Keynote - Critical Infrastructure Kung-Fu:
Evaluating Attacks and How to Defend

pwc

About Me

Chad Gray

Principal
PwC US/MX
Cybersecurity & Privacy

Summary

- Leader in C&P Practice, based out of Tysons/McLean Office is Washington D.C.
- Champion for Aerospace & Defense client sector
- Specializes in Operational Technology (OT) and Internet of Things (IoT) security

Background/Experience

- B.S. General Science, United States Naval Academy
- US Navy Information Warfare Officer, Retired
- Technical Director, SIGINT Technical Analysis (STA) Team, Ft. Meade, Maryland
- Founder of Booz Allen **Dark Labs** – R&D Cyber Incubator
- **NOT** a black-belt in any martial arts, but I've dabbled in Tae Kwon Do, Judo, Karate, Boxing, and Wrestling…

Agenda

- Discussion of OT, IoT, and Critical Infrastructure
- Characterizing the Cyber Threat
- Staying Ahead of the Threat
- Call to Action

Discussion of OT, IoT, and Critical Infrastructure

Operational Technology (OT)

- Technology that detects or causes change through monitoring or control of physical devices, processes, and events
- Where Cyber meets the physical world
- Examples:
  - HMIs, Historians
  - PLCs, IEDs, RTUs
  - Sensors, Actuators

Internet of Things (IoT)

- Networked electronic devices beyond typical desktops, servers, phones, and tablets
- Through connectivity, allow greater interaction of data and abilities
- Examples:
  - IP Cameras
  - Biometric sensors
  - Home Automation
  - Medical Devices
  - HVAC Systems
  - VR/AR Headsets

Critical Infrastructure

- Assets essential for a functioning and safe society and economy
- Can be classified at several levels - societal, national, regional, local
- Example:
  - Trans-oceanic fiber
  - Electric Power
  - Health Sector
  - Emergency Services
  - Transportation
  - Water/Wastewater
  - Financial

What is the Threat

Criminal Actors

- Financially motivated
- Types:
    - Intellectual Property Theft
    - Direct Gain - Ransomware
    - Indirect Gain - Destabilization for Stock Market Gain
- Trends:
    - Moving from high-volume low-yield ransomware to targeted high-yield attacks
    - Repurposing of leaked nation-state tools

What is the Threat (continued)

Nation State Actors

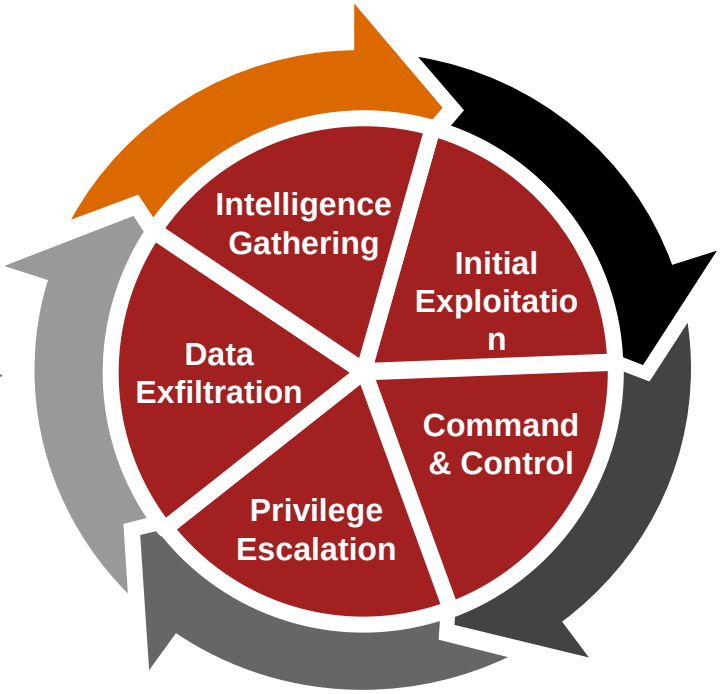
- Politically, Ideologically, Strategically, Defensively motivated
- Types:
  - Targeted Exploitation
  - Prepositioning
  - Deny, Degrade, Disrupt, Destroy
- Trends:
  - From clumsy, overt, attributable methods to covert, targeted, and surgical methods
  - Misattribution
  - Becoming more process oriented towards achieving a specific effect
  - Targeting Safety Instrumented Systems (SIS)

The OT Cybersecurity Kill Chain

How Threat Actors Can Use IT to Manipulate OT Systems

Targeted OT Attacks

- Threat actors use inherent vulnerabilities in OT systems to reach specific machines, individuals, networks, or organizations across all industries
- These exploitations are often signature-less and difficult to detect using traditional security defenses
- Over time, threat actors will gradually strengthen their foothold, until they are able to move laterally to critical systems and manipulate core OT functions or exfiltrate data
- Threat actors can maintain a persistent presence across multiple devices, until they are identified and removed



Intelligence Gathering	*Initial Exploitation*		*Command & Control*		*Privilege Escalation*		*Function Manipulation/Data Exfiltration*		
Conduct background research	Execute initial attack	Establish foothold	Enable persistence	Conduct enterprise recon	Move laterally to new systems	Escalate privileges	Gather and encrypt data of interest	Exfiltrate or alter data from affected systems	Maintain persistent presence

How to Stay Ahead of the Threat

Know Yourself

- Can't defend what you don't know you have
- Hardware, Software, Firmware, Network, Protocols
- People, Processes, Technology
- Third-Party and Supply-Chain
- Versions, Patch Levels
- CWE and CVE

Follow A Program

- Start with Existing Standards
- IEC 62443, NIST 800-82
- Start from the Enterprise down versus control level up
- Build relationships, understanding, and buy-in across IT and OT Organizations

Get a Good Stance

- Establish Security Zones
- Control flow of data
- Establish and Manage Firewall Rules
- Whitelist processes (design deterministically)
- Whitelist access
- Segment your SIS systems
- Guard Workstations, HMIs, and Data Historians
- Backup logic/configurations

How to Stay Ahead of the Threat (continued)

Protect Yourself

- Establish Monitoring to “see” threats or bad hygiene
- Industrial SIEMs - Level 1,2,3
- EDRs/Agents on Level 2,3 IT Assets
- Log Aggregation
- Think OT/IT Fusion for viewing in SOC to correlate across both environments

Analyze Your Foe

- With ability to “see”, create analytics to spot bad behaviors
- Build Use-Cases for Mitre Att&ck Framework - but beyond for the OT environment
- Apply machine learning techniques on logs and/or historian data
- Ingest Threat Intel

How to Stay Ahead of the Threat (continued)

Test Yourself

- Conduct “technical testing” (not calling it a “pentest”)
- Evaluate attack surface
- People, Process, and Technology
- Use different modes - White Hat, Grey Hat, Black Hat
- Insider Threat simulation
- Crisis Management Simulation

Practice Sparring

- Red Team - begin to emulate likely attack scenarios and/or actors
- Blue Team - Conduct training simultaneously to spot attacks and respond procedurally
- Build Attack Trees

How to Stay Ahead of the Threat (continued)

Master Your Domain

- Conduct Threat Hunting - Employ the “1%”
- Create a Research Environment to test new technologies, equipment, protocols
- Looking for the Unknown/Unknowns (new actors, new techniques, new vulnerabilities, new exploits)

How to Stay Ahead of the Threat (continued)

Defeat Your Adversary

- Stay ahead of actor's ability to evolve their techniques
- Keep moving - employ newer architecture, standards, and security measures to stay ahead
- Be disruptive - invest in innovation to create environments that are a first seen for your foe
- Force the enemy to play by your rules, not theirs

“I will forget the mistakes of the past, and press on to greater achievements”

-Chuck Norris

- Chun Kuk Do - 2nd Rule
- Get out of old habits - start forming new ones
- Don’t set sights on being good enough - focus on being great

“To be the best, you have to constantly be challenging yourself, raising the bar, pushing the limits of what you can do. Don’t stand still…leap forward!”

-Ronda Rousey

- 1st American Olympic Medalist in Judo
- 1st and longest reigning UFC Female Champion

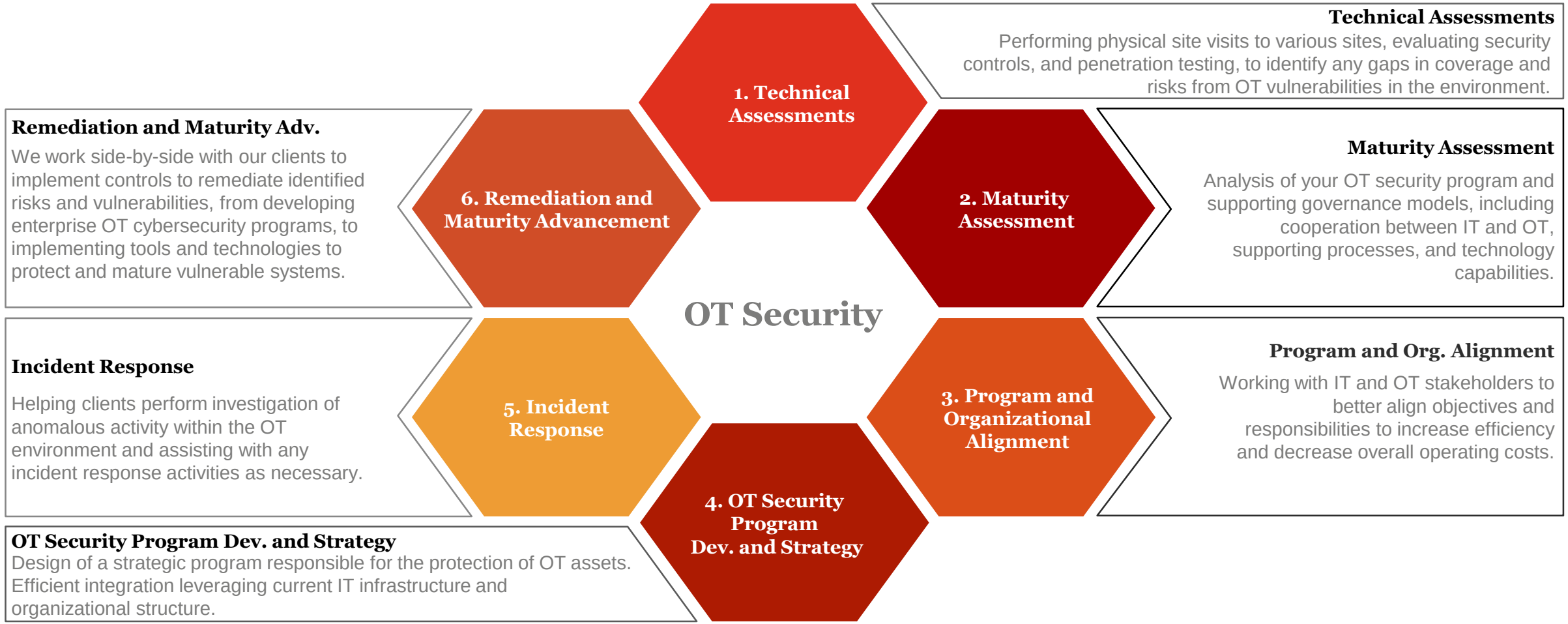
“Be Like Water - Remain fluid, adapt, and force your opponent to fight a different fight”

-Bruce Lee

- Develop your own styles
- Be unpredictable, and difficult for your adversary - to make them go away, or at least stay a step behind
- Don’t stop changing - constantly evolve. Be a moving target

PwC's ICS Security program components

Helping our clients from strategy through execution



Thank you

pwc.com