FORTINET

CyberSecurity Governance – Updates from the Front Line
Risk, Visibility, Time to Detect and Remediate Impact

Chris Roberts – Business Development Manager, Security Operations

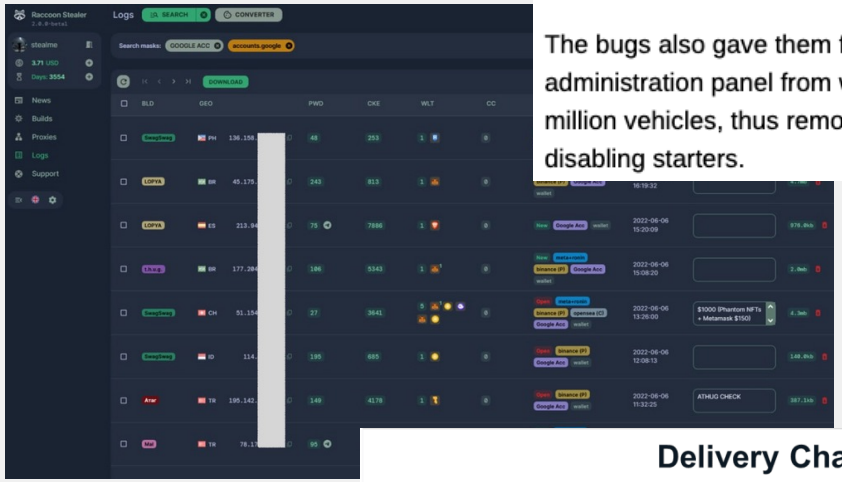
State of the Nation

- ***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

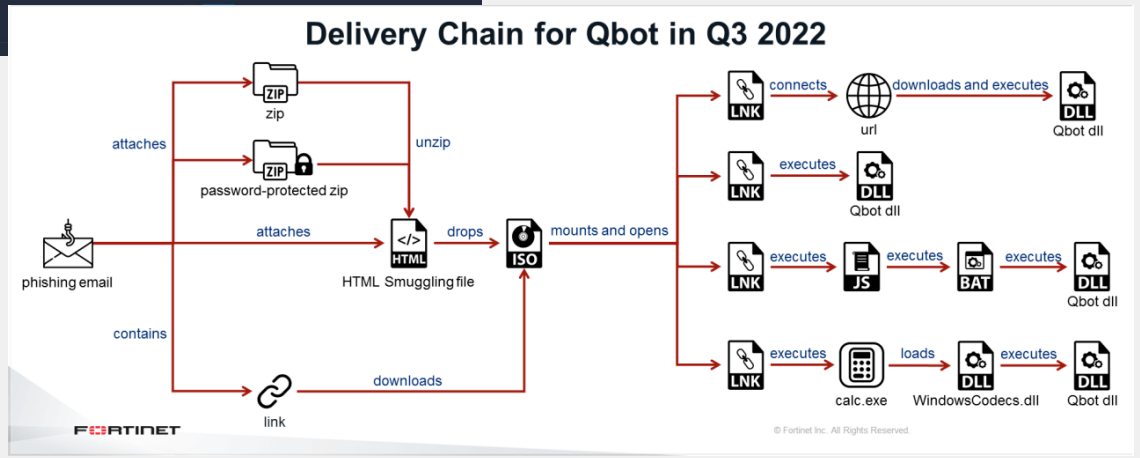
The most serious bugs, at least from a public safety perspective, were found in Spireon, which owns several GPS vehicle tracking and fleet management brands including OnStar, GoldStar, LoJack, FleetLocate, and NSpire spanning 15 million connected vehicles.

"This would've allowed us to track and shut off starters for police, ambulances, and law enforcement vehicles for a number of different large cities and dispatch commands to those vehicles," the researchers wrote.

The bugs also gave them full administrator access to Spireon and a company-wide administration panel from which an attacker could send arbitrary commands to all 15 million vehicles, thus remotely unlocking doors, honking horns, starting engines and disabling starters.



Racoon Stealer dashboard

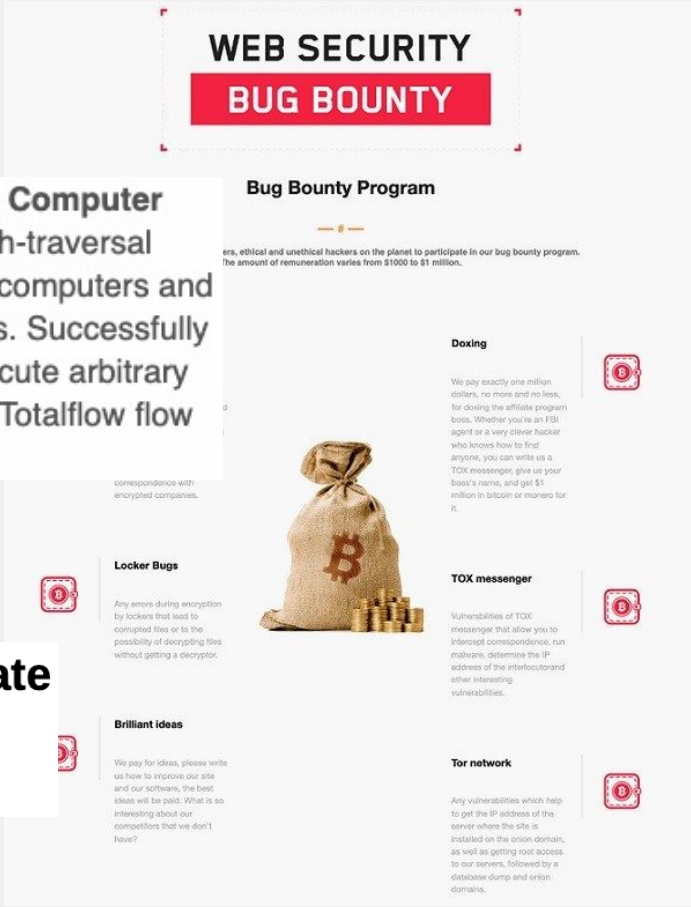


Ransomware Evolves

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.



Cybercrooks are telling ChatGPT to create malicious code

Chatbot might let unskilled criminals launch attacks, if the code works

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.

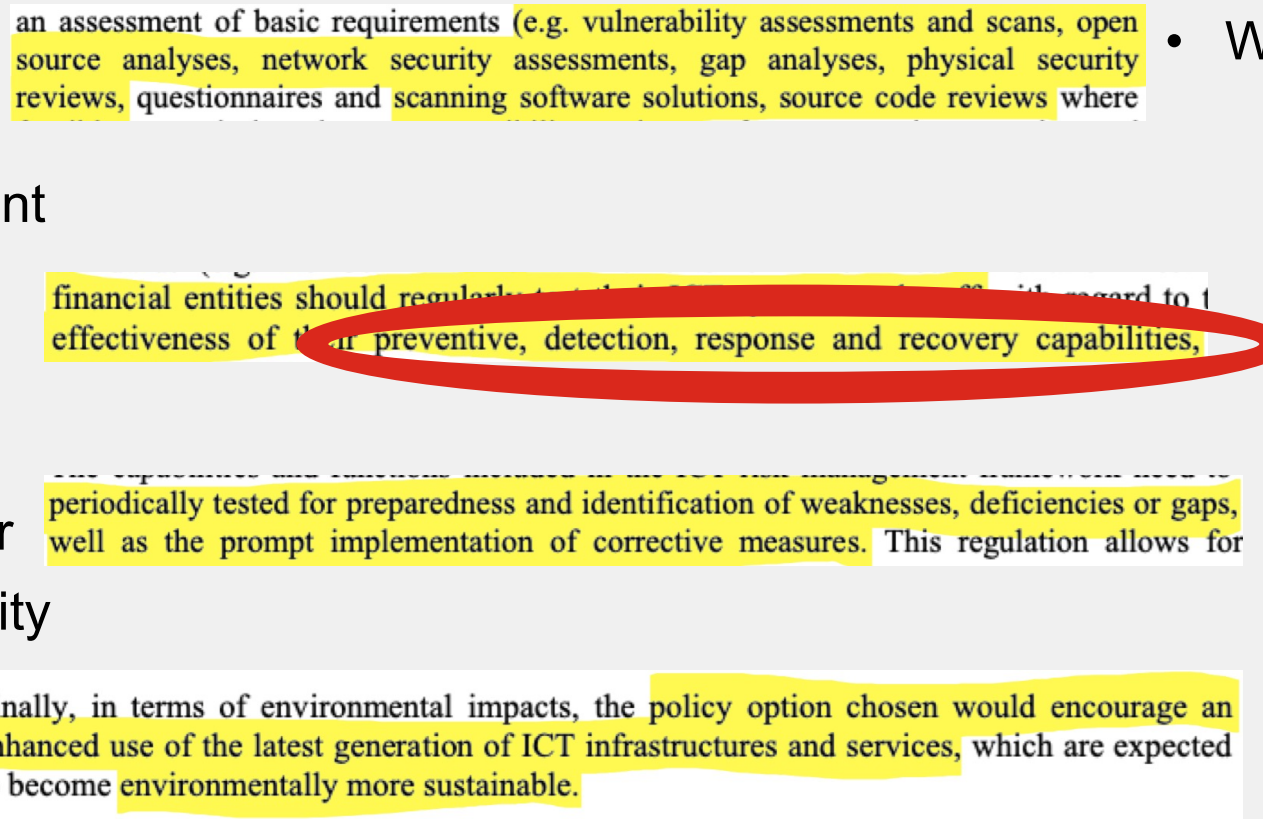
FortiGuard Labs

- Summary
  - 10666 in 1H 2022 vs 5400 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

Digital Operational Resilience Act Thoughts

- Driving
  - Automation
  - Secure Development
  - System Monitoring
  - Deception
  - Detonation
  - Endpoint Behaviour
  - Multi Vendor Visibility



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

effectiveness of

preventive, detection, response and recovery capabilities,

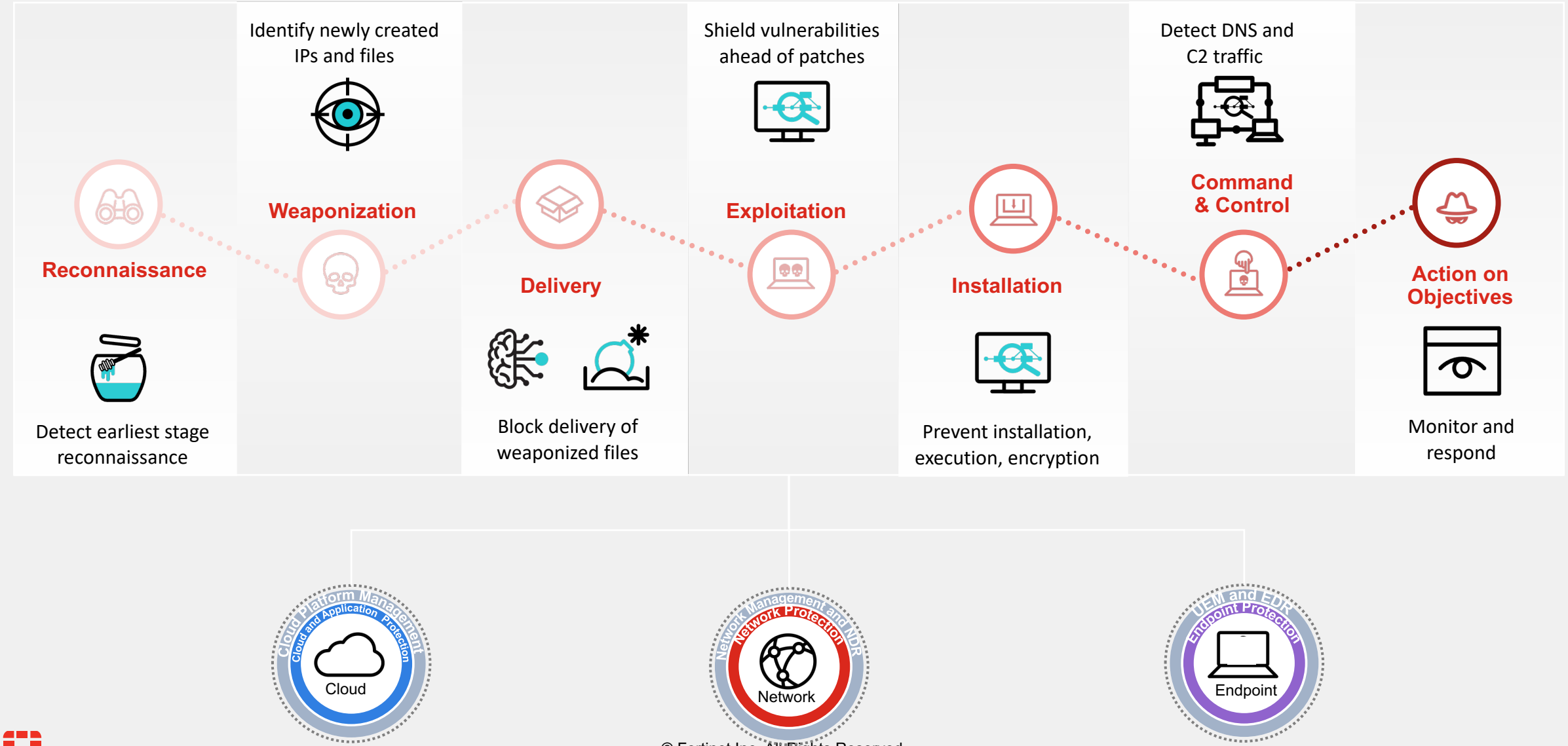
periodically tested for preparedness and identification of weaknesses, deficiencies or gaps, well as the prompt implementation of corrective measures. This regulation allows for

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.

- Why?
  - RBAC
  - Multi-tenancy
  - Deployment options
  - Commercial flex
  - Technical debt
  - Integration
  - Auditability
  - Automation
  - Simplicity
  - Asset Visibility

Understanding the Journey

Across the attack surface and along the cyber kill chain



Fortinet Security Fabric

The industry's highest-performing integrated cybersecurity mesh platform

Product Matrix

Click on icons in this document for additional information

Fortinet Brochure
Highlighting our broad, integrated, and automated solutions, quarterly

Free Training
Fortinet is committed to training over 1 million people by 2025

Free Assessment
Perform an assessment in your network to validate your existing controls

FortiOS
The Heart of the Fortinet Security Fabric

Secure Networking

FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiGate SD-WAN
Application-centric, scalable, and Secure SD-WAN with NGFW

FortiExtender
Extend scalable and resilient LTE and LAN connectivity

FortiAP
Protected LAN Edge deployments with wireless connectivity

FortiSwitch
Deliver security, performance, and manageable access to data

Linksys HomeWRK
Secure Work-from-Home solution for remote and hybrid workers

FortiNAC
Visibility, access control and automated responses for all networked devices

FortiProxy
Enforce internet, compliance and granular application control

FortiIsolator
Maintain an "air-gap" between browser and web content

Cloud Security

FortiGate VM
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiDDOS
Machine-learning quickly inspects traffic at layers 3, 4, and 7

FortiCNP
Manage risk and compliance through multi-cloud infrastructures

FortiDevSec
Continuous application security testing in CI/CD pipelines

FortiWeb
Prevent web application attacks against critical web assets

FortiADC
Application-aware intelligence for distribution of application traffic

FortiGSLB Cloud
Ensure business continuity during Unexpected network downtime

FortiMail
Secure mail getaway to protect against SPAM and virus attacks

FortiCASB
Prevent misconfigurations of SaaS applications and meet compliance

Zero Trust Access

FortiSASE
Enforce dynamic network access control and network segmentation

ZTNA Agent
Remote access, application access, and risk reduction

FortiAuthenticator
Identify users wherever they are and enforce strong authentication

FortiToken
One-time password application with push notification

FortiClient Fabric Agent
IPSec and SSL VPN tunnel, endpoint telemetry and more

FortiConnect
Simplified guest access, BYOD, and policy management

FortiGuard Threat Intelligence

Powered by FortiGuard Labs

Fabric Management Center: NOC

FortiManager
Centralized management of your Fortinet security infrastructure

FortiGate Cloud
Saas w/ zero touch deployment, configuration, and management

FortiMonitor
Analysis tool to provide NOC and SOC monitoring capabilities

FortiAIOps
Network inspection to rapidly analyze, enable, and correlate

FortiExtender Cloud
Deploy, manage and customize LTE internet access

FNDN
Exclusive developer community for access to advanced tools & scripts

Open Ecosystem

The industry's most extensive ecosystem of integrated solutions

Fabric Connectors
Fortinet-developed

DevOp Tools & Script
Fortinet & community-driven

Fabric API Integration
Partner-led

Extended Ecosystem
Threat sharing w/ tech vendors

Fabric Management Center: SOC

FortiDeceptor
Discover active attackers inside with decoy assets

FortiNDR
Accelerate mitigation of evolving threats and threat investigation

FortiEDR
Automated protection and orchestrated incident response

FortiSandbox / FortiAI
Secure virtual runtime environment to expose unknown threats

FortiAnalyzer
Correlation, reporting, and log management in Security Fabric

FortiSIEM
Integrated security, performance, and availability monitoring

FortiSOAR
Automated security operations, analytics, and response

FortiTester
Network performance testing and breach attack simulation (BAS)

SOC-as-a-Service
Continuous awareness and control of events, alerts, and threats

Incident Response Service
Digital forensic analysis, response, containment, and guidance

Support & Mitigation Services

FortiCare Essentials*
15% of hardware

FortiCare Premium*
20% of hardware

FortiCare Elite**
25% of hardware

FortiConverter
25% of hardware

* FortiCare Premium is formerly 24x7 Support. Lower support price for Switches and APs

** Response time for High Priority tickets. Available for FortiGate, FortiManager, FortiAnalyzer, FortiSwitch, and FortiAP

Communication and Surveillance

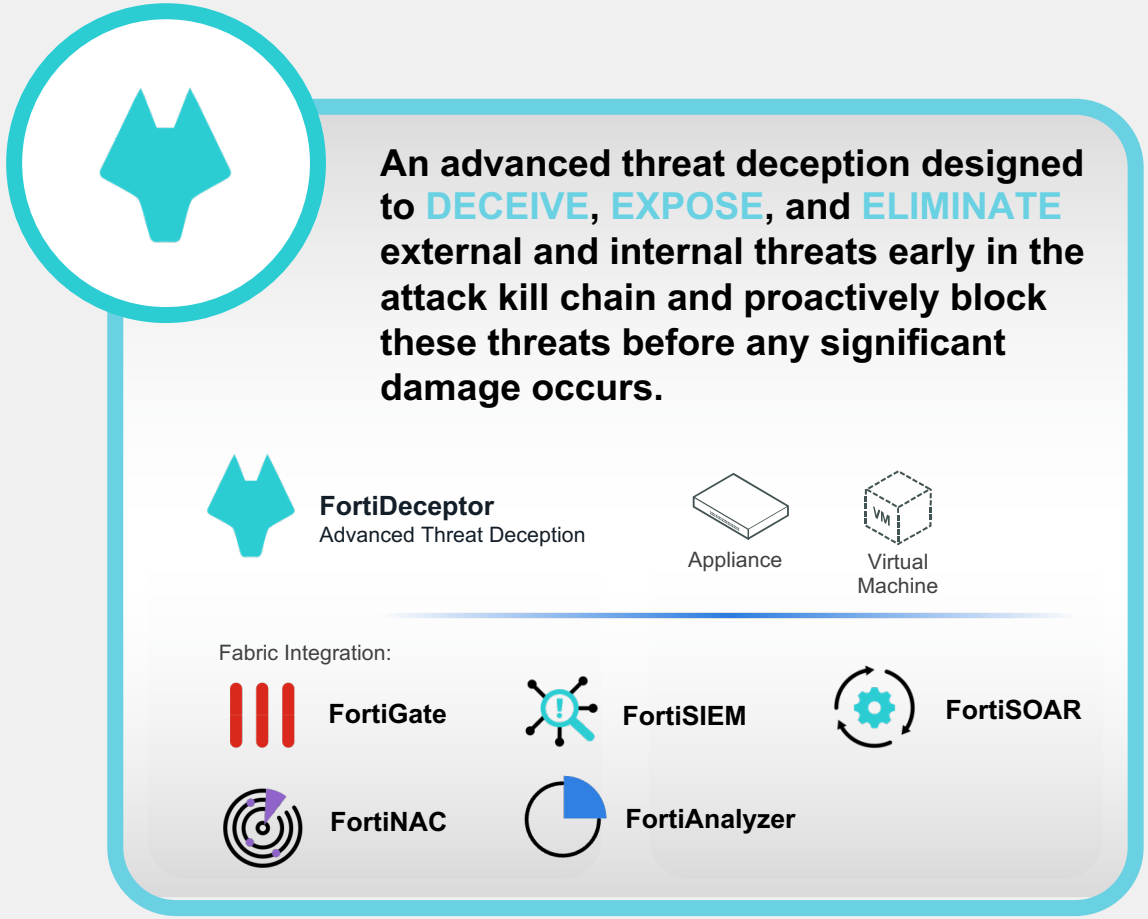
FortiFone
Robust IP Phones w/ HD Audio with centralized management

FortiVoice
Integrated voice, chat, conferencing management, and fax with centralized

FortiCamera
HDTV-quality surveillance cameras for physical safety and security

FortiRecorder
High-performance NVR with AI-powered video management software

Why Deception?



1 **Protects both OT and IT**

- SCADA/ICS profile e.g. Rockwell Ethernet/IP, Siemens S7, Bacnet, IPMI, Modbus and etc.
- Windows and Linux with Git, VPN, SMB, SQL, etc. applications, and honeytokens
- Aligns with Purdue Model

2 **Unintrusive and Easy**

- No re-plumbing and taking SCADA/ICS offline
- No operational delay to perform its duties
- Automated discovery of network and assets
- AI-based recommended deployment

3 **Early detection and response**

- Early unambiguous detection of an external/internal threat actor touching a decoy
- Automated response via Security Fabric

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)

Endpoint Protection

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

- Behavioral 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

Reconnaissance

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

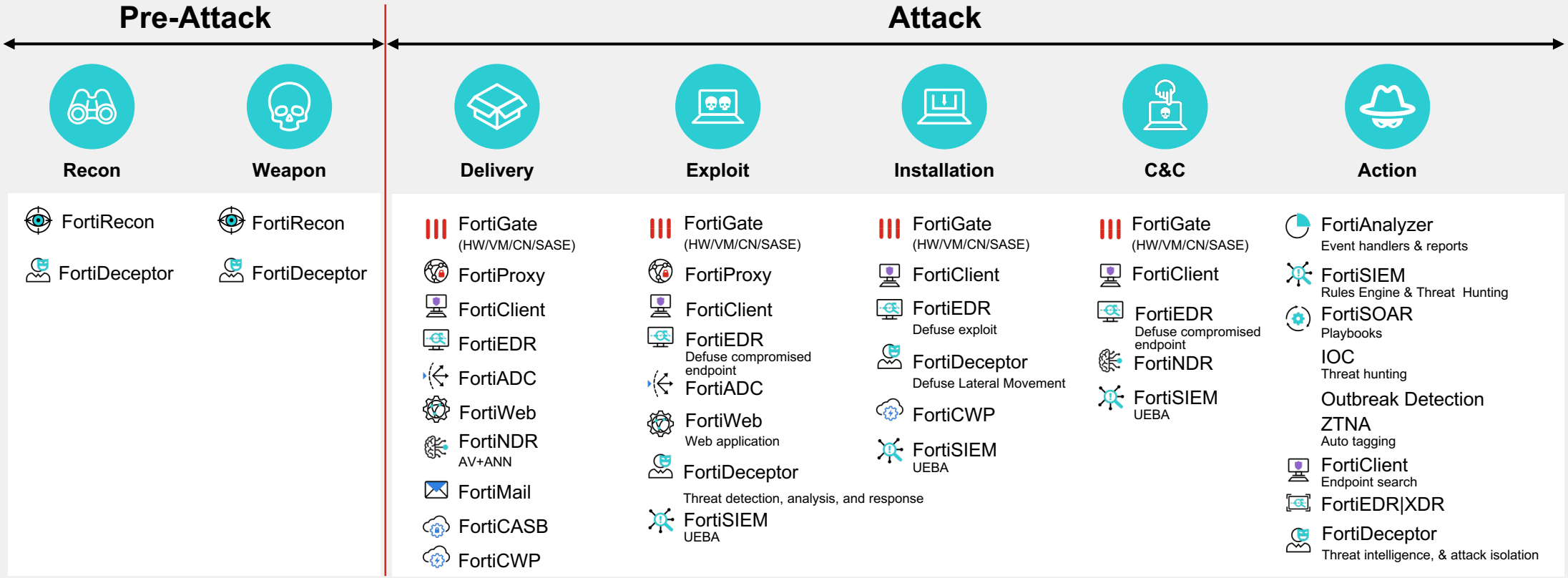
- Compliments existing solutions to complete visibility of the attack surface.
- Provides customers a view on what adversaries are seeing (EASM)
- Provides customer a view on what adversaries are doing (Brand Protection)*
- Provides customer a view on what adversaries are planning (ACI)*

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

- Protect the organizations brand reputation

Closing Thoughts

How to Break the Attack Sequence



In Summary

Some thoughts and conclusions

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

FORTINET Training Institute

https://training.fortinet.com/


FORTINET