Introduction to Threat Intelligence

BYU CSA

QUINCY TAYLOR
AARON ANDERSON

LET'S TAKE A STEP BACK:

What is Cyber Threat Intelligence?

Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors.

HTTPS://WWW.CROWDSTRIKE.COM/CYBERSECURITY-101/THREAT-INTELLIGENCE/

LET'S TAKE A STEP BACK:

What is Cyber Threat Intelligence?

Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors.

Needed by an organization or group for security. Required for prolem solving or decision making.

HTTPS://WWW.CROWDSTRIKE.COM/CYBERSECURITY-101/THREAT-INTELLIGENCE/

LET'S TAKE A STEP BACK:

What is Cyber Threat Intelligence?

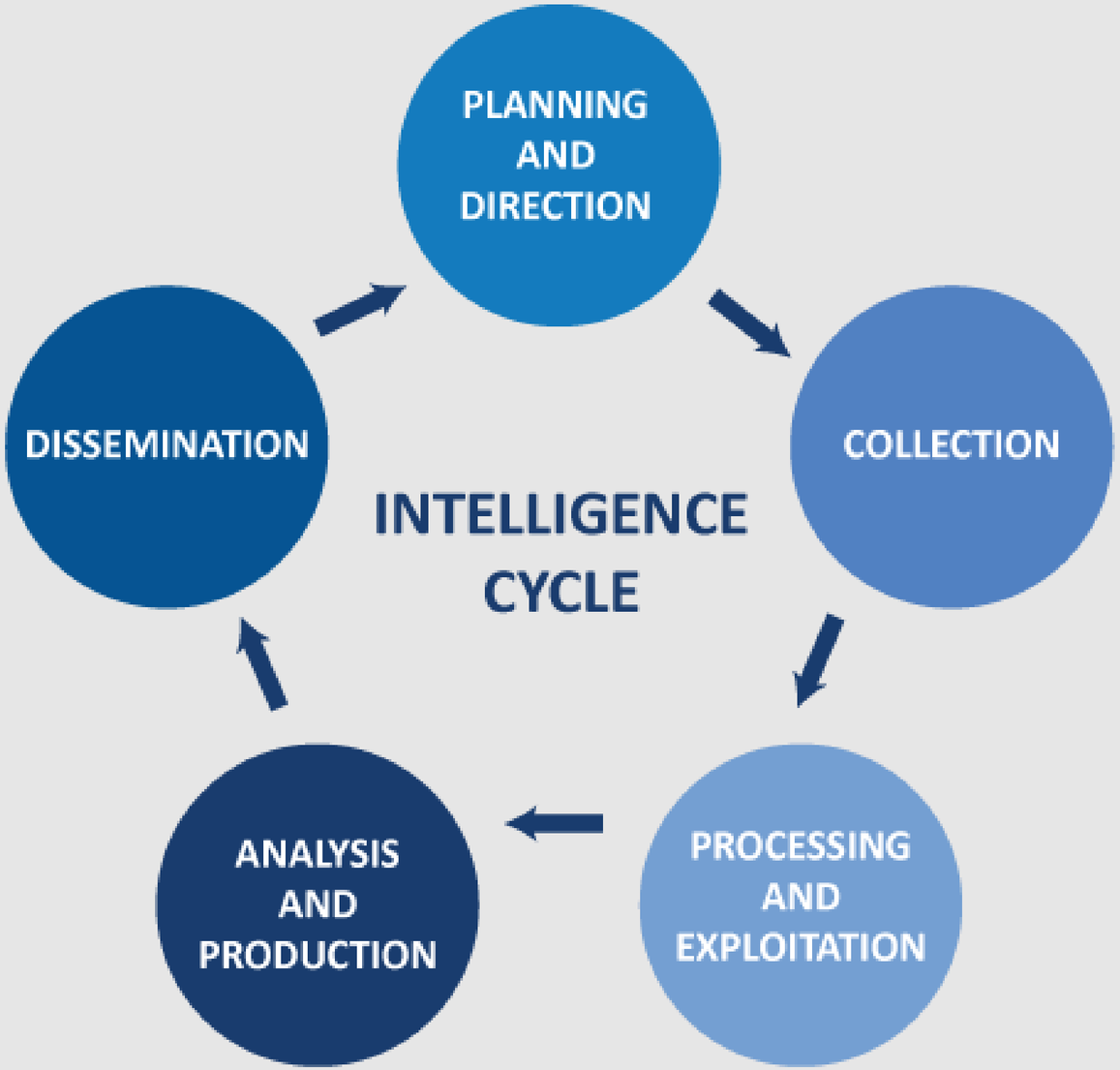
Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors.

Needed by an organization or group for security. Required for prolem solving or decision making.

Intelligence = result and process

HTTPS://WWW.CROWDSTRIKE.COM/CYBERSECURITY-101/THREAT-INTELLIGENCE/

The Cycle of Cyber Threat Intelligence



Where is Threat Intelligence in an Organization?

Security Operation Center - support, alert, triage, vulnerability management

Incident Response Support - facilitate information sharing

Strategy and Management - business decision and resource prioritization

Intelligence Planning

01.

Intelligence Requirements

- Objectives or questions from security team
- Leverage pain points in organization
- NO USELESS INTELLIGENCE
- Strategic, Operational, and Tactical considerations

Intelligence Planning

01.

Intelligence Requirements

- Objectives or questions from security team
- Leverage pain points in organization
- NO USELESS INTELLIGENCE
- Strategic, Operational, and Tactical considerations

02.

Threat Modeling

- Know what you have and what the adversaries want
- Know yourself - IP, Financial data, public assets
- Know the adversary - What do they eat?

Intelligence Planning

01.

Intelligence Requirements

- Objectives or questions from security team
- Leverage pain points in organization
- NO USELESS INTELLIGENCE
- Strategic, Operational, and Tactical considerations

02.

Threat Modeling

- Know what you have and what the adversaries want
- Know yourself - IP, Financial data, public assets
- Know the adversary - What do they eat?

03.

Collection Management Framework

- Where do we get data?
- How is it processed?
- What requirements can we fulfill?

A Sample External Collection Management Framework on Malware Data

	First seen date	Last seen date	IPs	Domains	RDNS	Historical Whois	current whois	ASN	New FQND	URL	MD5	SHA1	SHA256	SSDEEP
Virus Total	X	X	X	X						X	X	X	X	
Facebook threat exchange			X	X										
Malware domain list			X	X	X		X	X		X				
support.clean-mx.de			X	X				X		X				
malshare.com											X	X	X	X
malc0de.com			X	X				X		X	X			
zeustracker.abuse.ch		X	X	X				X		X				
vxvault			X	X						X	X			
malware.lu														
virusshare														
Malwr				X							X	X		
DeepViz	X	X	X	X				X	X	X	X	X	X	
openbl_1d OR Openbl_7d														

What is a Threat?

01.

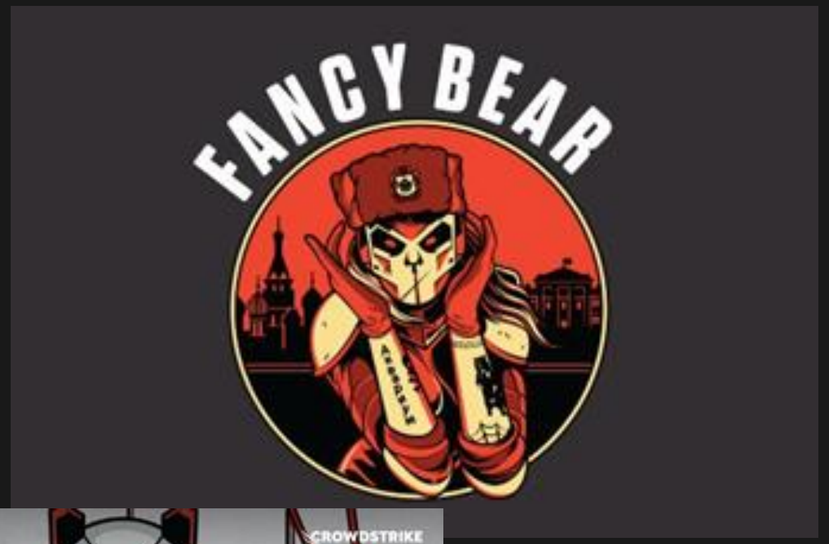
Individual or group with hostile intent, capability, and opportunity

02.

Advanced Persistant Threat (APT)

- typically well-funded, experienced teams of cybercriminals that target high-value organizations.
- a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time.

HTTPS://WWW.CROWDSTRIKE.COM/CYBERSECURITY-101/ADVANCED-PERSISTENT-THREAT-APT/K



CrowdStrike ~ 150 adversaries

“BEAR” refers to Russia, “CHOLLIMA” to North Korea, “PANDA” to China and “KITTEN” to Iran. “SPIDER” is used for eCrime that’s not state-sponsored.

WHY ANALYZE MITIGATED INCIDENTS?