Lesson 2

Explaining Threat Actors and Threat Intelligence

CompTIA

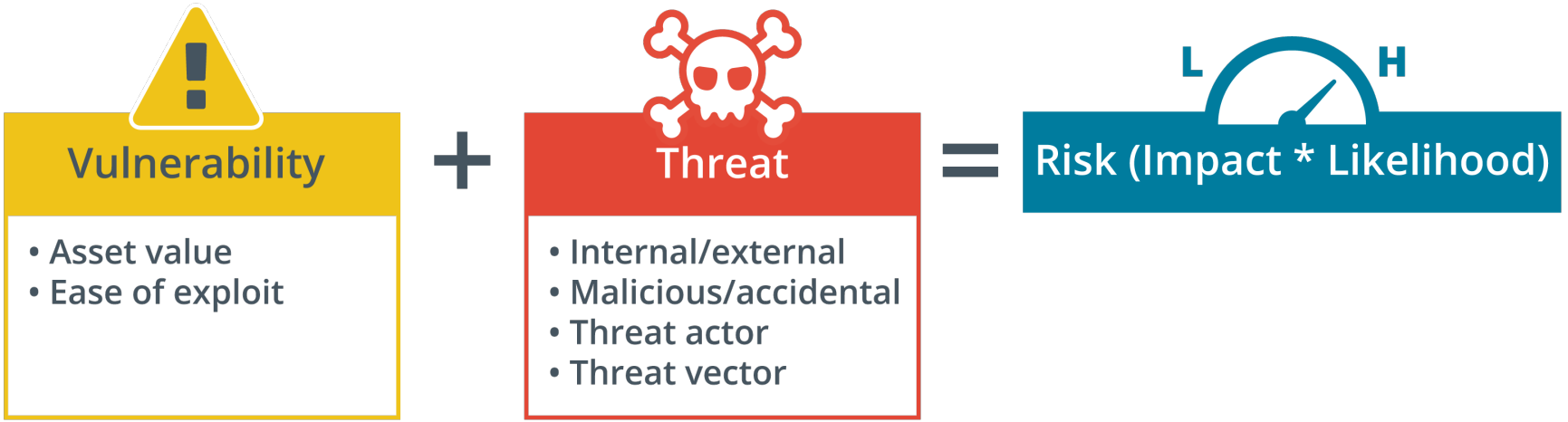
Topic 2A

Explain Threat Actor Types and Attack Vectors

Syllabus Objectives Covered

- 1.5 Explain different threat actors, vectors and intelligence sources

Vulnerability, Threat, and Risk



Attributes of Threat Actors

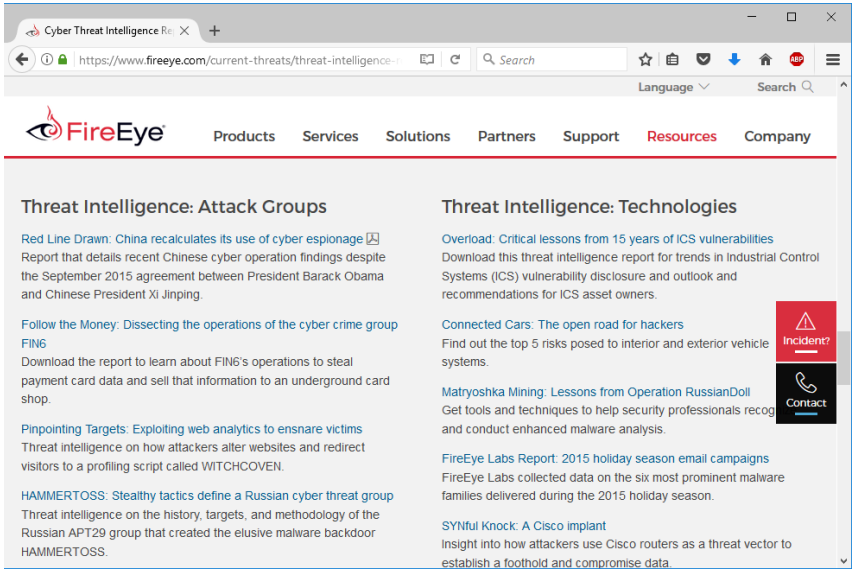
- Known threats versus adversary behaviors
- Internal/external
- Intent/motivation
  - Maliciously targeted versus opportunistic
  - Accidental/unintentional
- Level of sophistication
  - Resources/funding
  - Adversary capability levels

Hackers, Script Kiddies, and Hacktivists

- The “Lone Hacker”
  - White hats versus black hats versus gray hats
  - Authorized versus non-authorized versus semi-authorized
- Script kiddies
- Hacker teams and hacktivists

State Actors and Advanced Persistent Threats

- State-backed groups
  - Attached to military/secret services
  - Highly sophisticated
- Advanced Persistent Threat (APT)
- Espionage and strategic advantage
- Deniability
- False flag operations



Screenshot used with permission from fireeye.com.

Criminal Syndicates and Competitors

- Criminal syndicates
  - Operate across legal jurisdictions
  - Motivated by criminal profit
  - Can be very well resourced and funded
- Competitors
  - Cyber espionage
  - Combine with insider threat

Insider Threat Actors

- Malicious insider threat
  - Has or has had authorized access
  - Employees, contractors, partners
  - Sabotage, financial gain, business advantage
- Unintentional insider threat
  - Weak policies and procedures
  - Weak adherence to policies and procedures
  - Lack of training/security awareness
  - Shadow IT

Attack Surface and Vectors

- Attack surface
  - Points where an attacker can discover/exploit vulnerabilities in a network or application
- Vectors
  - Direct access
  - Removable media
  - Email
  - Remote and wireless
  - Supply chain
  - Web and social media
  - Cloud



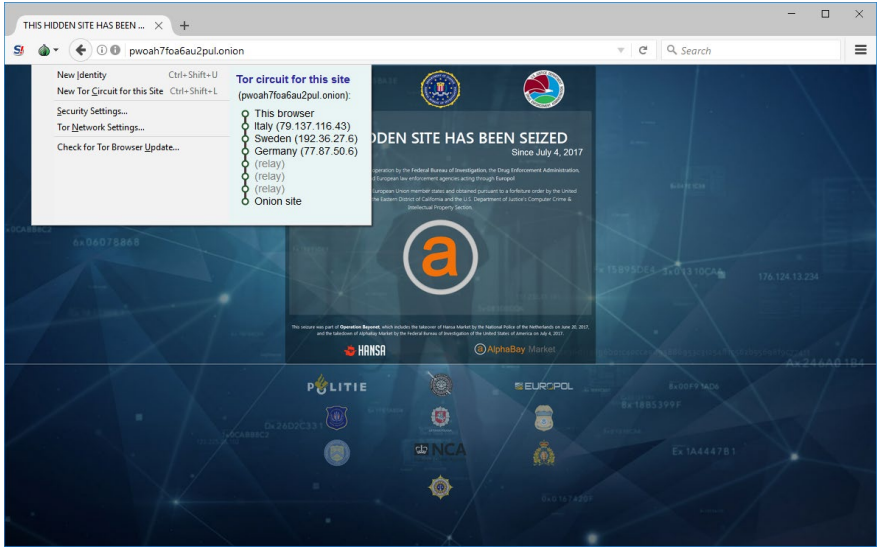
Topic 2B

Explain Threat Intelligence Sources

Syllabus Objectives Covered

- 1.5 Explain different threat actors, vectors and intelligence sources

Threat Research Sources



- Counterintelligence
- Tactics, techniques, and procedures (TTPs)
- Threat research sources
  - Academic research
  - Analysis of attacks on customer systems
  - Honeypots/honeynets
  - Dark nets and the dark web

Threat Intelligence Providers

- Narrative analysis and commentary
- Reputation/threat data feeds—cyber threat intelligence (CTI)
- Platforms and feeds
  - Closed/proprietary
  - Vendor websites
  - Public/private information sharing centers
  - Open source intelligence (OSINT) threat data sources
- OSINT as reconnaissance and monitoring

Other Threat Intelligence Research Sources

- Academic journals
- Conferences
- Request for Comments (RFC)
- Social media

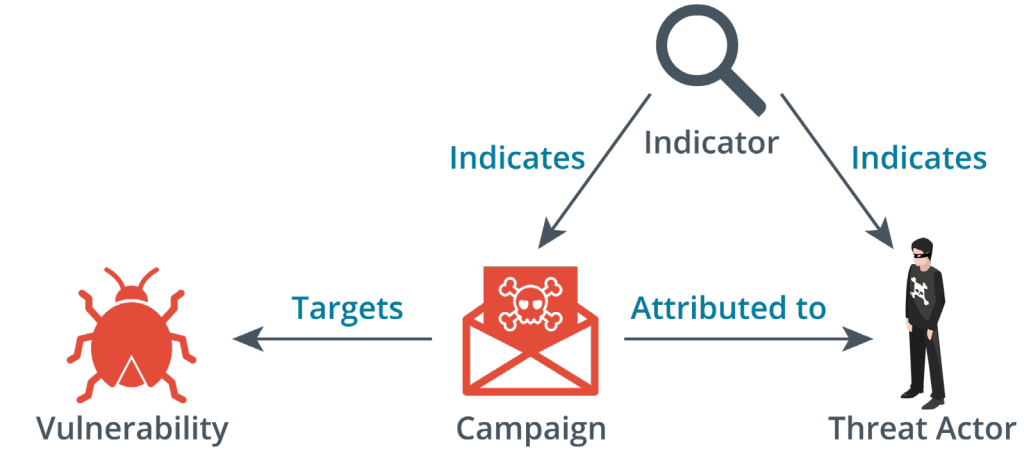
Tactics, Techniques, and Procedures and Indicators of Compromise

- Tactics, Techniques, and Procedures (TTPs)
  - Generalized statement of adversary behavior
  - Campaign strategy and approach (tactics)
  - Generalized attack vectors (techniques)
  - Specific intrusion tools and methods (procedures)
- Indicator of compromise (IoC)
  - Specific evidence of intrusion
  - Individual data points
  - Correlation of system and threat data
  - AI-backed analysis
  - Indicator of attack (IoA)



Threat Data Feeds

- Structured Threat Information exchange (STIX)
- Trusted Automated Exchange of Indicator Information (TAXII)
- Automated Indicator Sharing (AIS)
- Threat maps
- File/code repositories
- Vulnerability databases and feeds



Artificial Intelligence and Predictive Analysis

- Correlation between security intelligence/event monitoring and threat data
- Artificial intelligence (AI) and machine learning (ML)
  - Expert systems
  - Artificial neural networks (ANN)
    - Inputs, outputs, and feedback
    - Objectives and error states
- Predictive analysis
  - Threat forecasting
  - Monitor “chatter”

Lesson 2

Summary