Threat Intelligence for Dummies

Karen Scarfone

Scarfone Cybersecurity

Source Material

Threat Intelligence for Dummies ebook

- Co-authored with Steve Piper of CyberEdge Group
- Published by Wiley
- Sponsored by Norse
- Available for free download athttp://www.norsecorp.com/resources/threat-intelligence-for-dummies/index.htm (registration required)
- Today's talk is vendor agnostic

Agenda

- Understanding Threat Intelligence (TI)
- Gathering TI
- Scoring TI
- Using TI
  - To support incident response
  - To strengthen threat mitigation
- TI Purchasing Criteria

Basic Terminology

- Threat: the IT entity performing attacks
  - Person behind a threat is an attacker
- Attack: the malicious activity
- Threat indicator: data that indicates higher risk
  - IP address, URL, domain name
- Threat intelligence: threat indicators plus associated metadata
  - The result of analyzing potential threat indicators

Threat Indicator Metadata

- Timestamp: when the TI was collected
- Risk score: relative maliciousness of the TI
- Source: the origin of the TI
- Geolocation: the physical location of the host that presents the threat
- Threat category: anonymous proxy, bogon, bot, botnet, malware, passive DNS, etc.

Not all metadata are equally important

Why Does TI Matter?

- Incident prevention, detection, and response
  - Supported by next-generation firewalls, intrusion prevention systems, unified threat management appliances, web proxies, load balancers, and security information and event management (SIEM) systems
- Forensic investigations
- Risk assessment

TI Delivery

- Often think of machine-readable TI (TI feeds) as being the only form of TI
- Human-readable TI reports
- Console-based TI
- TI appliances

TI Data Gathering

- Primary locations
  - Existing data feeds
    - Often free
    - Concerns about data integrity
  - Internal customer networks
    - Can significantly speed threat detection
    - Can inadvertently expose sensitive information
  - External networks
    - Most comprehensive picture of threats
    - More costly than using other locations

Automated TI Sources

- Anonymous proxies
- Crawlers
- Free services
- Geolocation
- Honeypots
- Internet registries
- Internet Relay Chat (IRC)
- Peer-to-peer (P2P) networks
- And others…

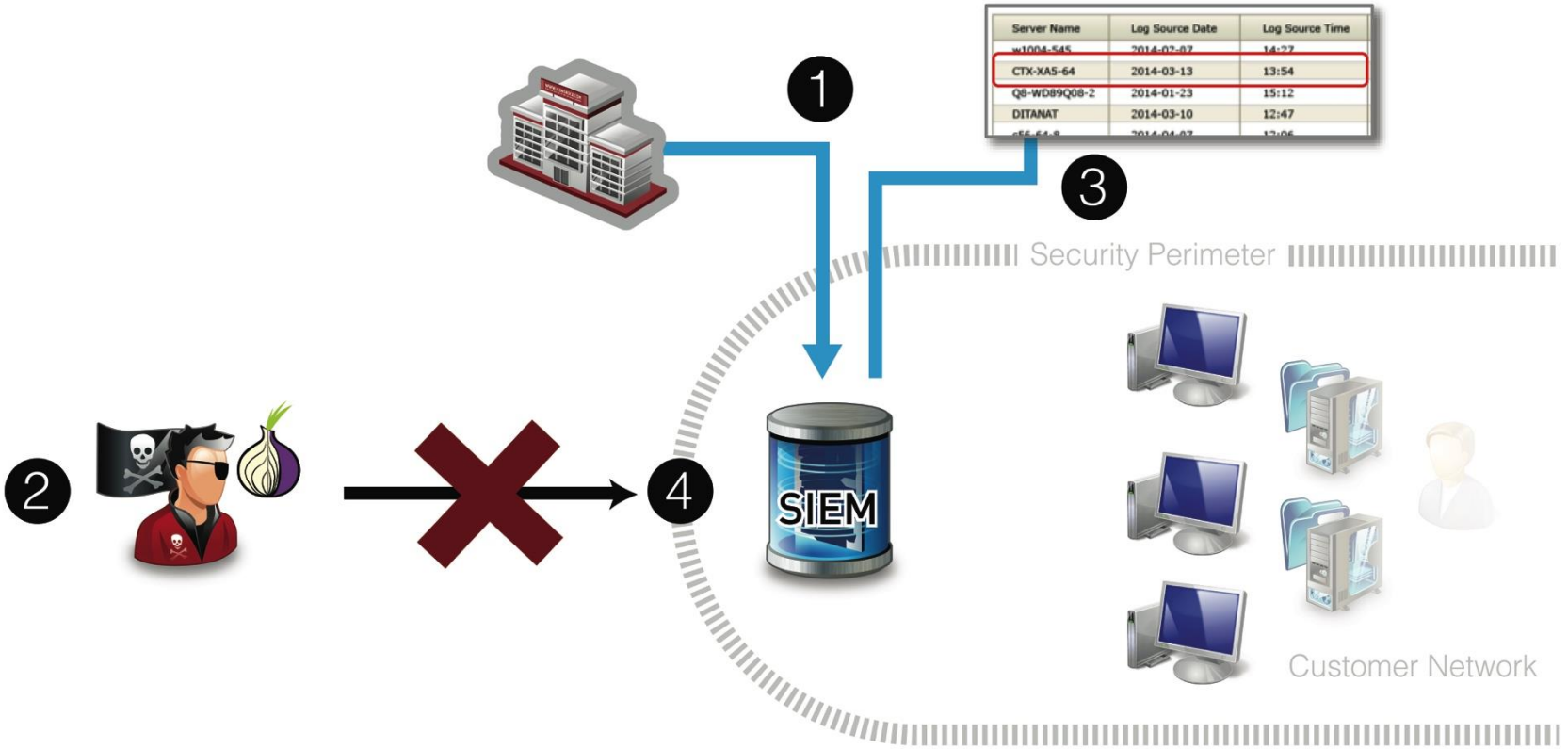
TI Scoring Basics

- Quality differs among TI sources and potentially within a single source
  - Confidence, timeliness
- Subjective nature of risk measurement
  - Dozens or hundreds of variables
- Score aging
- Score history
- Score threshold
  - Based on risk tolerance
  - Acceptable levels of false positives and negatives

Using TI in Incident Response

- Improves incident detection
  - Provides insights into the sources of observed events
  - Lists internal hosts that are compromised
  - Enables proactive attack detection and blocking by reusing information on current and recent attacks elsewhere
- Reduces workloads for existing devices
- Facilitates forensic investigations

Sample Architecture



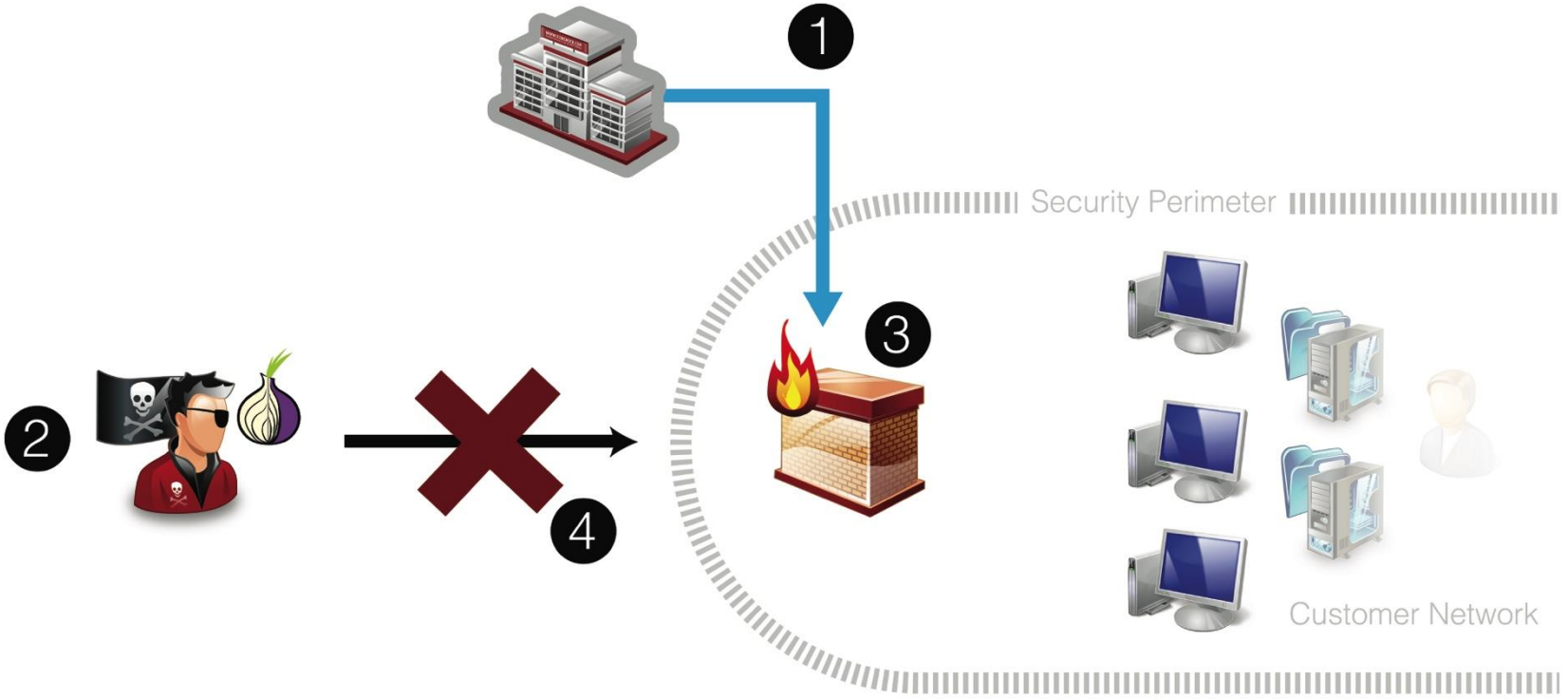
Using TI to Strengthen Threat Mitigation

- Stopping threats before they succeed
- Reducing impact of successful threats by detecting their compromises much faster
- Manual mitigation
  - Potentially minimizes false positives
  - Slow, easy to evade
- Automatic mitigation
  - IPS blocking network traffic
  - SIEM reconfiguring firewalls and IPSs

Threat Mitigation Strategies

- Blocking attacks
  - Community immunity
  - Anonymous proxy, bot, and botnet connection attempts
- Improving catch rates
  - How likely it is for your security controls to identify an attack in progress
- Stopping advanced attacks before compromise when possible
  - Can evade inclusion in TI feeds
  - Generally ineffective at stopping insider threats

Feeding TI into Existing Controls

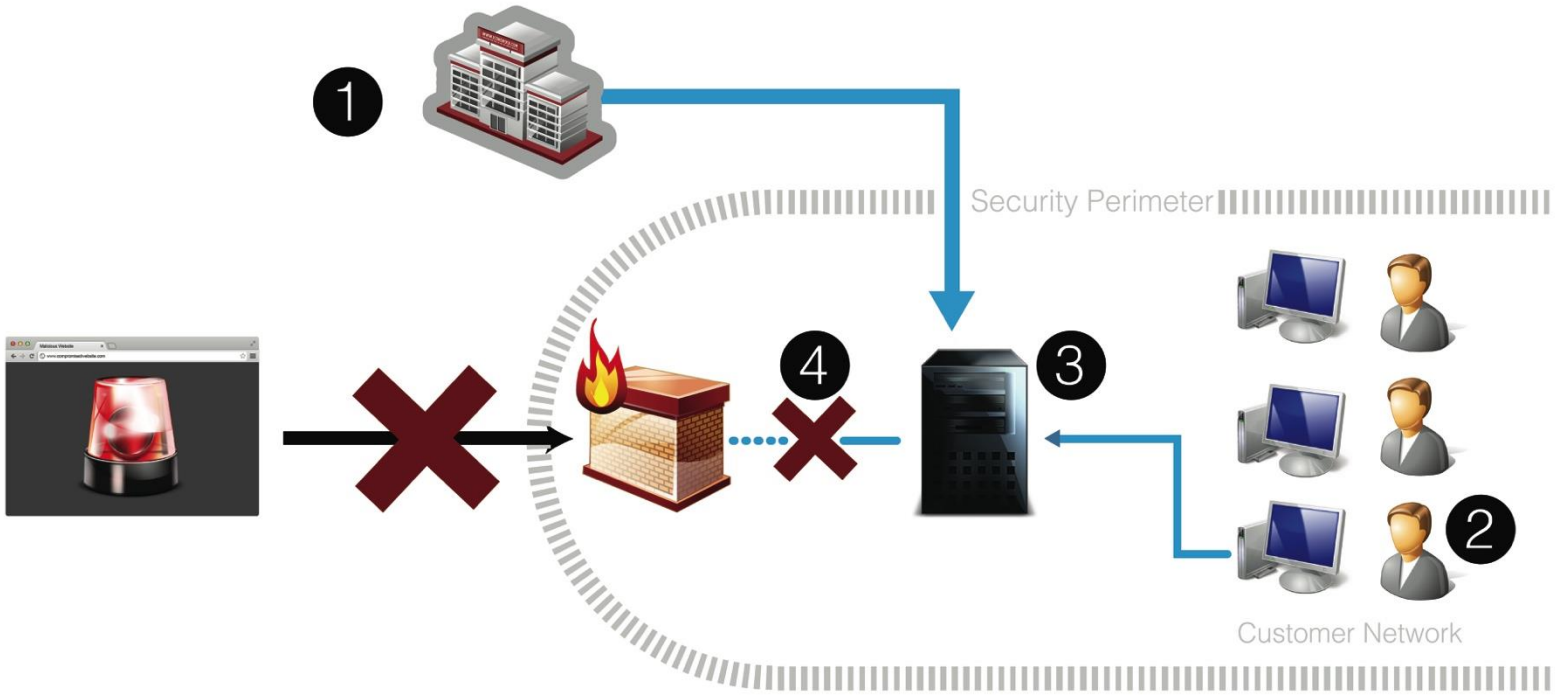


Firewall, unified threat management (UTM), or other device with firewall capabilities

Using TI with Existing Controls

- Pros
  - Block connection attempts and terminate existing connections
  - Reduce load on other security controls
- Cons
  - Not supported by all controls
  - Limited indicator processing and/or storage
  - Inability to keep up with frequent updates

Using a Dedicated TI Appliance



Using a Dedicated Appliance

- Pros
  - All the same pros as using an existing control
  - Reduces workload on existing controls
  - Designed to fully use the TI
- Cons
  - Cost

Ten Criteria for Evaluating TI Solutions

- Automation
- Integration and interoperability
- Frequency of updates
- Metadata richness
- Scoring sophistication
- Threat coverage
- Darknet visibility
- Geolocation accuracy
- Variety and number of sources
- Source quality

Recap

- Understanding Threat Intelligence (TI)
- Gathering TI
- Scoring TI
- Using TI
  - To support incident response
  - To strengthen threat mitigation
- TI Purchasing Criteria

Thank you!

Karen Scarfone

karen@scarfonecybersecurity.com

http://scarfonecybersecurity.com

https://www.linkedin.com/in/karenscarfone