Network Threat Hunting

Success: Part 3 of 3

Network Threat Hunting

- Visibility
- Analysis
- **Success**

Intro

Michael Meason – Deep 6 Security, LLC

- Areas of Influence
  - Telecommunications Engineering
  - Network Engineering
  - Cyber Security Operations
- Letters
  - BS in CIS, MS in Telecomm., CISSP, CSFI-DCOE, NSTISSI 4011,4015, CNSSI 4012-4016, Certified Cyber Intel Tradecraft Professional
- Others
  - Husband/Father, KG5DQA, Aviation
- Handle
  - SigmetXray

Intro

Trae Norman – Deep 6 Security, LLC

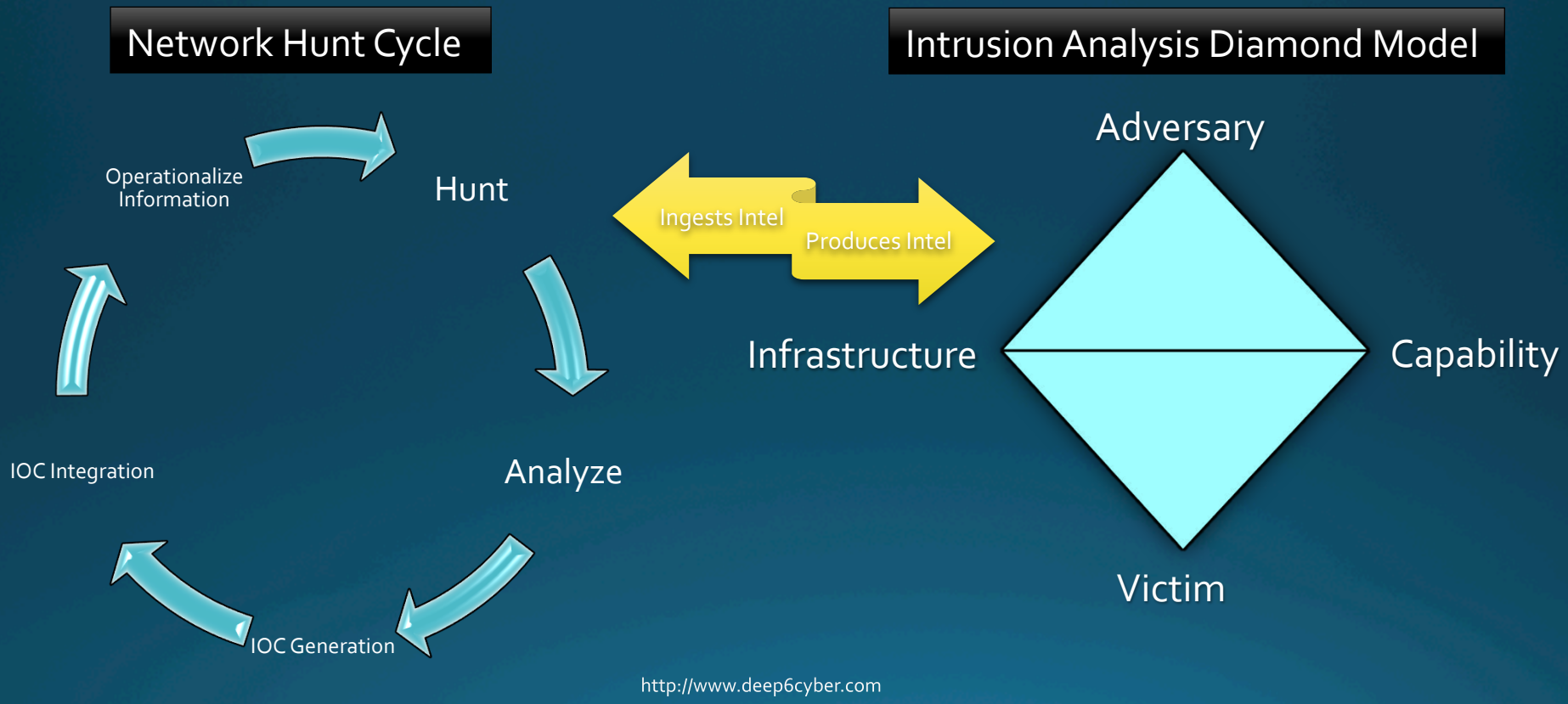
- Areas of Influence
  - Information Technology Administration and Engineering
  - Information Security
- Letters
  - CISSP, CEH, GCIA, GNFA, MCITP, MCSA, MCTS, BS in CIS
- Others
  - Husband/Father, Hobbyist Programmer
- Handle
  - SH

- Keys for Success
- Potential Tools
- Tips and Tricks
- Now What?

Keys for Success

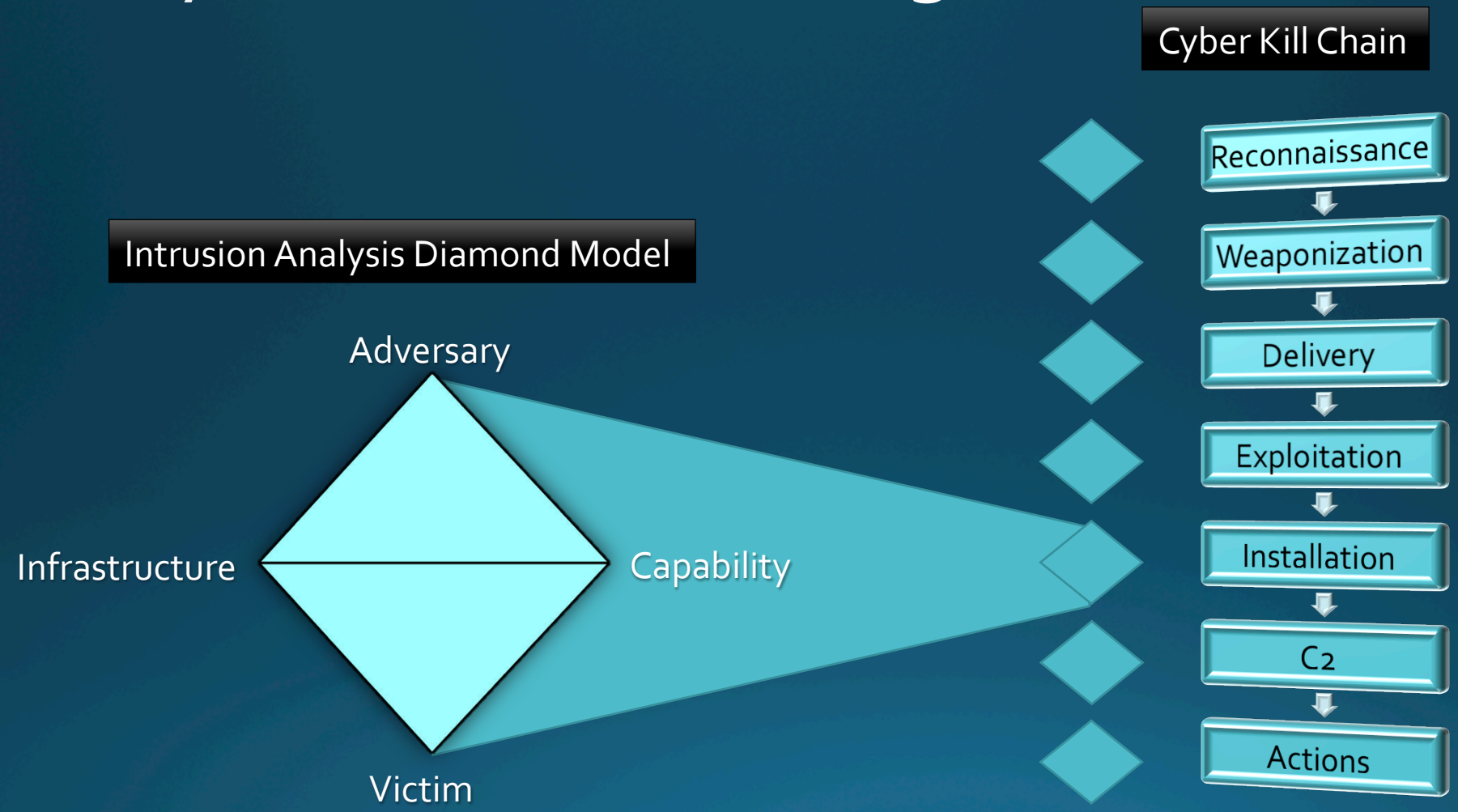
- Hunt Cycle
- Cyber Kill Chain Integration
- Concerns
  - Cost
  - Integration
  - Maturity

Hunt Cycle



http://www.deep6cyber.com

Cyber Kill Chain Integration



Cost Concerns of Hunting

- Use Open Source
- Analysts are relatively low cost
- Use automation as a tool
- Conduct during down times
- Gather data continuously for spontaneous hunts

Integration

- Gain visibility passively
- Integrate results for ROI
- Routinely schedule the hunts
- Document results and hot wash
- Produce general procedures of hunting
  - Caution: Don't constrain analysts

Maturity

- Hunting will mature your program
- Analysts get familiarity with:
  - Architecture
  - Operations
  - Data Flows
- General security knowledge will increase
- Stronger detective/preventative measures
- Operations will streamline
- Creativity will increase

- Keys for Success
- **Potential Tools**
- Tips and Tricks
- Now What?

Potential Tools

- Network Data Recorders
- Log Parsers
- Syslog
- Custom Software & Others

Network Data Recorders (NDR)

Commercial Products

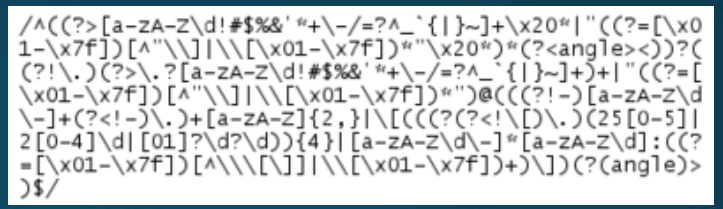
- Pro
  - Stability… usually…
  - Support and maintenance
  - User friendly… usually…
- Con
  - Dependency
  - Costs
  - Limited direction input
- Colasoft, nChronos
- CyberESI, DXR
- Savvius, Omnipliance

Open Source

- Pro
  - Free
  - Customizable
  - Inside visibility
- Con
  - Little to no support
  - Project could vanish
  - Greater knowledge needed
- AOL (unaffiliated), Moloch
- Community, OpenFPC
- Community, Packetpig

Log Parsers

- Many many log analyzers out there
- Fit the tool to the device
- Try to get analytics
- Reports and GUI usually help



- Examples
  - ManageEngine, Firewall Analyzer
  - Microsoft, Log Parser 2.2

Syslog

- Benefits
  - Standardized format
  - Easily parsed
  - UDP or TCP
  - Encrypted
- Know Regular Expressions
- Data aggregation

- Examples
  - Good 'ole plain Linux
  - Splunk

Custom Software & Others

- Custom Software
  - Pros
    - Adaptable
    - Little to no cost
  - Cons
    - Ongoing maintenance

- Anything you can write to assist you
- Make sure you have support for in-house code

- Keys for Success
- Potential Tools
- **Tips and Tricks**
- Now What?

Tips and Tricks

- PCAP Filters
- Geo Discrimination
- Capture Filters
- Perimeter

PCAP Filters

- Display filters remove the white noise
- Understand the pcap filter syntax
- Try these
  - IP Protocol Specific
    - ip.proto == <TCP/UDP/ICMP>
  - SNMP Community Strings
    - snmp.community == public || snmp.community == private
  - NetBIOS External
    - nbss && ip.dst != [<INSERT HOME NET>]
  - Mirai Botnet Typical Scan
    - port.dst == [23, 123, 2323, 5060, 27015] && ip.src != [<INSERT HOME NET>]
  - DNS Egress Filtering Monitor
    - port.dst == 53 && ip.src != [<INSERT HOME DNS SERVERS>]

Geo Discrimination

- Block the countries you don't need on egress
- Elevates your organization in the fruit tree
- Remember to update the RIR databases
- Start with these
  - Russia, China, Syria, Iran… well every other country besides USA
- Review https://www.state.gov/ for a list of banned countries

Capture Filters

- Capture Filters increase retention without added cost
- Only the traffic you want to look at
- Reduces resource consumption on the capture device

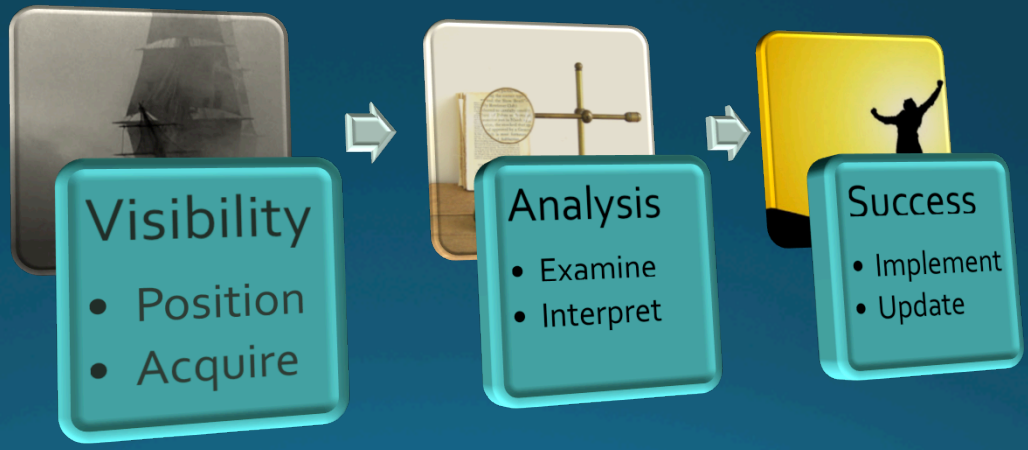
Perimeter

- Always have eyes on your perimeter packets
- NAT traffic useless without translation table
- Behind firewall/router
- Be inside DMZ, these are windows into your house

- Keys for Success
- Potential Tools
- Tips and Tricks
- **Now What?**

Now What?

- Gather your tools
- Analyze your data
- Generate goodness



Circle of Goodness

2017 Security Education Week

Austin, Texas -- May 15-19, 2017

time left: 46 days | 18 hrs | 06 min

Home | Agenda | Session Details | 2017 Instructors | Venue | Contact Us | Register!

Session Details

Introduction to Network Threat Hunting for Utilities (8 hours)

Mike Meason, Deep 6 Security, LLC

This session will instruct students on theoretical and practical concepts which facilitate the creation of network threat hunting operations in utilities. The concepts will be provided as a foundational approach to ensure that all audience members attain knowledge required to begin threat hunting operations no matter the maturity level of their current operations. This course will address prerequisites required as well as more in-depth technical approaches to threat hunting based on the day-to-day experience of utility security operations.

http://security-education-week.energysec.org/registration/

Questions?

mike@deep6cyber.com
trae@deep6cyber.com
Twitter - @deep6cyber.com