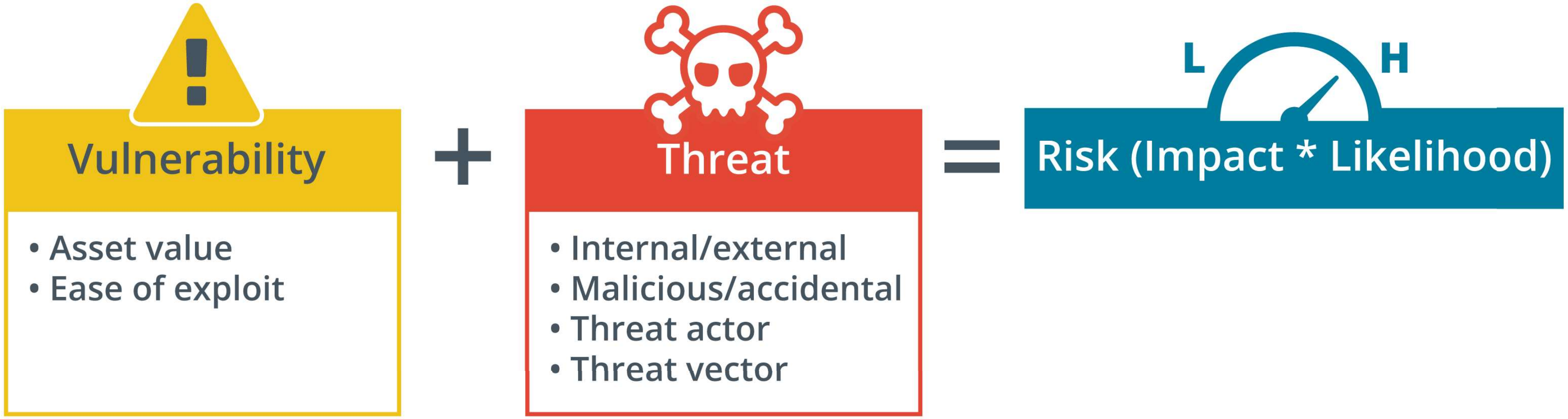
Vulnerability, Threat, and Risk



Vulnerability

- Asset value
- Ease of exploit

+

Threat

- Internal/external
- Malicious/accidental
- Threat actor
- Threat vector

=

Risk (Impact * Likelihood)

Attributes of Threat Actors

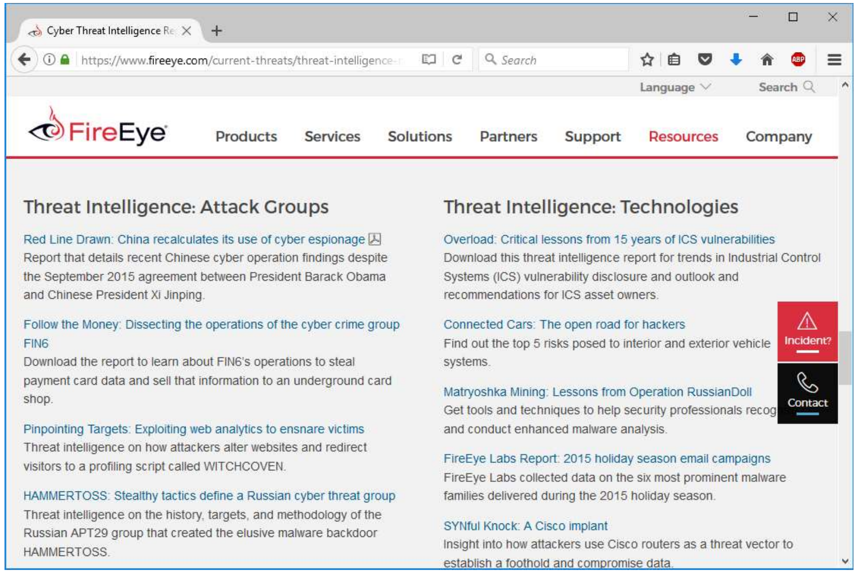
- Known threats versus adversary behaviors
- Internal/external
- Intent/motivation
  - Maliciously targeted versus opportunistic
  - Accidental/unintentional
- Level of sophistication
  - Resources/funding
  - Adversary capability levels

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



Threat Intelligence: Attack Groups

Red Line Drawn: China recalculates its use of cyber espionage
Report that details recent Chinese cyber operation findings despite the September 2015 agreement between President Barack Obama and Chinese President Xi Jinping.

Follow the Money: Dissecting the operations of the cyber crime group FIN6
Download the report to learn about FIN6's operations to steal payment card data and sell that information to an underground card shop.

Pinpointing Targets: Exploiting web analytics to ensnare victims
Threat intelligence on how attackers alter websites and redirect visitors to a profiling script called WITCHCOVEN.

HAMMERTOSS: Stealthy tactics define a Russian cyber threat group
Threat intelligence on the history, targets, and methodology of the Russian APT29 group that created the elusive malware backdoor HAMMERTOSS.

Threat Intelligence: Technologies

Overload: Critical lessons from 15 years of ICS vulnerabilities
Download this threat intelligence report for trends in Industrial Control Systems (ICS) vulnerability disclosure and outlook and recommendations for ICS asset owners.

Connected Cars: The open road for hackers
Find out the top 5 risks posed to interior and exterior vehicle systems.

Matryoshka Mining: Lessons from Operation RussianDoll
Get tools and techniques to help security professionals recog and conduct enhanced malware analysis.

FireEye Labs Report: 2015 holiday season email campaigns
FireEye Labs collected data on the six most prominent malware families delivered during the 2015 holiday season.

SYNful Knock: A Cisco implant
Insight into how attackers use Cisco routers as a threat vector to establish a foothold and compromise data.

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