RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **AIR-F05**

Through the Eyes of the Adversary: How to Build a Threat Intel Program

Jason Rivera

Director: Threat Advisory Group, Global
CrowdStrike / Threat Intelligence
@Jason_JHR

Scott Jarkoff

Director: Threat Advisory Group, APJ & EMEA
CrowdStrike / Threat Intelligence
@jark

AGENDA

- **SECTION 1:** Understanding Conflict & the Purpose of Threat Intelligence
- **SECTION 2:** Perceiving Threat Intelligence Through the Eyes of the Adversary
- **SECTION 3:** Threat Intelligence Capability Areas
- **SECTION 4:** Serving Stakeholders & Forming the Team
- **SECTION 5:** Examples of how to Operationalize Threat Intelligence

Section 1: Understanding Conflict & the Purpose of Threat Intelligence

The purpose of threat intelligence is to understand the conflicts in which we are engaged.

In general, there are three types of conflicts:

SECURITY

ECONOMIC

IDEOLOGICAL

SECURITY

ECONOMIC

IDEOLOGICAL

The nature of these conflicts fundamentally divides us into two opposing sides: ourselves and the adversary

OURSELVES

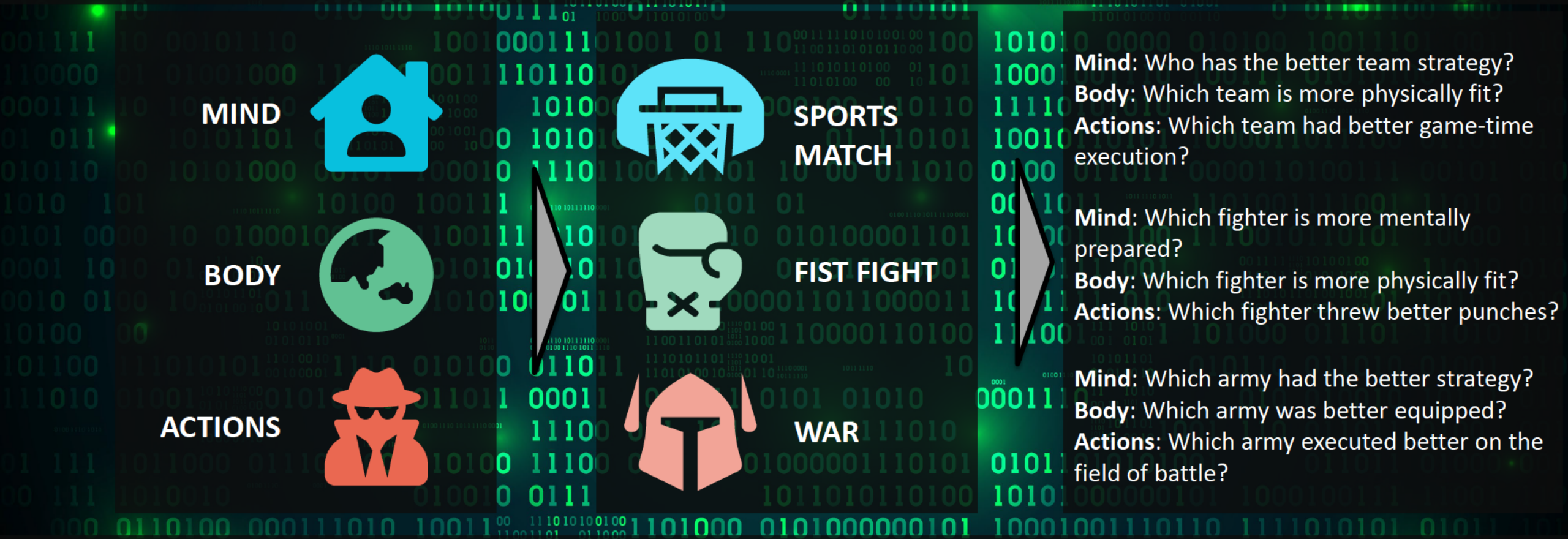
ADVERSARY

CROWDSTRIKE

We leverage threat intelligence to understand the conflicts between ourselves and the adversary, and to do this, we must understand the problem through the eyes of the adversary.

Section 2: Perceiving Threat Intelligence Through the Eyes of the Adversary

All conflicts between ourselves and the adversary can be visualized as a function of three components:



You will notice that in all conflicts, both friendly and non-friendly, the same three components still apply

Now let's apply a cyber lens to this concept

OURSELVES

ADVERSARY

STRATEGIC (Mind)

What industry am I in and what are my business critical strategic assets?

INDUSTRY ASSETS

What adversaries are motivated to target industry and how might they do so?

MOTIVE INTENT

OPERATIONAL (Body)

How will the adversary exploit my people, processes, & technologies?

PEOPLE PROCESS TECHNOLOGY

What capabilities will the adversary use against me and what infrastructure will these capabilities come from?

CAPABILITY INFRASTRUCTURE

TACTICAL (Actions)

How will the adversary gain access to my organization across the digital, physical, and psychological access vectors?

DIGITAL PHYSICAL PSYCHOLOGICAL

What tactics, techniques, & procedures (TTPs) will the adversary leverage to gain access to my organization?

TTPs

The goal of threat intelligence is to obtain an understanding of the above elements of conflict

Let’s dissect that exact information we want to understand about the adversary

ADVERSARY

EXAMPLES

STRATEGIC (Mind)

MOTIVE

INTENT

Ideological
Economic
Security
MOTIVE

Extortion
Destructive
Espionage
INTENT

OPERATIONAL (Body)

CAPABILITY

INFRASTRUCTURE

Malware
DDoS
Social Engineering
CAPABILITY

Malware-as-a-Service
Hostile IP / VPN / Proxies
Botnets / C2 / Spam
INFRASTRUCTURE

TACTICAL (Actions)

TTPs

Physical Device Compromise
Supply Chain
Phishing

Lateral Movement
Strategic Web Compromise
Vulnerability Compromise

TTPs

We want to be able to dissect the specific components of our adversary & communicate that information to stakeholders

Section 3: Threat Intelligence Capability Areas

RSAConference2020 APJ
A Virtual Learning Experience

There are three fundamental spaces in which all conflicts occur:

OUR SPACE

CONTESTED SPACE

ADVERSARY SPACE

SPORTS

CHESS

WAR

SPORTS	CHESS	WAR
OUR SPACE: Our goal CONTESTED SPACE: The field ADVERSARY SPACE: Their goal	OUR SPACE: Our king CONTESTED SPACE: The chess board ADVERSARY SPACE: Their king	OUR SPACE: Our country CONTESTED SPACE: The territory in-between ADVERSARY SPACE: Their country

Once again, this principle applies regardless of the type of conflict in which you are engaged

Let’s also apply a cyber lens to this concept

OUR IT ENVIRONMENT

THE INTERNET

THE ADVERSARY’S ENVIRONMENT

INTEL ENRICHMENT

THREAT MONITORING

THREAT REPORTING

Within each of these operational spaces is an associated threat intelligence capability area

How do we conduct threat intelligence in each of these capability areas?

INTEL ENRICHMENT

Consume threat intelligence indicators of attack/compromise (signature-based & behavioral) in order to enrich defensive alerting & blocking systems.

IOC Ingestion Sensor Tuning

Malware Analysis

THREAT MONITORING

Monitor the Internet for threats against business interests, to include leaked credentials, PII, brand infringement, malware, malicious mentions, exposed footprint, etc.

Surface Web Social Media

Deep/Dark Web Digital Footprint

THREAT REPORTING

Consume reporting on adversarial motive, intent, capabilities, infrastructure, and TTPs in order to understand the adversary's operational posture

What? So What?

What Next?

CROWDSTRIKE

What are some of the best practices & common myths?

INTEL ENRICHMENT

Best Practices

- High degrees of automation
- Ingestion of timely content
- Ingestion of content derived from attack telemetry

Common Myths

- "More is better"
- "All intel can be automated"
- "Threat intelligence is only about indicators"

THREAT MONITORING

Best Practices

- Well-crafted keywords
- Knowing where to look
- Expectation management

Common Myths

- "All the answers are on the dark web"
- "I am going to find lots of threat actor chatter"

THREAT REPORTING

Best Practices

- Bottom line up front
- Reporting that is actionable
- Reporting that focused on implications

Common Myths

- "I should only care about my sector or geography"
- "All the answers should be fed to me on a silver platter"

Section 4: Serving Stakeholders & Forming the Team

There are generally three different types of threat intelligence stakeholders

Each stakeholder is of a particular type…

And each of them has particular needs.

The Threat Intelligence team should be designed to best serve the organization's stakeholders

SRATEGIC

OPERATIONAL

TACTICAL

Strategic Analysts

Talented speakers and presenters; good at simplifying technical content for non-technical audiences

Operational Analysts

Understands the role of the SOC teams; good at translating intel into actionable next steps

Tactical Analysts

Understands malware functionality at the binary level; granularly understands & can communicate adversary TTPs

Briefs threat information to strategic stakeholders; receives feedback & redirects intel program focus accordingly

Helps the SOC understand specific adversary campaigns; advises SOC on actions necessary to mitigate threats

Reverse engineers malware; assists with ingestion automation; maximizes automated defenses through continual system tuning

Different stakeholders require analysts that possess different qualities

Section 5: Examples of how to Operationalize Threat Intelligence

Scenario 1: A financially motivated eCrime actor seeking to conduct a ransomware attack

OURSELVES

ADVERSARY

STRATEGIC (Mind)

All

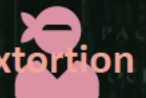
INDUSTRY

Financial Assets

ASSETS

Financially motivated eCrime actor(s)

MOTIVE



Extortion

INTENT

OPERATIONAL (Body)

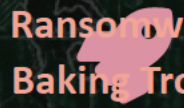
Domain Admins

PEOPLE

PROCESS

Domain Controller

TECHNOLOGY



Ransomware

Baking Trojan

CAPABILITY

Hostile IP / VPN / Proxies

INFRASTRUCTURE

TACTICAL (Actions)

2

DIGITAL

PHYSICAL

1

PSYCHOLOGICAL

Phishing 1

TTPs

Vulnerable OS 2

Let’s see how threat intelligence can help us better understand this threat

Scenario 1: A financially motivated eCrime actor seeking to conduct a ransomware attack

INTEL ENRICHMENT

- Consume indicators of most current banking trojan families associated with ransomware.
- Consume YARA & SNORT rules to block against custom compiled ransomware.

THREAT MONITORING

- Conduct web-scraping against potential credential leaks that could be used to achieve remote logins.
- Monitor for malicious inbound botnet traffic distributing downloaders.

THREAT REPORTING

- Consume threat reporting on major ransomware operators and how they exploited peer targets.
- Consume threat actor profile data on ransomware operators; provide installation techniques to threat hunting team

Tactical Stakeholders

SIEM AV EDR

Operational Stakeholders

Threat Hunters

Vulnerability Management

Strategic Stakeholders

CISO CTO

CROWDSTRIKE

Scenario 2: A nation-state actor with intent to conduct espionage against a pharmaceutical company

OURSELVES

ADVERSARY

STRATEGIC (Mind)

Healthcare

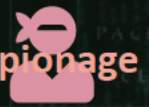
INDUSTRY

Intellectual Property

ASSETS

Enhance nation's healthcare capacity

MOTIVE



Espionage

INTENT

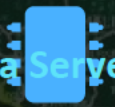
OPERATIONAL (Body)

Scientists

PEOPLE

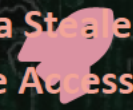
Classified Communications

PROCESS



Data Servers

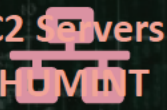
TECHNOLOGY



Data Stealers

Remote Access Tools

CAPABILITY



C2 Servers

HUMINT

INFRASTRUCTURE

TACTICAL (Actions)

3

DIGITAL

1

PHYSICAL

2

PSYCHOLOGICAL

USB Thumb Drive 1

Lateral Movement 3

TTPs

Bribery 2

Let's see how threat intelligence can help us better understand this threat

Scenario 2: A nation-state actor with intent to conduct espionage against a pharmaceutical company

INTEL ENRICHMENT

- Consume indicators of most current remote access tools and associated downloaders
- Engage in automated sandbox analysis of malware associated with nation-state actors that steal intellectual property

THREAT MONITORING

- Conduct web-scraping in search of intellectual property leaks and/or evidence of insider threats
- Scrape for malicious malware that could potentially be leveraged to steal data

THREAT REPORTING

- Consume reporting on actors known to steal intellectual property and familiarize the org with associated TTPs
- Read strategic reporting on China and advise physical security on how they might leverage insiders to steal data

Tactical Stakeholders

Sandbox AV EDR

Operational Stakeholders

Insider Threat

Vulnerability Management

Strategic Stakeholders

Physical Security

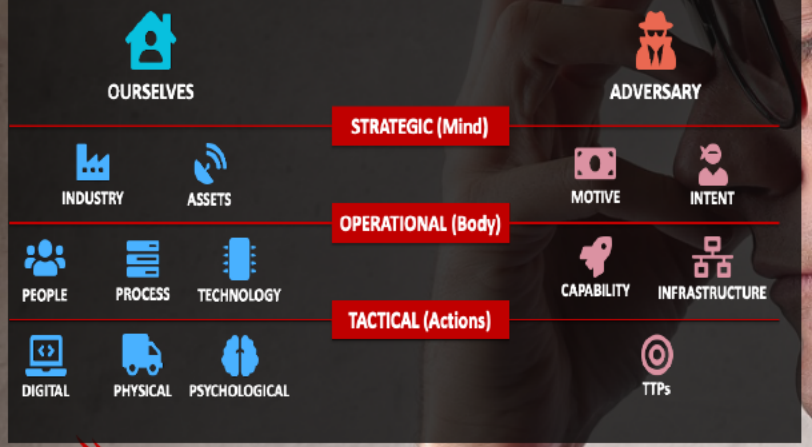
CTO

Summary

In summary, we talked about the following:

Conflict

The Eyes of the Adversary



Intel Capability Areas

Intelligence Stakeholders

CROWDSTRIKE

RSAConference2020 APJ
A Virtual Learning Experience

RSAConference2020 APJ

A Virtual Learning Experience

Questions?