
A Primer on Threat Intelligence
Dr. Courtney Falk
OPTIV

Outline

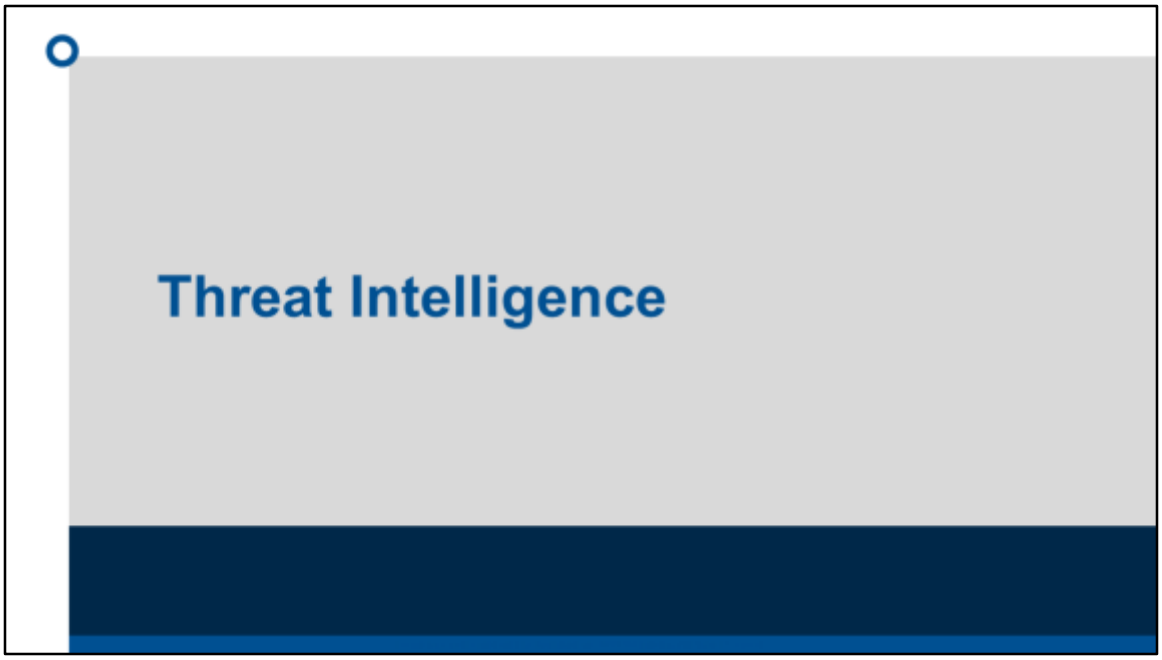
- What is threat intelligence?
- How does one mature a threat intelligence program?

OPTIV

Who am I?

- Former member of the intelligence community
- Hoosier by geography, Boilermaker by choice
  - Three-time graduate of Purdue University
- CISSP
- Research scientist for Optiv, Cyber Threat Intelligence
- International man of mystery and bon vivant
- Hates the term: "APT"
- Reach me at: first name dot last name at optiv.com

OPTIV


Threat Intelligence

A Definition

- Intelligence work comes from a military history
  - Like cryptography, it eventually finds a use case in industry
  - But for a company, it's fighting with one hand tied behind your back
- Collection, analysis, and reporting of data
  - Not an intelligence product until a human analyzes it
  - Corroborate data (see Mandiant's APT1 report)
  - Determine confidence
- It's a flashlight, not Sauron's eye
  - Collection of salient data is not guaranteed
- Basic concepts:
  - Who are the individuals or groups threatening your organization?
  - Tools, techniques, and procedures (TTPs)

5

OPTIV

Mandiant's APT1 report can be found at:
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

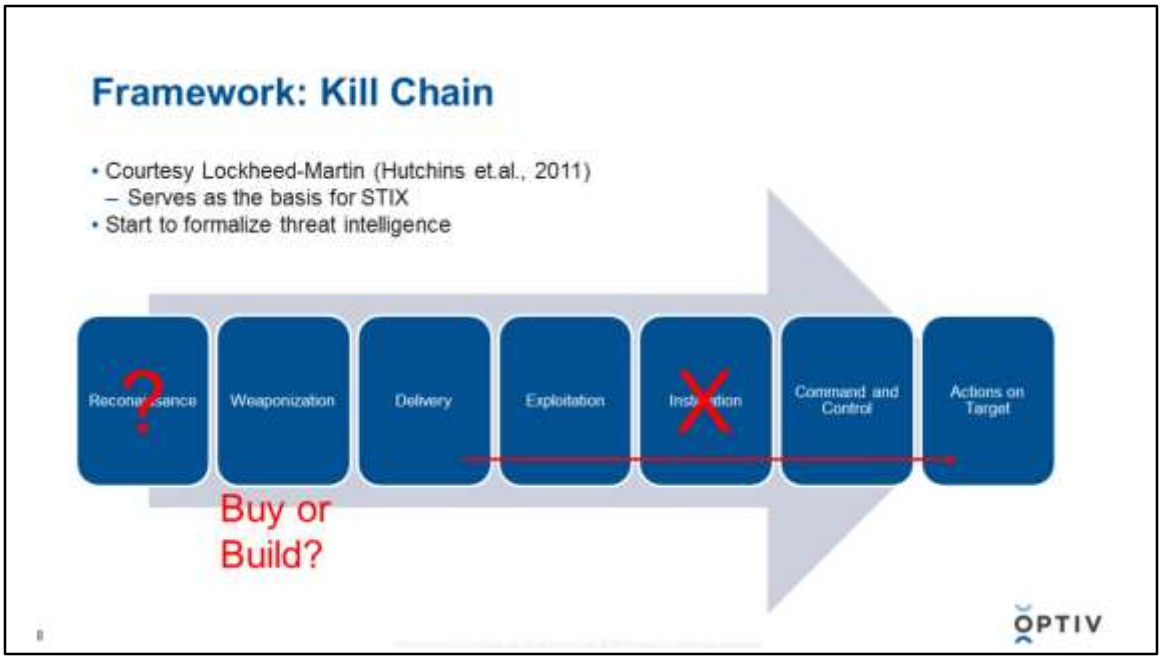
The Intelligence Cycle

OPTIV

Do I Need It?

- How big are you?
  - Mom and pop shops can't afford a dedicated threat analyst position
  - More work than can be dumped on somebody with an existing job
  - Are there historical precedents?
  - Does your vertical have attack trends?
    - Spring is tax and identity theft season
    - Hospitals
  - Has your organization already been attacked?
- Is it required as a part of insurance?
- Are you safeguarding others' information?
  - Payment cards
  - Personally identifiable information
- How mature is your understanding of threat intelligence?

OPTIV



Kill chain paper:
http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Standards and Sharing

- Indicators of attack
  - CybOX
  - OpenIOC
- Putting it together
  - Structured Threat Intelligence eXpression (STIX)
- Share it
  - Trusted Automated eXchange of Indicator Information (TAXII)
- Please don't roll your own
  - A lot of time and effort
  - Error prone
  - Non-interchangeable

OPTIV

CybOX: https://cybox.mitre.org/about/
OpenIOC: http://www.openioc.org/
STIX: https://stixproject.github.io/


Maturing Threat
Intelligence

Maturity

- The organizational needs for threat intelligence vary by size and maturity
- EclecticIQ defines a TI maturity model of 8 dimensions of 5 steps each
- Consider just the awareness dimension:
  1. Aware
     Know about threats
  2. Reactive
     Employ threat indicators and related tools
  3. Adaptive
     Improve the security posture based on human analysis
  4. Purposeful
     Focus on threats and actions relevant to the organization
  5. Strategic
     Threat intelligence informs the organization's decision making process

11

OPTIV

Find the EclecticIQ threat intelligence maturity model paper at: https://www.eclecticiq.com/resources/white-paper-threat-intelligence-maturity-model

Ways Forward

- Some light reading
  - FireEye/Mandiant - M-Trends
  - Symantec - Internet Security Threat Report
  - Ernst & Young - Global Information Security Survey
  - Akamai (DDoS)
- Getting involved
  - Information sharing and analysis centers (ISACs)
    - There is an ISAC for every business vertical and then some
      - Financial services (FS-ISAC)
      - Automotive manufacturing (Auto-ISAC)
      - Non-federal, multi-state government (MS-ISAC)
    - National Council of ISACs
  - FBI InfraGard
    - Chapters based on regional and local geography
  - When in doubt, lurk more

OPTIV

Automate It with Tools

- Centralize your collection
  - SIEMs; aggregate your data/logs in one place
- Threat feeds (analogies to Wikipedia)
  - Some are free, some are pay-for-play
  - Do they validate and filter their data?
- Threat intelligence platforms (TIPs)
  - Sqrrl
  - Recorded Futures
  - Anomali ThreatStream
  - Phantom Cyber
- Hire some investigators
  - IntSights
  - Eclectic IQ
- Automate all the things
  - OpenC2 (DHS)

OPTIV

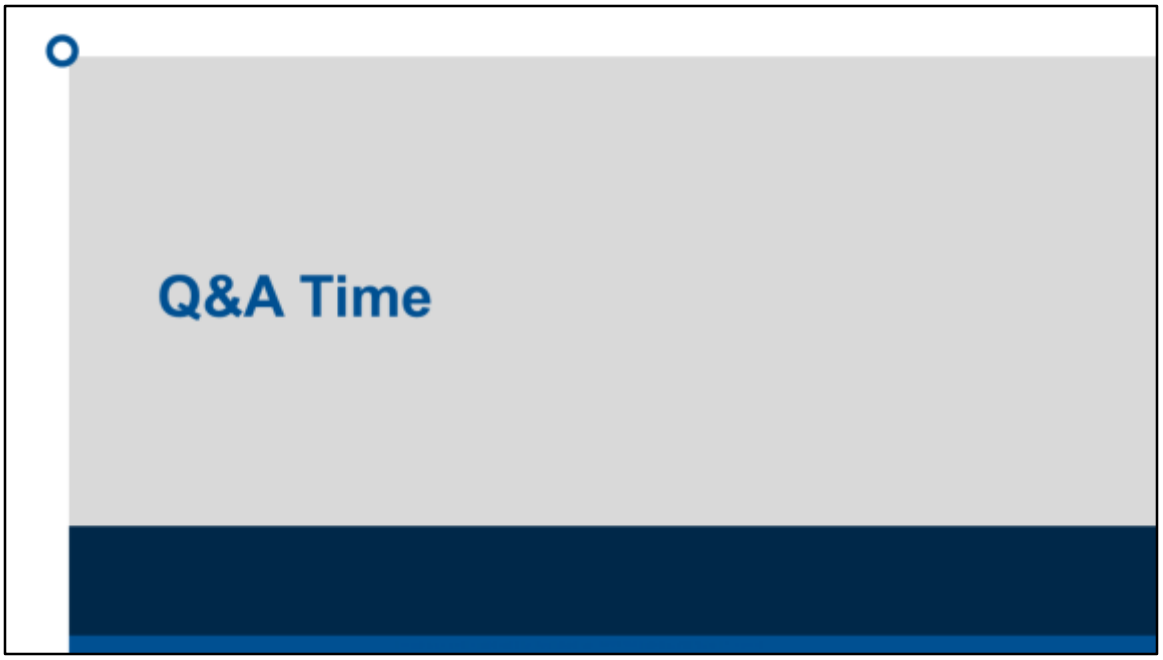
Threat Hunting

- Be proactive (one of the more mature TI levels)
- What aren't your tools catching?
  - Find the unknown unknowns
- Can contribute your findings back to the community

14

OPTIV

Image courtesy Sqrrl: https://sqrrl.com/solutions/cyber-threat-hunting/


Q&A Time


OPTIV