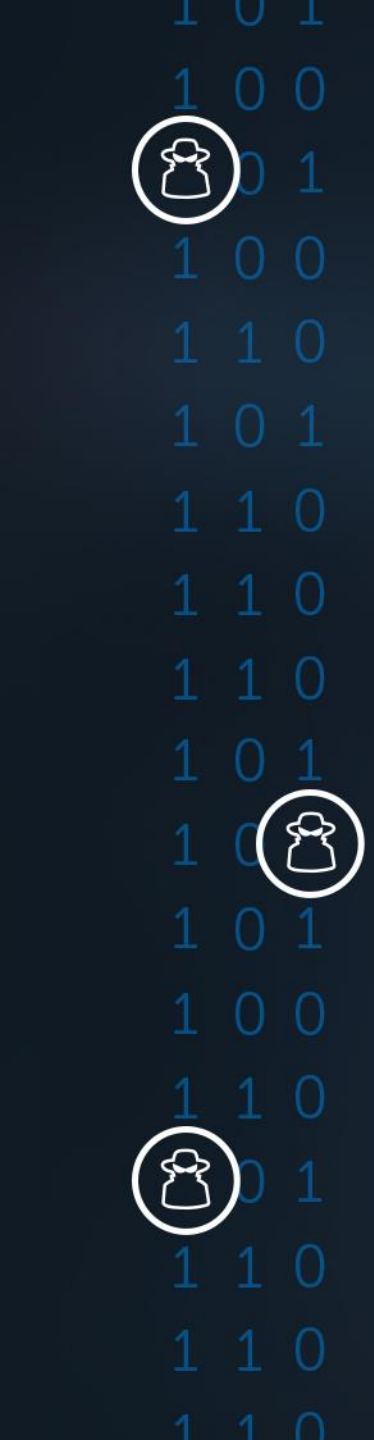


ANOMALI®

The Value of Threat Intelligence

David Empringham, Principal Sales Engineer

About Me

- Involved in Security since the late 90’s
- Started with 1 of the pioneering SIEM solutions
- Branched off into Governance, Risk & Compliance
- Cyber Threat Intel – feeds, curation, expansion, operationalization

** Disclaimer: This presentation does not have all the answers or a big red easy button.*

Value of Threat Intelligence - Where To Start?

- Sources of threat data/intelligence
  - OSINT – Open Source Intelligence
  - Exchange Membership
  - Commercial Vendors
  - Inhouse Tradecraft Analysis/Hunting

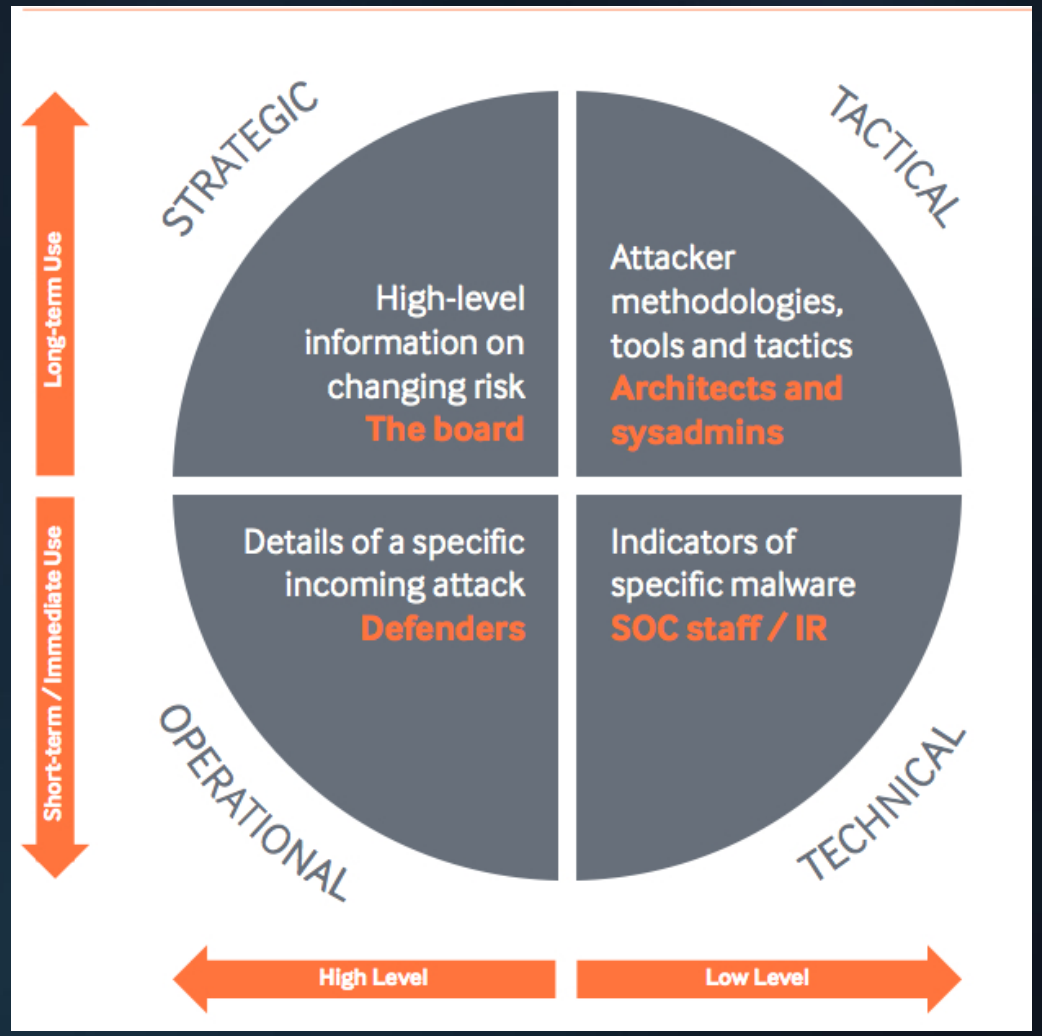
- Where is your Organization in the cyber journey?
  - Beginner – manually collecting/integrating OSINT
  - Intermediate – automatic integration, data reviews
  - Advanced – SOAR, strategic intel, remediation run book?

How Do CTI Sources Differ?

- OSINT
  - Specific classifications – Domain, IP, Hashes, etc.
  - Atomic indicators
    - Refresh frequency?
  - Integration into existing security controls
- Exchange Platform / Collaboration
  - Atomic indicators VS Finished Intel?
  - Collaboration? Dialog with co-members?
  - Integration into existing security controls?
- Commercial
  - Relevant organizational or industry specific analysis
  - Custom research or professional services
  - Niche focus

Types of Intelligence

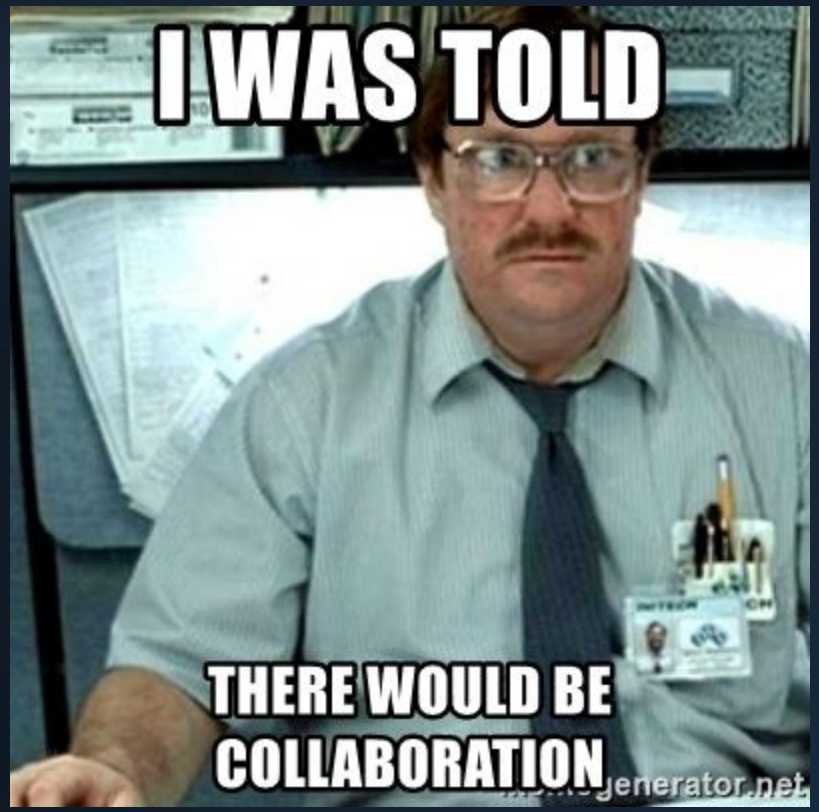
- Tactical
  - Atomic indicators
  - Automation – feeds or API
  - Integration into security tools (TIP)
- Operational
  - Who, Why & How
  - Requires human analysis
  - SOC Operations
- Strategic
  - Difficult to generate
  - Geopolitical situations
  - Financially motivated
  - Educated decisions to mitigate risk



OSINT – Considerations

- Volume
  - Quantity VS Quality?
    - Vast amounts of IOCs VS sub-set of high fidelity, high confidence IOCs
  - Indicator status?
    - IOC Lifecycle – active VS inactive; process to age out?
    - Housekeeping – removal of inactive indicators?
- Collection & Ingestion
  - Format Standards – Structured VS Unstructured
    - STIX, JSON, CSV, email, etc
  - Frequency – hourly, daily
    - Full pull or delta of new indicators?
- Integration
  - Into existing security controls – format?
  - Active versus inactive/false positive?
  - Fidelity…

Exchange Platforms – Considerations



- Collaboration with Peers
  - Active sightings
  - Finished intelligence?
  - Forums or discussion boards?
- Manual export or automated feed?
  - Supported formats/standards – STIX, OpenIOC, etc
  - Full threat model constructs/associations?
- Global? Regional?
  - Language support in portal/platform?
- Risks Generic/cross vertical or Unique to Industry

Commercial Feeds – Considerations

- Relevant?
  - Relevancy to your organization – custom analysis service related to your organization
- Uniqueness of data?
  - Only paying for curation
  - Vendor differentiation
  - Feeds targeting specific classification of threat – C&C Domain, DGA, Malware Hash, etc
- Decay window or periodicity of data
  - Immediate activity or strategic focusing on associations and long term trends?
- Integration into environmental security controls
  - Automation, operationalization
  - Tracking ROI
- Existing Security Posture
  - Resources, budget, maturity, progam

Other Sources of Intel

- Tradecraft Intel Generation
  - Requires resources
  - Mature cyber programs
  - C.A.R.T.
    - Complete – enough information to make a decision?
    - Accurate – is the expanded information enough to make a *good* decision?
    - Relevant – is the intel related to me, my organization and the mission?
    - Timely – is the creation of the intel soon enough to make a decision?

Checkpoint

So far we've talked about:

- Different sources of threat data/intel
- Different types of threat data/intel
- Considerations and challenges
- Organization maturity

Deriving Value or Driving Value?

Definition:

- Derived - obtain something from (a specified source)

  "they derived comfort from this information"

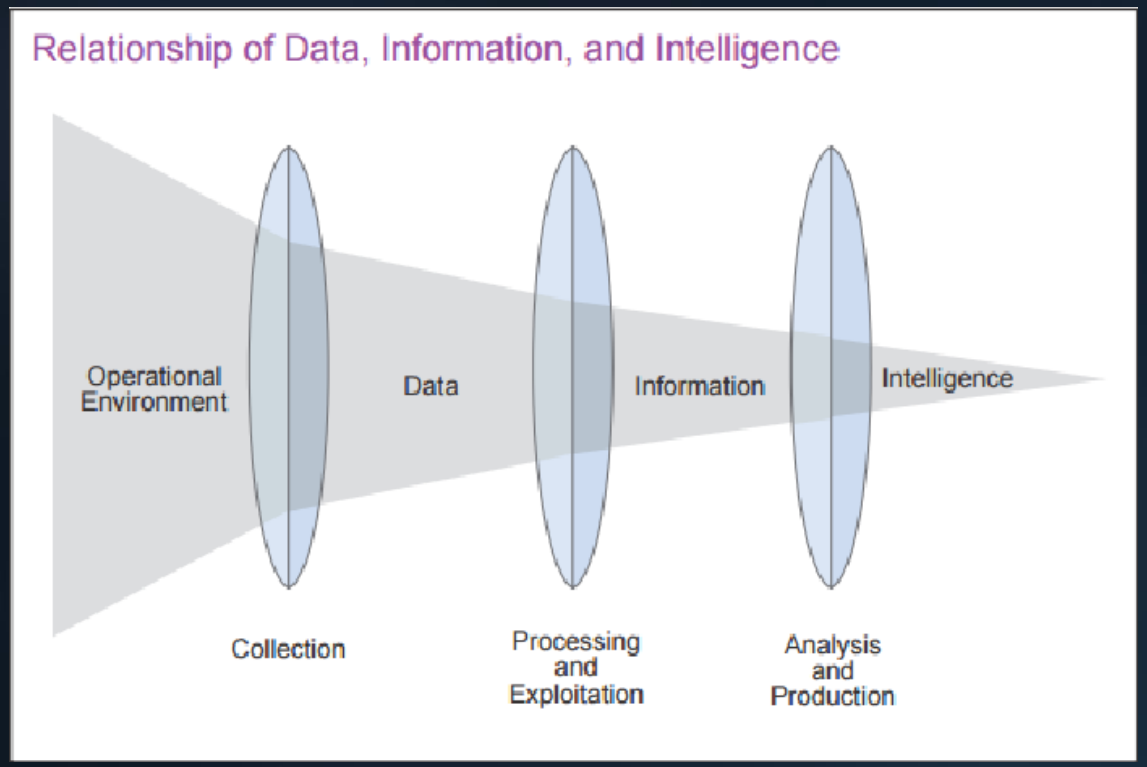
- Driving – communication force; exerting pressure

  “driving a process or a series of activities undertaken to achieve a goal”

Deriving Value from Threat Intelligence?

- Context
  - historical tracking (changes in iType classification over time), reporting sources, changes in confidence or severity
- Indicator Expansion / Enrichment
  - pDNS, pSSL, Whois, OpenPorts, VT, WOT
- Integrations
  - Destinations for tactical integration of ***select*** IOCs
- Threat Intelligence Management Platform

Driving Value from Threat Intelligence



- Workflow & Process
  - Collection, enrichment, attribution
    - Based on evidence & IOC characteristics
    - Tracking – long term, strategic motivations
    - SOCMINT, Deep & Dark Web
  - Finished Intelligence
    - Environmental context
      - Asset criticality
      - Current asset exposures
    - Relevant to the Organization
- Threat Intelligence Management Platform
  - Critical tool in the workflow
  - Key part of the process

How Do I Get There?

- Planning, Policy, Process
- Investment in staff & resources
  - Skills Gap Analysis
  - Workflow audit & assessment
- Team Training
  - Course curriculum from skills gap assessment
  - Role-based

How Do I Get There?

- Workflow
  - Audit/assessment of existing internal tools configuration
    - 3rd party consultant / Professional Services
    - Action plan to fill gaps in remediation process

- *Refine, Refine, Refine*

Summary

Is there value in threat intelligence?

Recipe:

- Threat Intelligence Management Platform
- Workflow and process
- Investment in staff

Thank-you

Q & A