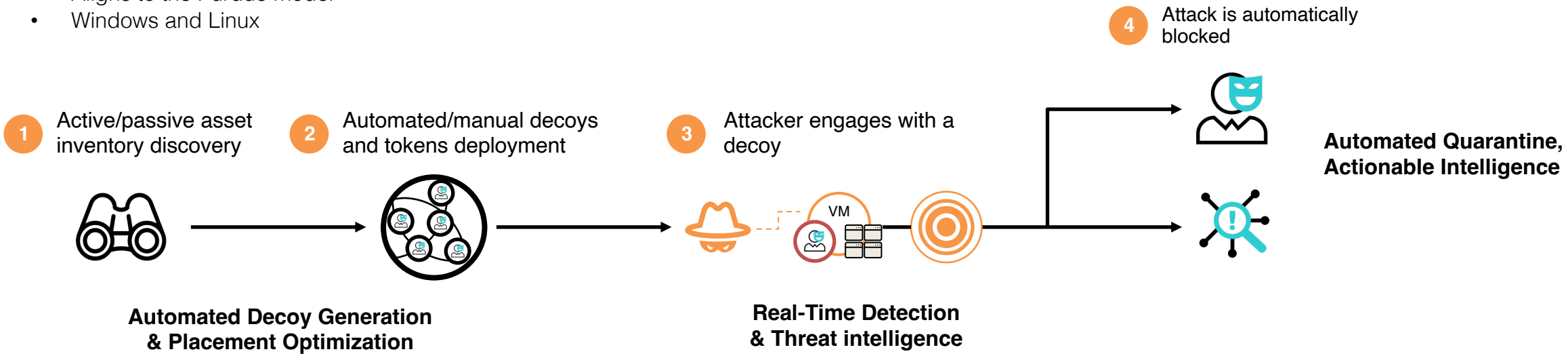
Deception

- **Why Deception**
  - Deceive – External and Internal threats with deceptive decoys
  - Expose – hacker activity with early and accurate detection
  - Eliminate – threats by automating responses
  - Reduces dwell time

- **Protects both OT and IT environments**
  - SCADA/ICS profiles
  - Aligns to the Purdue model
  - Windows and Linux

- **Unintrusive and Simple**
  - AI-based recommended deployment
  - No operational delay
  - No need to take IT/OT systems offline

- **Early detection and response**
  - High fidelity alerting – early and unambiguous detection of a threat actor touching a decoy
  - Drive automated response



Comprehensive detection, closing visibility gaps, diverts attackers from sensitive assets to shift the balance to defender's advantage

Deception – The Art of the Possible…

Windows Decoy

- Windows 7
- Windows 10
- Windows Server 2016
- Windows Server 2019

Windows Lure/ Tokens

- SMB
- RDP
- TCP Port Listener
- SQL (server)
- Cache Credentials
- Fake Network Connection
- HoneyDocs (Office & PDF)
- SQL ODBC
- SAP Connector
- FTP

VPN Decoy

- FortiOS

Lures Available

- SSLVPN

Linux Decoy

- Ubuntu 16.0.4
- CentOS

Linux Lure/ Tokens

- SSH
- SAMBA
- SMB
- RDP
- GIT
- FTP
- ESXi
- ELK

IoT Decoys

- Cisco Router
- IP Camera
- Printers (HP, Lexmark, Brother)
- UPS

Cloud Decoys

- AWS
- AZURE
- GCP

Application Decoys

- SAP
- ERP
- POS
- Medical

SCADA Decoy & Lures

- HTTP
- FTP
- TFTP
- MODBUS
- S7COMM
- BACNET
- IPMI
- TRIXONEX
- GUARDIAN-AST
- IEC 60870-5-104
- EtherNet/IP (Rockwell)
- DNP3
- Triconex (Schneider Electric)

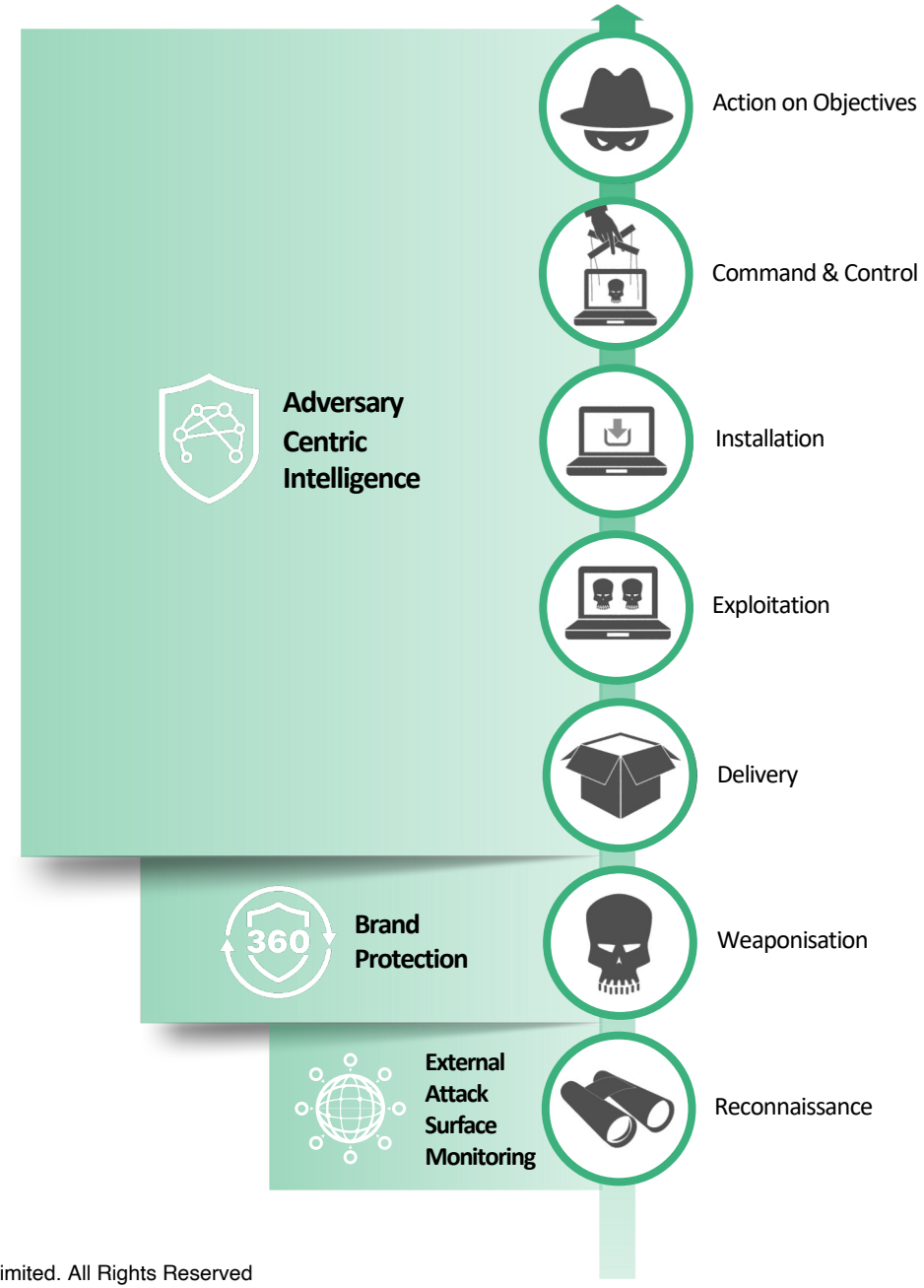
Reconnaissance…

FortiRecon provides visibility, intelligence allowing the customer to take controlled risk-based security actions:

- Compliments existing solutions to complete visibility of the attack surface.
- Provides customers a view on what adversaries are seeing (EASM)
- Provides customer a view on what adversaries are doing (Brand Protection)*
- Provides customer a view on what adversaries are planning (ACI)*

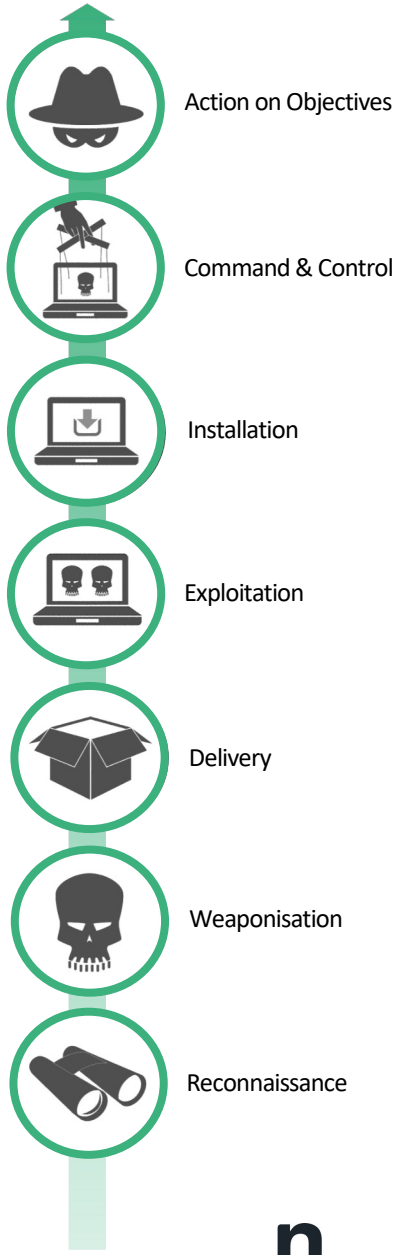
Take mitigating / remediating actions earlier reducing the impact and cost of cyber attack

- Protect the organisations brand reputation



In Summary…

- Threat actors continue to evolve
- Deception is a viable mechanism
- Behavioural protection is now critical
- Automation drives efficiencies
- Integration & visibility is a must
- Contextual intelligence is a must
- Security awareness is a high priority
- External understanding can drive better posture
- MTTD & MTTR must be driven down



Thank you.