arcX Cyber Threat Intelligence 101 part 2

Day 15/365

How do organizations use CTI?

CTI in an organizations is all about adding context and understanding where you sit in the "threat landscape"

Cybersec is not just CTI

- SOC
- IR
- Patch and vulnerability management
- Human resources - ?

CThreat is ever-evolving and increasing levels of threat (extinction level events, this is new)

due to this, CSEC needs to move from reactive to proactive (still defensive)

The corporate network is becoming larger and more diffuse

diffuse - laptops smartphones and tablets , more difficult to monitor

---

CTI in practice within an organisation

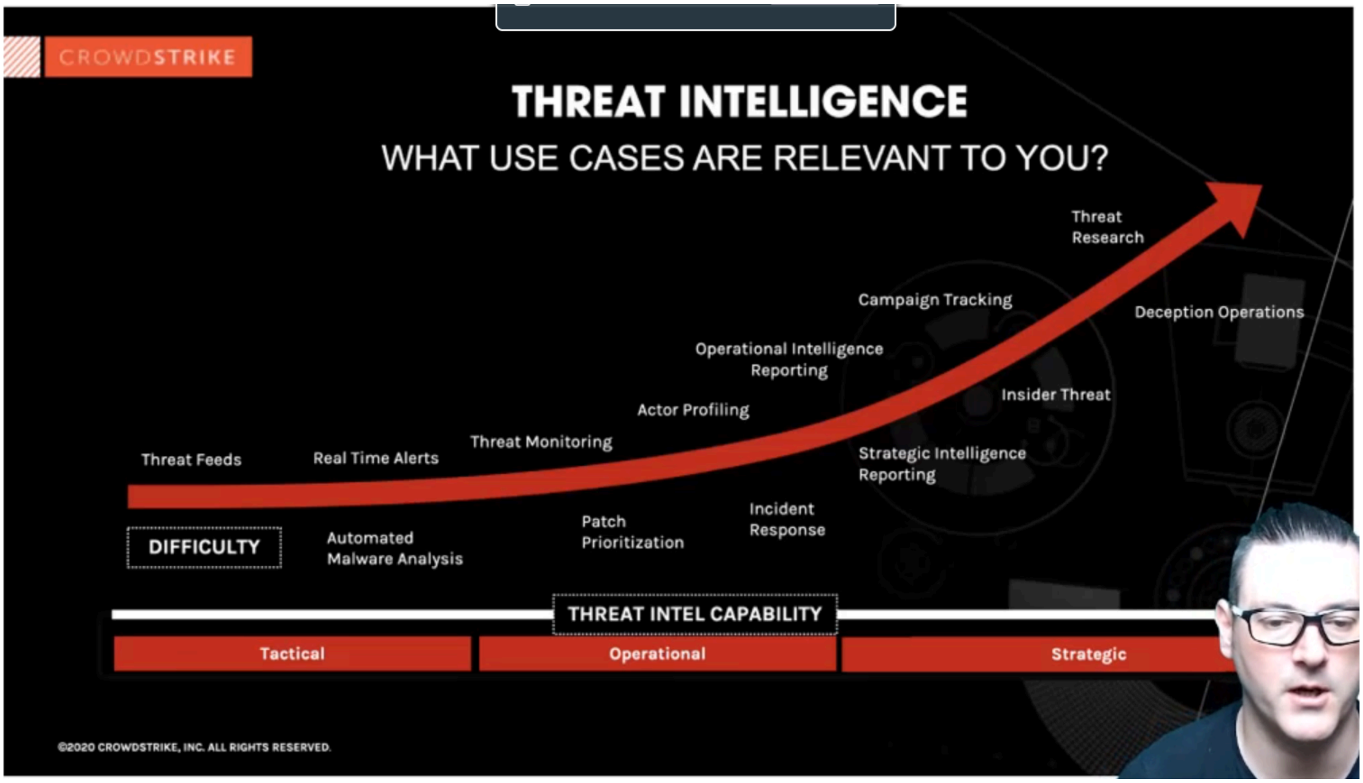
- Security Operations Centre (SOC) - feeds into tangible security such as firewalls i.e. indicators of compromise (IOC)
- Incident Response - attributes an attack to a defined group or individual
- Patch and Vulnerability Management - prioritisation
- Human Resources - policy around areas like crisis management.
- Business Risk Management - cyber has an impact on all business areas

---

CTI can be used in a huge range of business processes

- Strategic Level - the 'board' and senior decision makers.
- Operational Level - SOC operations and security controls application
- Tactical Level - threat hunting within log files.

Actionability changes quite significantly at every level



CROWDSTRIKE

THREAT INTELLIGENCE

WHAT USE CASES ARE RELEVANT TO YOU?

Threat Feeds

Real Time Alerts

Threat Monitoring

Actor Profiling

Operational Intelligence Reporting

Campaign Tracking

Threat Research

Deception Operations

Insider Threat

Strategic Intelligence Reporting

Incident Response

Patch Prioritization

Automated Malware Analysis

DIFFICULTY

THREAT INTEL CAPABILITY

Tactical

Operational

Strategic

©2020 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

how organizations use CTI

Cyber threat intelligence is an area of cyber security that focuses on the collection and analysis of information about current and potential attacks that threaten the safety of an organisation or its assets.

Through the implementation of this tactic, organisations can take proactive steps to ensure that their systems are secure. By using cyber threat intelligence and analysis, data breaches and other issues can potentially be prevented, saving your organisation the significant financial costs of having to set any incident response plans in motion.

The purpose of cyber threat intelligence is to give organisations an in-depth understanding of the threats that pose the greatest risk to their infrastructure and devise a plan to protect their day-to-day business. CTI Analysts strive to provide as much actionable intelligence as possible.

Through the process of analysis, you can develop an understanding around why a threat actor may attack your systems to begin with. Knowing the opposition’s motive can shed light onto what areas of your systems could be the most vulnerable.

To round off this recap we want to highlight some of the key reasons that organisations use cyber threat intelligence:

- Identify and assess potential threats to their networks and systems.
- Enhance their overall security posture by proactively taking measures to prevent attacks.
- Improve incident response efforts by having up-to-date information about known threats.
- Prioritise resources for the mitigation of high-risk vulnerabilities.
- Monitor external sources for signs of a potential breach or attack.

- Stay informed about the tactics, techniques, and procedures used by malicious actors.

The role of a CTI Analyst

- Not just a lone gun, working with other professionals that might have no idea about what you're talking about (and viceversa)

You provide insight into the threat
There are different ways of how you provide that insight

Recommended book: Psychology of Intelligence Analysis by Richards J. Heuer
The work explains the mix between art craft and science inside intelligence analysis

Cyber threat intelligence analysts gather data to track, evaluate, and report on threats that could have an impact on an organisation. They do this by combining contextual knowledge of the whole threat landscape with analytical abilities.

Analysts combine a variety of sources, including private data collections and open source intelligence (OSINT) evaluation, to produce a complete picture of an organisation's risk posture that informs the steps the business takes to mitigate these risks.

They create short-term and long-term evaluations to help security teams better understand the threats they face and what they can do to prevent attacks and breaches in the future.

The roles and responsibilities of a CTI Analyst typically include:

- Identifying organisational intelligence requirements
- Collecting relevant data and conducting all-source analysis to inform decision making process
- Identifying, monitoring, and assessing potential threats or weaknesses
- Validating that security qualifications and requirements are met
- Creating reports that highlight key findings for security teams and other members of the organization
- Presenting findings to other teams and proposing counteractions to mitigate threats