CYBER THREAT
In the last several years, we’ve seen a disturbing trend attackers are innovating much faster than defenders are.

Cyber threat intelligence is to provide the ability to recognize and act upon indicators of attack and compromise scenarios in a timely manner. While bits of information about attacks abound, cyber threat intelligence (CTI) recognizes indicators of attacks as they progress, in essence putting these pieces together with shared knowledge about attack methods and processes.
GOALS

A robust CTI program can shed light on a multitude of strategic business concerns and risks, while providing highly technical actions, countermeasures, and metrics to the cyber security program at large. It can potentially provide answers to questions like:

<table>
<thead>
<tr>
<th>What are the most significant threats facing our organization?</th>
<th>What assets are (potentially) being targeted, and by whom?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>How can our organization protect against these cyber threats?</td>
<td>How can our organization use intelligence to augment and improve our security and business operations</td>
</tr>
</tbody>
</table>
REAL TIME INTELLIGENCE

• Availability of real-time intelligence can help organizations prevent and contain the impact of cyber attacks.

• Cyber threat intelligence becomes the foundation on which a firm builds its secure, vigilant and resilient capabilities.
Tactical intelligence:

- Tactical cyber intelligence is information from direct adversary action inside your systems or from other sources that have the potential to immediately influence your tactical decisions.
- Provides technical intelligence that can be rapidly integrated within an organization’s native sensor and first line of defense capabilities.
- Typically derived from real time monitoring of systems.

Operational Cyber Intelligence:

- Operational cyber intelligence is data that can inform day-to-day decision-making, resource allocation and task prioritization.
- Trend analysis, showing the technical direction of threat actors, indications that an adversary has selected a particular target, and revelations of malicious tactics, techniques and procedures.
CTI Architecture

External cyber threat intelligence feeds:
- Commercial feeds
- Law enforcement
- Industry associations
- Security researchers
- Underground forums
- Hash databases
- GEOIP data

Internal threat intelligence feeds:
- Fraud investigations
- Security event data
- Abuse mailbox info
- Vulnerability data
- Sandboxes
- Human intelligence

Proactive surveillance:
- Honeynets
- Malware Forensics
- Brand monitoring
- P2P monitoring
- DNS monitoring
- Watchlist monitoring

Risk assessment process:
- Risk acceptance process
- Risk mitigation
- Risk remediation

Urgent security control updates

Cyber threat intelligence collection, research, and analysis process

Threat intelligence reporting:
- Line of business teams
- Security, fraud, and operational risk teams
- Third parties, subsidiaries

Infrastructure logs
Application logs
Technology configuration data
Security information and event management fulfills two main objectives:

1. detecting in (near) real-time security incidents.
2. efficiently managing logs.

SIEM collects information (e.g., logs, events, flows) from various devices on a network, correlates and analyzes the data to detect incidents and abnormal patterns of activity, and, finally, stores the information for later use (reporting, behavior profiling, etc.).

SIEM helps in

- Discover internal/external threats.
- Monitor (privileged) user activity and access to resources.
- Provide compliance reporting.
- Support incident response.
Who will be benefited in Financial Service

- Banks: including commercial banks, investment banks and central banks
- Non-bank financial institutions: asset managers, insurance companies, finance and loan companies, mutual funds
- Other financial services: credit card companies, payment service providers, investment funds.
- Markets: stock markets, debt markets, derivatives markets, commodities markets, foreign exchange markets
- Financial markets infrastructure: payment systems, central securities depositories, trade repositories, messaging systems.
USE CASES

- Corporate Data Theft
- Fraud
- Insider Threat
- Emerging Malware
- The Role of the Deep & Dark Web
Recommendation for Financial Services Organization

- Use Threat Intelligence to Take a Proactive Approach to your Security Program.
- Leverage Automation Tools to Sift Through the Noise
- Track Threats Specific to Your Organization
- Evaluate Risks – Not Just Compliance – as a Way to Increase Security
- Never Underestimate the Power of Cyber Security Training
THANK YOU

For More Information Please Visit our Website

www.infopercept.com