ICS Active Defense

About Me

- Robert M. Lee (@RobertMLee)
- AF Cyber Warfare Operations Officer
  - My views/comments definitely only represent me
- Co-Founder Dragos Security LLC
- SANS ICS 515 Course Author
- SANS FOR 578 Course Co-Author
- PhD Candidate at Kings College London
- Author of:
  - *SCADA and Me: A Book for Children and Management*
  - *Little Bobby*

A Bit of History

John Boyd and the Aerial Attack Study

- Before Boyd, if you were a fighter pilot you had it or you didn't
- "Feel the stick" "Who's the best? Not you if you have to ask…"
- John Boyd was a U.S. Air Force fighter pilot who "had it"
  - (The OODA Loop guy…)
- Saw that there were lessons to be derived from case studies
- Developed strategy and a science behind air-to-air combat
- Revolutionized fighter pilot tactics (1950's – 1970's)
- On-going non-static strategy and process (evolved over time)

The Need in Our Field

- Silos and Stubbornness
  - "I've done this for 30 years what would you know"
  - "Yea well you're from IT you just don't get it"
- Defense is currently fairly static and binary
  - Poorly defined winning or losing
- Myths and excuses dominate the popular mindsets
  - "Hackers always get through"
  - "Traditional defense fails"
  - "Blame the APT"
- Very little learning from engagements with the adversary
  - They are there and we are definitely a target; time to learn!

Active Defense

Active Defense In Other Domains

- Mao Zedong – 1937
  - "On Guerilla Warfare"
- Active Air and Missile Defense – 1950's – 1980's
- General Depuy – 1976
  - "FM 100-5 Operations"

Active Defense's Purpose

- Relied heavily on indications/warnings and adversary info
- Mobile force that took advantage of strengths
- Quick response to adversary where it was advantageous
- Assumed adversary had upper hand (tech, numbers, etc.)
- Was intended to "counter-attack" internally but not strike back

Categories of 'Cyber' Defense

- Defense is intended to restore peace and equilibrium
- Multiple aspects contribute to defense, it's not binary
- More granularity is needed than "intel" "defense" "attack"
- Conceptual framework for analyzing case-studies:

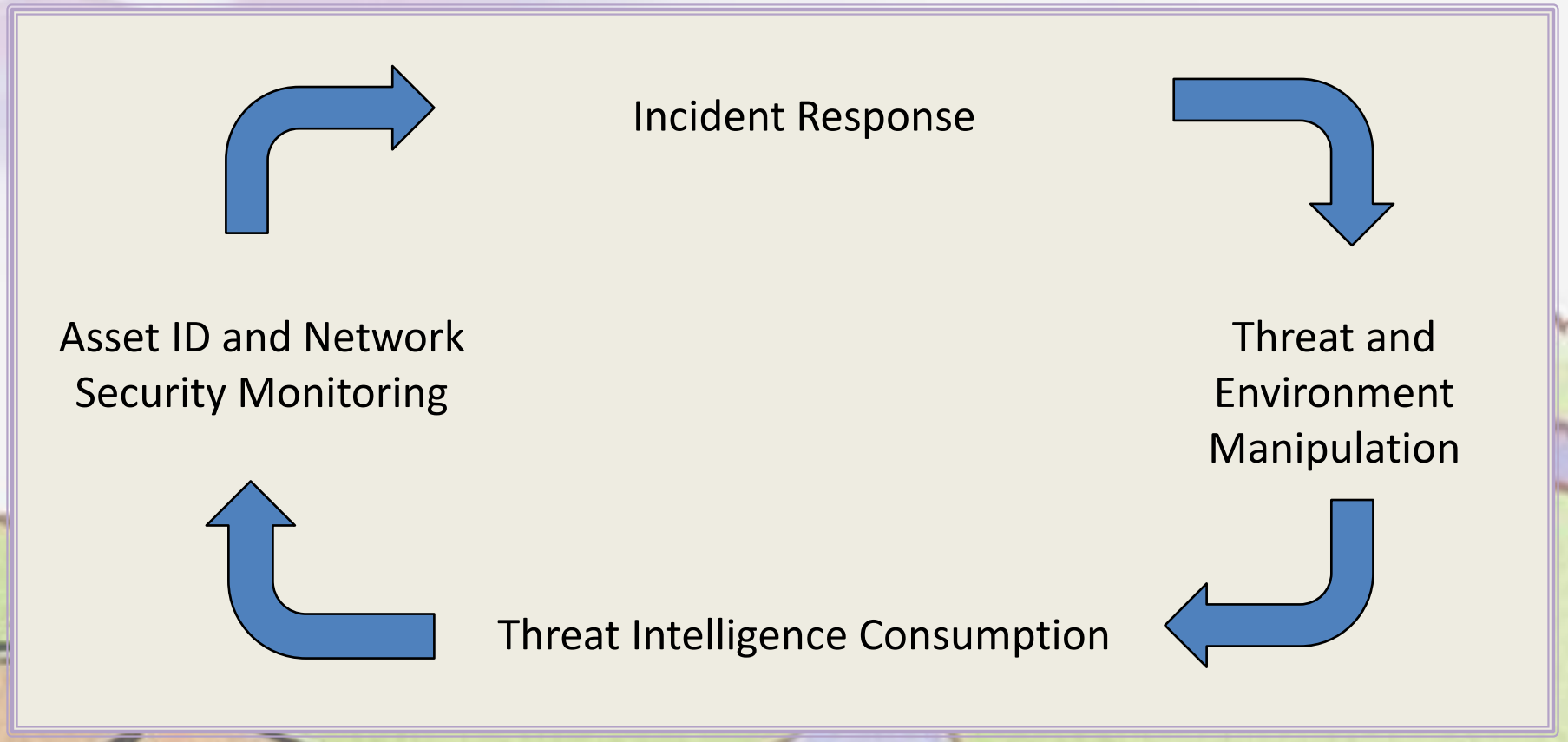
Architecture – Passive Defense – Active Defense – Intel - Offense

A Strategy for Active Defense

Influences for the Strategy

- Developed in IC, USAF, Private Sector, Academia, and Training
- Influenced by the works of so many in the community and building upon what has been developed instead of tearing all apart and trying to start over (observational vs. innovative)
- Analysis of case-studies where defense failed
- Analysis of case-studies where defense succeeded
- Tested in various settings including government SOC and ICS/SCADA community

Active Cyber Defense Cycle



Threat Intelligence Consumption

- Helps solve the #1 issue – What do I do with it?
- Creating Threat Intel and "consuming" Threat Intel lead to different results and mindsets
- Threat Intel != Threat Data
  - Articulated process (Intelligence Lifecycle, ACH, etc.)
- In ACDC:
  - Know the operational environment/threat landscape
  - Know what options are even available to the adversary
  - Identify what is needed specifically for the organization/mission
  - Articulate internal and external knowledge to make the teams better

Example: BlackEnergy2 and Threat Intel

- Scenario:
  - BlackEnergy2 (BE2) was previously criminal linked only but then was observed targeting ICS specifically (GE CIMPLICITY, Siemens, etc.)
- Threat Intelligence (generation)
  - Teams and vendors identify the malware, OSINT, patterns among the victims, different modules and variations of the malware, and attempt to identify the adversary motive, infrastructure, capabilities, and victims
- Threat Intelligence Consumption
  - ICS Facility X previously determined what their threat landscape was
  - ICS Facility X previously incorporated into training and plans to use IOCs
  - ICS Facility X already knows good sources of external AND internal data
  - ICS Facility X now knows if they are vulnerable and how to look for BE2

Asset Identification and Network Security Monitoring

- Asset Identification – know thyself
- Network Security Monitoring:
  - Collect
  - Detect
  - Analyze
- Generally understood in security operations/ntwk monitoring
- In ACDC:
  - True understanding of the network means its easier to find abnormal
  - Threat intel to guide searches and incident responders to fight threats
  - Assistance throughout the process and even against multiple threats
  - ICS facilities are fairly static; *shouldn't* have Enterprise like traffic

Example: BE2 and Asset ID and NSM

- Scenario:
  - BE2 communicates to external command and control (C2) servers and scans the networked environment; infection confirmed in ICS Facility X
- Asset Identification
  - Knowing the infrastructure helps “hunt” through it for NSM but also helps to determine the threat landscape
  - Knowing the network topologies helps identify “odd”
- Network Security Monitoring
  - Personnel would have identified the abnormal C2 communication as BE2 was targeting Internet connected ICS assets; easy to map communications
  - Internal network scanning can be revealed with whitelists of communication even if at a high level and for information purposes only

Incident Response

- Response after a true threat is identified
  - Determine the scope of the threat
  - Collect useful/forensically sound evidence
  - NIST standard model (as a guideline)
- Focus is on keeping operations running not just kill the malware
- Biggest IR problem is lack of preparation ahead of time
- In ACDC:
  - Preparing with the teams, training, and identifying weak spots
  - Understanding what systems are most critical or most likely to be hit

Example: BlackEnergy2 and Incident Response

- Scenario:
  - With confirmed BE2 incident, the ICS Facility X team begins work while utilizing the NSM personnel to focus and target their hunt
- Incident Response
  - In OT you cannot just quickly go through “identify, contain, eradicate”
  - ICS Facility X enabled logging on devices (including field) and centralizes their collection for analysis; identifies ahead of time devices that can’t
  - ICS Facility X identifies the scope of the infection of BE2 to inform leadership on what systems need cleaned and when/where/how
  - ICS Facility X knows what it can and cannot do locally but knows how to access and obtain forensically sound digital evidence
  - ICS Facility X captures sample of malware and related data for analysis

Threat and Environment Manipulation

- Interacting with and manipulating the threat to learn from it
  - Only done in YOUR network not theirs
  - Mostly based on malware analysis but not all threats are malware
- Interacting with and manipulating the environment
  - Only battlefield in history where we can change the territory
  - C2 sink holing, defeating hard coded malware, etc.
- In ACDC
  - Taking samples of threat from Incident Response or NSM to work with
  - Using the network against it while learning from it (IOCs, TTPs, etc.)
  - Feeds back into Threat Intelligence Consumption

Example: BE2 – Threat and Environment Manipulation

- Scenario:
  - BE2 samples obtained and passed from IR to the TEM personnel
- Threat and Environment Manipulation
  - Running BE2 in sandboxes reveals network traffic that can be identified
  - Analyzing the code of BE2 shows plugins for this toolset
  - The plugins gave it the capability to steal passwords, scan the network, identify information from various aspects of the system, and destroy
  - The Dstr (Destroy) plugin is of particular concern for ICS
  - TEM analysts having identified the malware's capabilities could make recommendations to change the environment (logical re-routing of IPs)
  - TEM analysts could create IOCs for the NSM and IR team; passed through Threat Intelligence Consumption team this would be paired with other threat research such as that from anti-virus vendors

Example: Full Circle

- Network Security Monitoring
  - Identify the abnormal network traffic such as odd Internet connections to the BE2 command and control servers or internal traffic such as network scanning
- Incident Response
  - Identify the impacted systems and contain the infection while informing leadership of changes and passing data throughout the cycle
- Threat and Environment Manipulation
  - Collect and analyze the BlackEnergy2 sample from the IR team
  - Malware analysis to determine its capabilities and potential impact on the environment
  - Make recommendations for logical network changes to re-route exfil and C2 traffic
  - Create IOCs
- Threat Intelligence Consumption
  - Collect and formulate the internal data sources
  - Seek and obtain external data so efforts are not duplicated (inform TEM)
  - Pass IOCs to NSM to watch for re-infections, more infected systems, etc. for IR to handle
  - Pass IOCs to IR to scope the infection fully and eradicate the threat

Implementing the Strategy

- Outsource is ok as long as the teams work together
  - Most ICS facilities cannot sustain a SOC type organization
  - At the very minimum plan ahead of time and identify the person who essentially “owns” that process
- Must understand the purpose and the organization’s missions
  - No response can be effective towards defense without understanding this
- When not actively engaged with a threat - train
- Store lessons learned and developed knowledge over time
- Mix IT and OT personnel into the various teams
  - Get them to field sites and integrate with those running the show
- Can be used at a team level and the organizational level

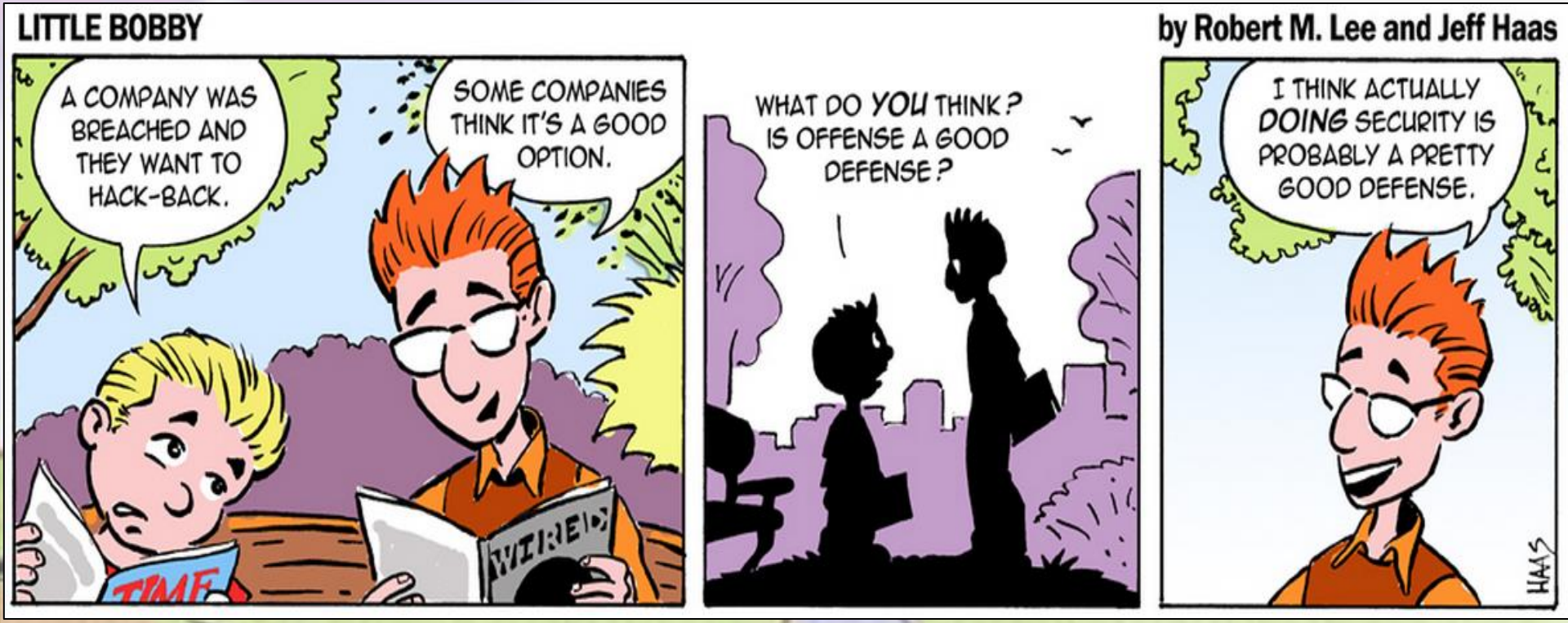
Conclusion

- Must think of a strategy (not just a PPT version of a strategy)
- Determine and define processes that play to strengths
- ACDC is one strategy – determine if it works for you
  - If it doesn't work for you then find something that does
- Understand self and the threat to counter appropriately
  - There are limited options available to adversaries
- Security is hard but – Defense is Doable

Takeaway Resources

- "Boyd: The Fighter Pilot Who Changed the Art of War"
  - by Robert Coram
- "Strategy: A History"
  - by Lawrence Freedman
- "The Practice of Network Security Monitoring"
  - by Richard Betjlich
- "Incident Response and Computer Forensics 3rd Edition"
  - by Jason Luttgens, Matthew Pepe, and Kevin Mandia
- "Psychology of Intelligence Analysis"
  - by Richards Heuer
- Threat Intel/Intrusion Analysis Resources
  - www.activeresponse.org
- Little Bobby
  - www.LittleBobbyComic.com

Questions?


LITTLE BOBBY
by Robert M. Lee and Jeff Haas
A COMPANY WAS BREACHED AND THEY WANT TO HACK-BACK.
SOME COMPANIES THINK IT'S A GOOD OPTION.
TIME
WIRED
WHAT DO YOU THINK? IS OFFENSE A GOOD DEFENSE?
I THINK ACTUALLY DOING SECURITY IS PROBABLY A PRETTY GOOD DEFENSE.
HAAS