

# Applying a Threat Informed Defense

Achieving Business Resiliency

Yuri Kramarz, Principal Engineer, Cisco Talos IR  
Tim (Wadhwa-)Brown, Security Research Lead, CX CoE Security  
May 2023



# Agenda



- ▶ The Case for a Threat Informed Defense
- ▶ Changes in the Threat Landscape
  - ▶ A Responder's View
  - ▶ Updates to ATT&CK
- ▶ Prioritising Critical Business Functions
  - ▶ Secure by Design
  - ▶ Efficacy in Response and Detection

# Modern Business and Cyber Resiliency

- Who are we?
- What is resiliency?
- What is a threat informed defense?

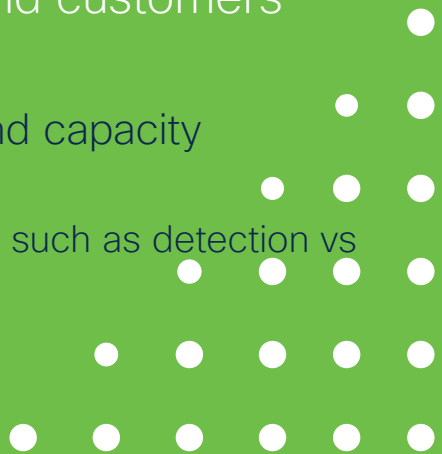
# The Ever Changing Threat Landscape

- In Q1FY23, healthcare sector targeted the most out of other sectors
- Hybrid cloud that is unmonitored
- Opaque supply chains
- Network, system, environmental complexity
- Alert fatigue
- Digitation of previously 'analogue' assets



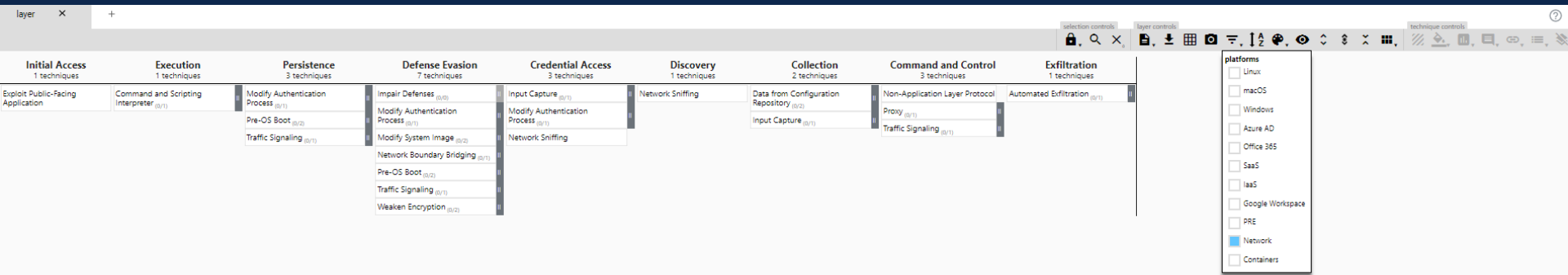
# How Cisco Works With MITRE's ATT&CK

- ▶ Cross-Cisco effort including Talos, CX and internal assurance and engineering functions
  - ▶ Active contributions to Networking, Linux and other domain matrices
  - ▶ Contribution of Threat Intelligence at a technique, groups and software level
- ▶ Benefits to Cisco and customers
  - ▶ Shared language
  - ▶ Allows capability and capacity measurement
    - ▶ Including questions such as detection vs visibility



# ATT&CK Can Help You Understand The Threats

- <https://mitre-attack.github.io/attack-navigator/>
  - Create New Layer
  - Enterprise
  - Filters > Platforms > Network



# What Impacts Business Resiliency?

- Architecturally
  - *Loss of confidentiality*
  - *Loss of integrity*
  - *Loss of availability*
- Business
  - Fines from data loss
  - Service outage impacting revenue
  - Loss due to fraud

*It depends on the business function...*

# What Are We Trying To Protect?

- Endpoint
  - Confidentiality
    - Data theft
  - Integrity
    - Fraud
  - Availability
    - Ransomware
- Server
  - Confidentiality
    - Data theft
  - Integrity
    - Fraud
    - Defacement
  - Availability
    - Denial of service
    - Ransomware


*It depends on the service...*



# Our Approach to Threat Modelling

- Analyse TI and ATT&CK for historical reporting
  - Who, how, why
- Collect and ingest critical asset data
  - Identify likely tactics for all critical assets
  - Select techniques based on technologies and other dependencies
- Map assets and techniques to a graph
  - Identify critical components in the kill chain
- Select, implement and validate necessary controls
  - Iterate





*Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.*

@JohnLaTwC

# Building Secure by Design Architectures

- What questions are we trying to answer?
  - Architects: Where do we place our controls to maximise our resilience?
  - Engineers: What risks do we need to consider when we operationalise technology?
  - Red Teams: What business functions would an adversary attack and why?
- Threat modelling with ATT&CK gives us the tools to help qualify and quantify these problems



# Preparing to Defend Your Critical Assets

- Understand the actual assets and processes
- Have a plan
- Build a long term resilience into security and assume some controls will fail
  - Map likely attack paths into MITRE ATT&CK and see what is detected
  - Purple Team and Threat Model your way into an active defence!



# Customer Challenges

Vertical specific systems not well understood

Prevention only security

Poor detection and response capabilities

Significant investment to implement and operate SOC

Keeping ahead in the ever-developing threat landscape

# Business Outcomes

Clearly defined threat model describing realistic, customer specific scenarios

Focused coverage mapping capabilities and capacity to scenarios

Supports governance, people, process and technology

Comprehensive development/improvement plans aligned to existing controls and identified gaps

# Cisco Value

Distinguished Cisco internal SOC

Expert security SMEs, with extensive experience in multiple regions and verticals

Proven methodology to evaluate and align real world threats to customer specific scenarios using MITRE's ATT&CK framework

Questions?

