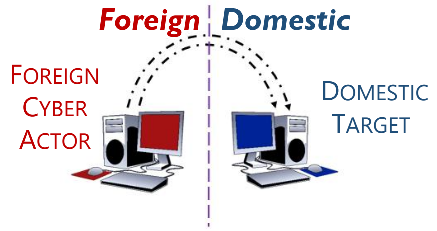
MALICIOUS CYBER ACTIVITY



Key Challenges in
CYBER THREAT INTELLIGENCE

See It

We see and collect a fraction of the universe of malicious cyber activity.

Make Sense of It

- *Make dots out of raw data*
- *Connect the dots*
- *Assess threat in context*
- *Generate finished intelligence*

○ ***Process it***

Make "dots" out of raw data

- *How much of the data we collect is actively exploited?*
- *How much is available for research or reference?*

○ ***Analyze it***

Connect the dots

- *How do we share data from diifferent methods, agencies, and disciplines?*
- *How do we blend technical, regional, and functional analysis and expertise?*

○ ***Contextualize it***

Assess threat in context

- *How do we understand vulnerability and consequence when we lack firsthand insight for potential targets that are outside of our own networks?*

○ ***Make it Relevant***

Generate finished intelligence

- *What do we want the recipient of our reporting to do with it?*
- *How does this differ depending on the audience? (e.g., policymaker vs. network operator)*

Share It

Once analyzed, share with the appropriate audience.

Share it internally
Share it externally

Directly ***Indirectly***

Was it delivered?

- *If yes, was feedback given?*
- *If no, why not? (Resource limitation, report content)*

Use It

Even if threat reporting is shared, it may not be used!

Did the recipient use it?

Yes ***No***

If not used, why not?

- *Not Timely?*
- *Not Actionable?*
- *Lacked Context?*
- *Other?*

Feedback Provided?

Feedback drives process and content improvement and also enriches provider understanding of the victim/target.

Tools to Drive Change Include:

Organizational Structure
Internal Processes
Partnerships
Legislation
Technology
Resources
Oversight