Cyber Threat Intelligence Plan and Proposal For NetStore

Veeraiah Nannapaneni

University of San Diego

Spring 2019

What is Cyber Threat Intelligence (CTI)

"Any sort of threat intelligence is simply assessed information, and can only be understood in the context within which it is created and the proposed purpose of its use. The purpose is usually to increase awareness of defined situations and environments and to aid in decision-making, at either an operational, tactical or strategic level" (Ernst & Young. n.d).

Figure: (Nuspire. n.d)

Cyber Threat Intelligence Plan and Proposal

How do you use Cyber Threat Intelligence

CTI can be used in the following 5 steps.

Automatically consolidate all sources of cyber threat intelligence – internal and external

Context provides better understanding of the threat and what it means to your environment.

Prioritization based on the parameters you set is critical to ensure relevance.

Automatically applying curated threat data to your environment turns intelligence into better protection and mitigation.

CTI must be updated and enriched regularly in order to tune your threat library, stay focused on what matters and make better decisions (ThreatQuottient, n.d).

Cyber Threat Intelligence Plan and Proposal

What can Threat Intel do for NetStore

Threat intelligence can help NetStore gain knowledge of the menaces and maximize security before an undesired event occurs. Here are 6 actions that a CTI can help.

Prevent data loss

Monitor malicious IPs and domains to gather intelligence data.

Detect breaches

Deep packet inspection together with network monitoring allows security analysts to detect viruses, intrusion, and protocol non-compliance.

Incident response

Provide guidance in breach regarding its magnitude, and method of operations and help identify the compromised systems.

Threat analysis

Offers insights into the necessary defense mechanisms and other measures that may be required.

Data analysis

Helps discover information about the attacker's motive.

Threat intelligence sharing

Help organizations learn about other threats in the industry.

NetStore Assets that needs to be Protected

- Employees Personally Identifiable Information (**PII**)
- **Intellectual property** such as source code, engineering designs, software programs.
- **Confidential business information** such as business plans, customer lists, competitive bid information, and trade secret.
- **Insider** information on financial results, mergers, and other news that affect stock prices.
- **Credentials and IT systems information** such as login credentials, suppliers and service providers, and other third parties with access to your systems.
    - Some of the most damaging data breaches in recent years started when user IDs and passwords were stolen from third parties (Friedman, n.d).

Cyber Threat Intelligence Plan and Proposal

Five Threat Actors Targeting NetStore

It is important to understand the threats, motives and capabilities of threat actors so we can develop counterintelligence.

- **Cybercriminals**
- **Competitors and Cyber Espionage Agents**
- **Insiders**
- **Opportunistic**
- **Internal User Error**

Threats, Motives and Capabilities of Cybercriminals

Cybercriminals

Image Credit: http://vpnexpress.net

Threat:

- Credit card and Financial account data
- Personally Identifiable information
- Credentials

Motive:

- Financial Gain

Capabilities:

- Highly Technical
- Well-Founded
- Large Numbers

Threats, Motives and Capabilities of Competitors and Cyber Espionage Agents

Competitors and Cyber Espionage Agents

Image Credit: http://royaldutchshellplc.com

Threat:

- Intellectual Property
- Business and Financial information
- Credentials

Motive:

- Espionage and Ideology
- Competitive advantage

Capabilities:

- Highly Technical
- Well-Founded
- Very Patient
- Persistent
- High Intensity

Threats, Motives and Capabilities of Insiders

Insiders

Image Credit: https://cdn.meritalk.com

Threat:

- Intellectual Property (IP)
- Business and Financial Records
- Credentials
- Trade Secrets

Motive:

- Personal Financial Gain
- Revenge

Capabilities:

- Insider knowledge
- Aware of Policies Procedures and Technology

Threats, Motives and Capabilities of Opportunistic

Opportunistic

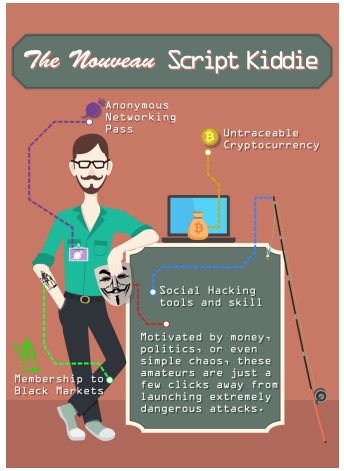

Image Credit: blog.fortinet.com

Threat:

- DDoS
- Credential theft
- Credit card and financial data

Motive:

- Desire for Notoriety
- Profit
- Fun, Thrills, or skill refinement

Capabilities:

- Limited Technical Knowledge
- Use off-the-shelf exploit tools
- Novices or amateurs (Welgan, 2017)

Threats, Motives and Capabilities of Internal User Error

Internal User Error

Image Credit: 20103740.blogspot.com

Threat:

- Misconfiguration
- Poor patch management
- Use of default usernames and passwords or easy-to-guess passwords

Motive:

- Unintentional

Capabilities:

- Lack of Product Knowledge
- Lack of Training

Threat Actors Potential Attack Methods

There are several methods threat actors will use to gain access to the NetStore

Cybercriminals

Attack Methods:

- Phishing
- Social Engineering
- Brute Force and
- Botnets

Competitors and Cyber Espionage Agents

Attack Methods:

- Phishing
- Social engineering
- Brute Force
- Botnets and
- Credential Escalation

Insiders

Attack Methods:

- Credential escalation
- Knowledge of policies, procedures and technology
- They are also aware of vulnerabilities

Opportunistic

Attack Methods:

- Use of pre-build hacking tools by amateur criminals
- Professional hacking tools, vulnerabilities exploitation

Internal User Error

Attack Methods:

- Misconfigurations
- Unintentional elevated credentials (Irwin, 2014)

Cyber Threat Intelligence Plan and Proposal

Risk Reduction Plan

Recommendation mainly focuses on educating employee's about cybersecurity to create an army of defenders within the company along with implementing End-Point protection, Cyber Threat Intelligence Platform, Incident Reponses Plan, and proper Patch management.

Patch Management

- Implement SolarWinds Patch Manager Software
- Run Monthly asset discovery
- Test all patch's in a sandbox before applying them companywide

Cyber Threat Intelligence Platform

- Implement FireEye iSIGHT Threat Intelligence

End-Point Protection

- Protect End-Point devices using security products like McAfee Endpoint protection

Incident Response Plan

- Utilize NIST computer incident security handling guide to develop the plan
- Conduct mock drills

Training

- Proper training of the latest threats and attacks further reduce the organization's cyber risk
- Periodic surveys to be conducted to learn about any gaps within the current security practices and update the security training programs

Cyber Threat Intelligence Plan and Proposal

References:

Davis, J. (2018, November 1). NetApp's CISO, Phillip J. Ferraro shares his thoughts on the role of the CISO in complex organizations. Retrieved from https://governmenttechnologyinsider.com/netapps-ciso-phillip-j-ferraro-shares-his-thoughts-on-the-role-of-the-ciso-in-complex-organizations/#.XGjm8y2ZPUI

Ernst & Young. (n.d). How do you find the criminals before they commit the cybercrime? Retrieved from https://www.ey.com/Publication/vwLUAssets/EY-how-do-you-find-the-criminal-before-they-commit-the-cybercrime/%24FILE/EY-how-do-you-find-the-criminal-before-they-commit-the-cybercrime.pdf

Friedman, J., Bouchard, M. (n.d.). Definitive Guide to Cyber Threat Intelligence. Retrieved from https://cryptome.org/2015/09/cti-guide.pdf

Giandomenico, A. (2017, June 27). You're your Enemy: Understanding Threat Actors. Retrieved from https://www.csoonline.com/article/3203804/security/know-your-enemy-understanding-threat-actors.html

Insider Threat. (2017, December). In Software Engineering Institute. Retrieved from https://www.sei.cmu.edu/research-capabilities/all-work/display.cfm?customel_datapageid_4050=21232

Irwin, S. (2014, September 8). Creating a Threat Profile for Your Organization. Retrieved from https://www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492

Cyber Threat Intelligence Plan and Proposal

References:

Nuspire. (n.d). Threat Intelligence. Retrieved from https://www.nuspire.com/technologies/threat-intelligence/

ThreatConnect. (n.d). What is Threat Intelligence? Retrieved from https://threatconnect.com/threat-intelligence/

Threat Intelligence Subscriptions. (n.d). Retrieved March 10, 2019, from https://www.fireeye.com/solutions/cyber-threat-intelligence-subscriptions.html

ThreatQuottient. (n.d). 5 Steps to Mastering the Use of Cyber Threat Intelligence. Retrieved from https://www.threatq.com/cyber-threat-intelligence-five-steps/

UNLOQ. (2017, January 19). What is Cyber Threat Intelligence, And Why You Need It. Retrieved from https://blog.unloq.io/what-is-cyber-threat-intelligence-and-why-you-need-it-fd33e24954da

Warlock. (2013, September 11). OSINT (Open-Source Intelligence) https://resources.infosecinstitute.com/osint-open-source-intelligence/#gref

Welgan, J. (2017, May 02). Threat Actor Profiles: Script Kiddies. Retried from https://www.cybervista.net/threat-actor-profiles-script-kiddies/