Integrated Cyber

Johns Hopkins University Applied Physics Laboratory
Laurel Maryland, Oct 2 and 3, 2018

https://iacdautomate.org

APL JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Actionable Information

Consumers drive what is actionable

- You must consider how information is used to make it actionable
- The consumers determine value
  - Their view of timely, accurate, etc are different than providers think

How Do We Make Information Actionable

- **Let's start with IOCs**

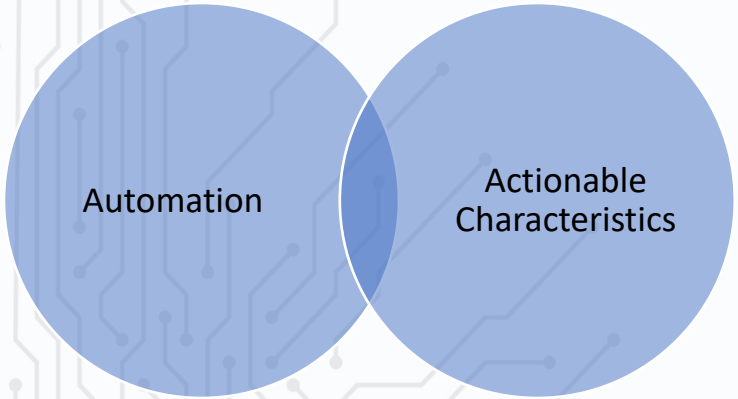
- **Issues**
  - **Too many**
  - **Too hard to determine if applicable**
  - **Too easy for the adversary to change – so not very impactful**

- ***Must triage, prioritize, and respond to IOCs in as automated manner as possible***

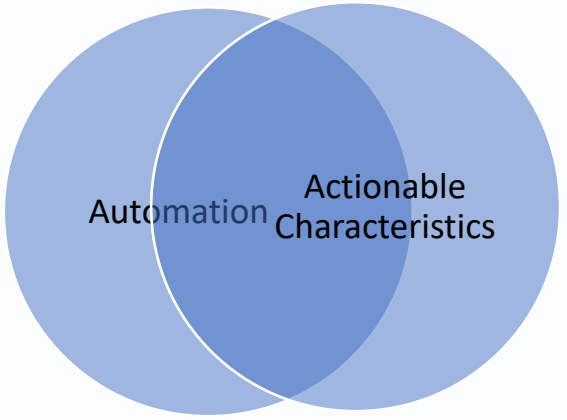
Current State of Net Defense Environments

- **Automation opportunities may be limited**
  - **Products are intended to interact with a human through the user interface**
  - **Services have licensing restrictions that limit automation**
  - **Many current products cannot be integrated or orchestrated in an automated manner**
- **Culture**
  - **Many organizations are not willing to automate decision processes or responses**

Automated Capabilities Today



Goals for Automated Capabilities



So what makes IOCs actionable for network defenders?

What Should be Shared?

- **Most cyber threat information sharing includes lots of details**
- **But hard for the consumer to determine which pieces of information are most applicable or important to them**

AND - it is not the volume or velocity that is needed, it's the *right* information at the *right* time with the *right* value

- **Valuable for whom?**
  - **Analysts or defenders? Incident Response team? Vulnerability Management team? Forensics?**
- **Valuable for doing what?**
  - **Detect? Assess? Analyze? Monitor? Protect?**

What are the 'value' propositions?

Valuable information- A Few General Traits

Scalable
- Static information such as a domain name is not effective against domains generated by DGA.
  - Example – What information will identify persistent adversaries continually morphing attack technique over time

Timely
- Value diminishes with time, specially for tactical information for the defender.
  - Example – More strategic information about TTPs has value for a longer period of time

Trusted
- If the threat information is not from a trusted source or if the integrity is not vetted, there are limitations on its usefulness
  - Example – Security alerts generated from untrusted partners may cause havoc

Contextual
- Without the ability to relate information to my priorities, vulnerabilities, or environment, it is useless.
  - Example – A Net Defender can use mitigations customized to the relevant kill-chain phase, if known

Translatable
- Adversary TTP information must be translatable to CND Tools and Techniques.
  - Example – Mapping for Information related to Common Vulnerability Enumeration (CVE), CWE, CCE

Granular
- Specific and granular information is more actionable without unintended effects.
  - Example – If the adversary only uses a subdomain, the whole domain doesn't need to be blocked

Measurable
- What are good measures of the 'Value' of information?
  - Example – How at risk am I to the threat, or how urgent is the needed remediation

What is the Community's Position on 'Value'?

- **Often the desirable traits are mutually competing. So, how do we get the desirable ones we need is the real question.**
  - **For example, two of the 5 guiding principles of the Cyber Threat Alliance (CTA) are related to 'timely' and 'contextual', which may be at odds with each other. To get more context, may make the information less timely.**

How does the community make a tradeoff of 'values'?

What is valuable to network defenders?

Integrated Adaptive Cyber Defense is sponsored by the Department of Homeland Security and the National Security Agency in collaboration with The Johns Hopkins University Applied Physics Laboratory.

Our goal is to dramatically change the timeline and effectiveness of cyber defense via integration, automation, and information sharing.

https://www.iacdautomate.org


@IACD_automate


https://www.linkedin.com/groups/8608114


icd@jhuapl.edu