LegalSEC SUMMIT 2018

PRACTICAL THREAT AUTOMATION

Session 223

PANEL

- **Jaquar Harris**
  - Intelligence Manager, Global Resilience Federation
- **Kevin Moore**
  - Chief Security Officer | Fenwick & West LLP
- **Richard Timbol**
  - ISSM Davis Polk & Wardell LLP
- **Michele Gossmeyer (moderator)**
  - Global Director, Information Governance, Risk & Compliance, Dentons

INTRO

- Threat automation overview
  - Purpose
  - Goals
  - Current info
- Architecture overview of speaker's implementations
  - value of setup
  - pitfalls encountered

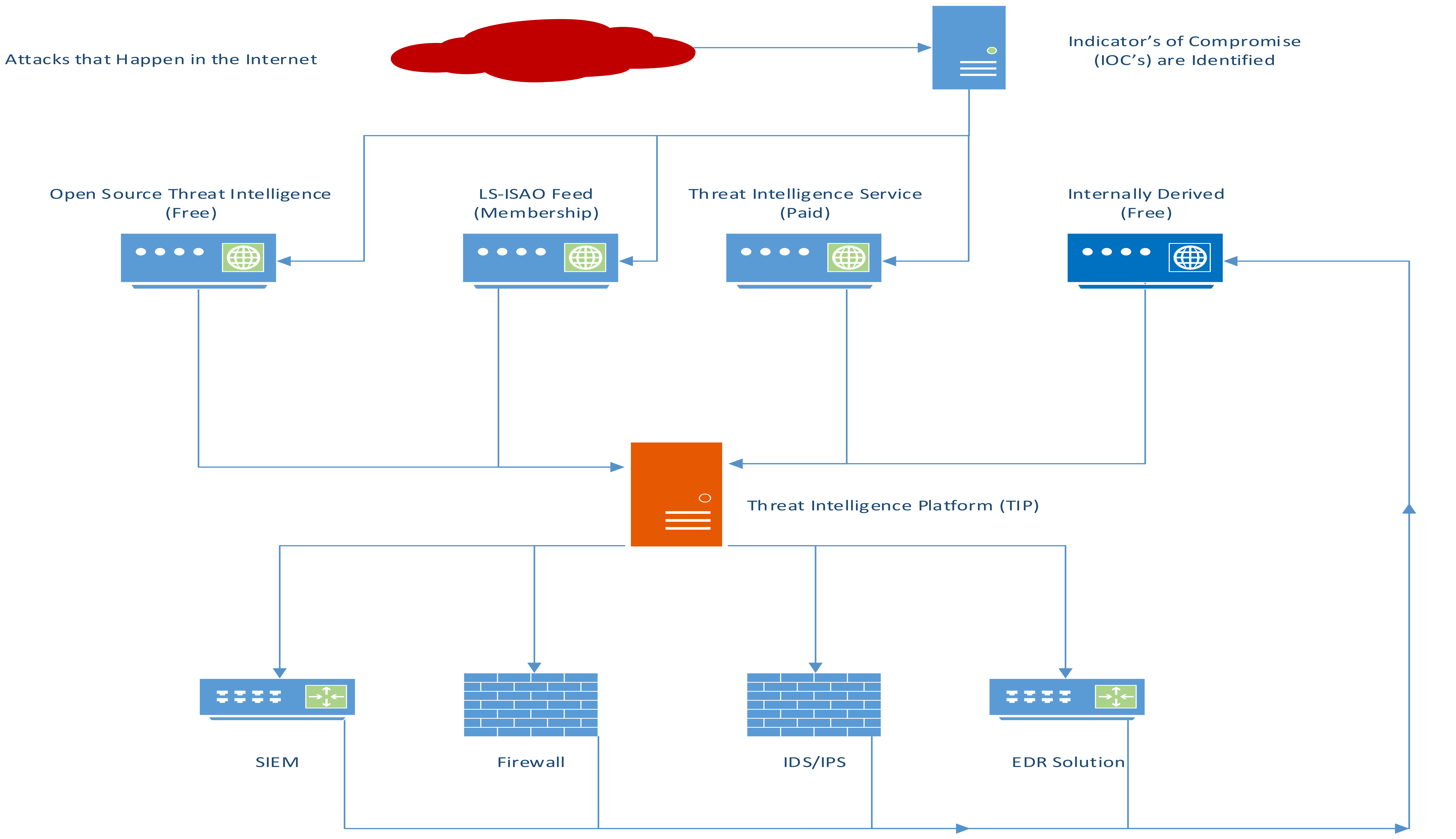
OBVIOUS BUT IMPORTANT…

- **Have a clear strategy before trying to implement**
  - What type of Indicators of Compromise (IoC) can your security products pivot on?
  - What type of formats can ingest the intelligence?
  - What are their limitations? e.g. Next-Gen Firewalls are limited to the tens of thousands of ip's they can have on a block list
  - How do you develop workflow around those limitations?
  - How do you intend your products and staff to use the intelligence?

THE KEY COMPONENTS

- Timely & Relevant Threat Intelligence Feeds
  - You can’t ingest them all without drowning!
  - Should contain the types of IoC’s you can use.
- A Simple to Use & Maintain Threat Intelligence Platform (TIP)
  - Should import/export in the formats your security tools use.
  - Once setup should be able to leverage scripts or rules to function in a 99% automated mode.

THE FLOW & ARCHITECTURE OF A THREAT INTELLIGENCE ECOSYSTEM



Attacks that Happen in the Internet

Indicator's of Compromise (IOC's) are Identified

Open Source Threat Intelligence (Free)

LS-ISAO Feed (Membership)

Threat Intelligence Service (Paid)

Internally Derived (Free)

Threat Intelligence Platform (TIP)

SIEM

Firewall

IDS/IPS

EDR Solution

LegalSEC SUMMIT 2018

THE EVERYTHING LINK FOR THREAT INTELLIGENCE

An “Awesome” curated list of Threat Intelligence Feeds, Platforms & Tools

https://github.com/hslatman/awesome-threat-intelligence

INSIGHTS FROM KEVIN

- Automation: automatic handling of a task in an information or cyber security system
  - Works well within a single product or system, but…
- Orchestration: required to automate many tasks or process between other products, tools or systems
  - Get more value out of your people, processes and tools
  - Streamline detection, response, and remediation.

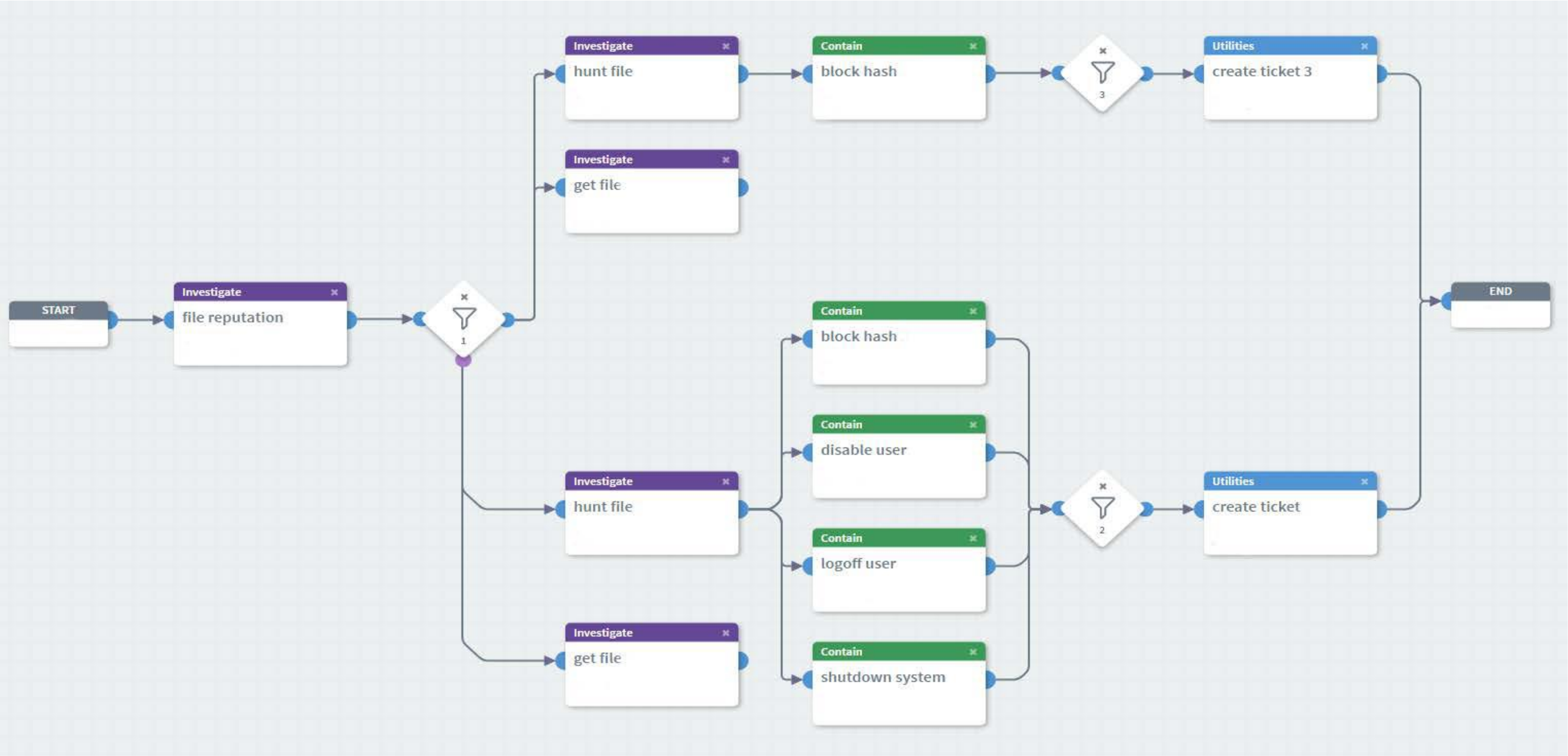
CURRENT CHALLENGES

- Managing multiple tools and processes manually
- "Best of breed" security systems do not integrate well
- Feeds – Prevention is great if high fidelity and quality
  - Relevance/Context
    - How does the intel relate directly to your organization.
    - Is the intel related to internal network activity or alerts
  - Enrichment
  - Speed
- Rotation of IOCs
- Staffing requirements/challenges

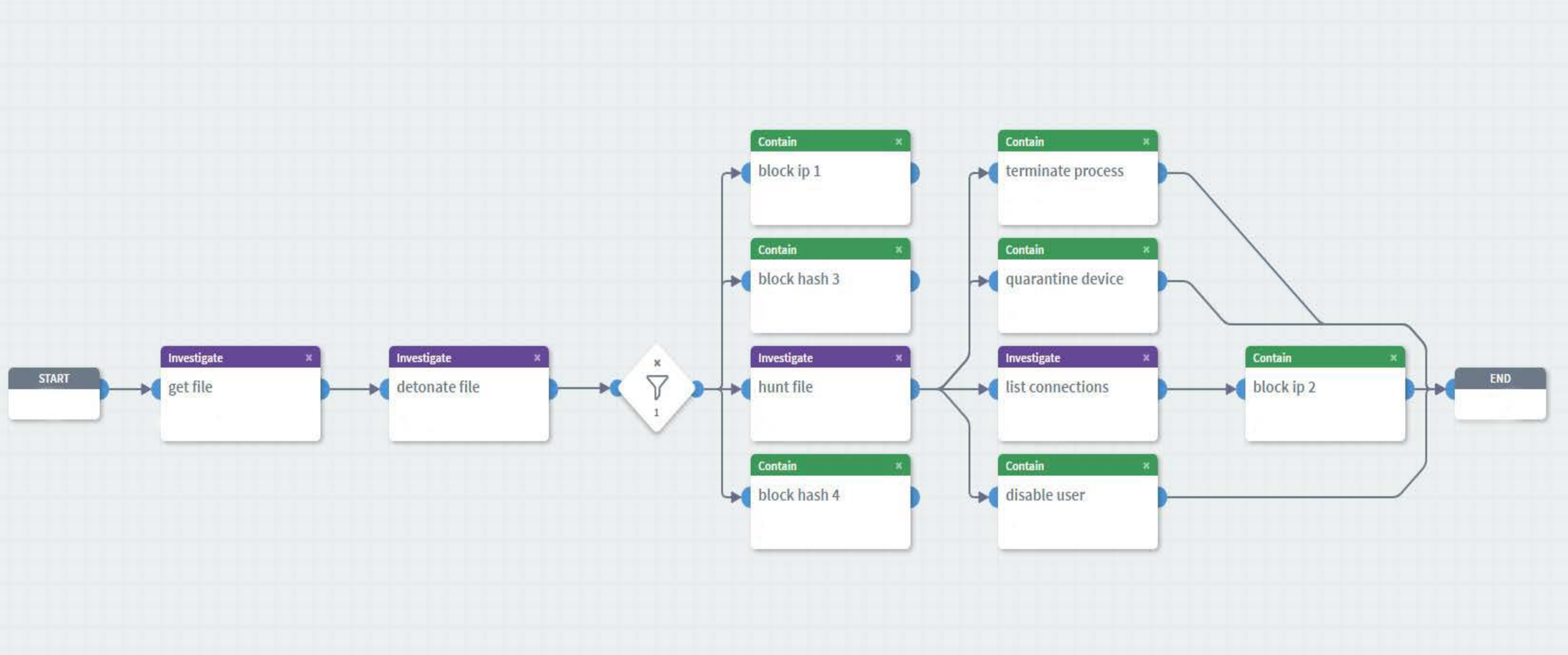
SAMPLE - WHAT ARE WE DOING

- Perch Security
  - TIP + IDS/IPS + MSP of TI
  - Injests feeds compares to network traffic and alerts on hit of IOC
- Phantom – Orchestration and Automation
- Cisco
  - pxGRID → ISE → Infrastructure via ACLs
  - Threat Intelligence Director (TID)

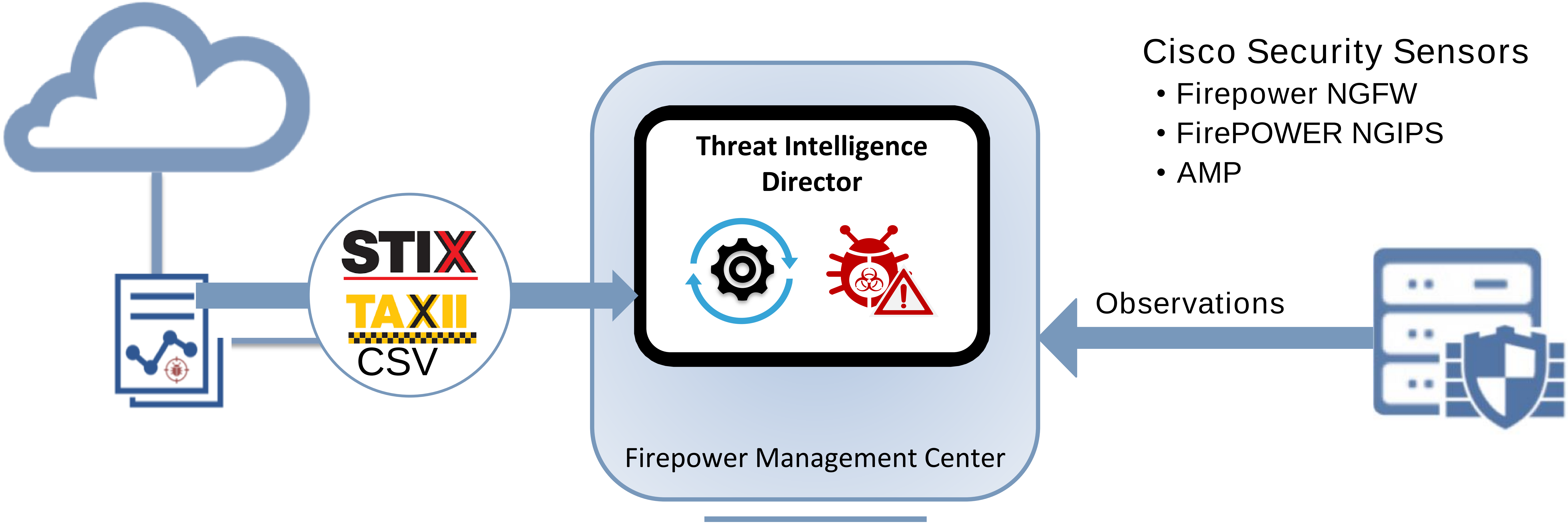
MALWARE PLAYBOOK - EXAMPLE



RANSOMWARE PLAYBOOK – EXAMPLE



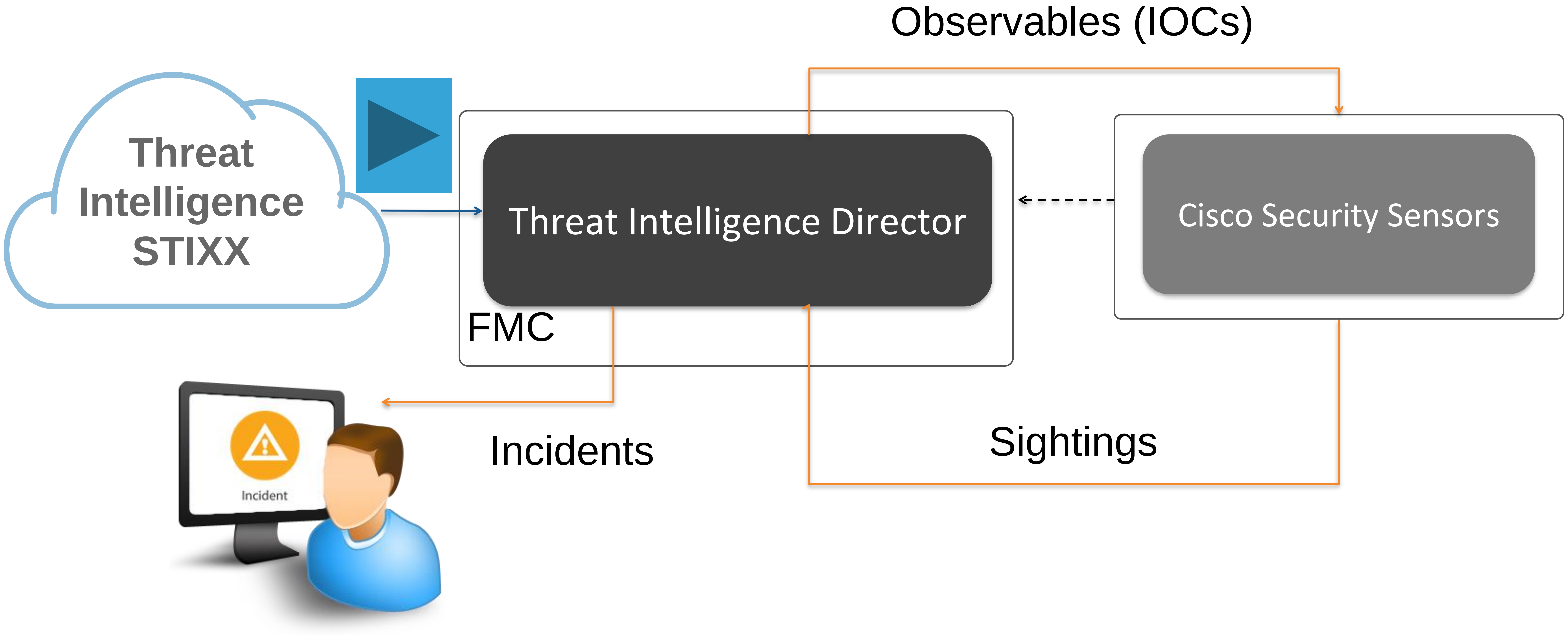
CISCO THREAT INTELLIGENCE DIRECTOR OPERATIONALIZE THREAT INTELLIGENCE



Cisco Security Sensors

- Firepower NGFW
- FirePOWER NGIPS
- AMP

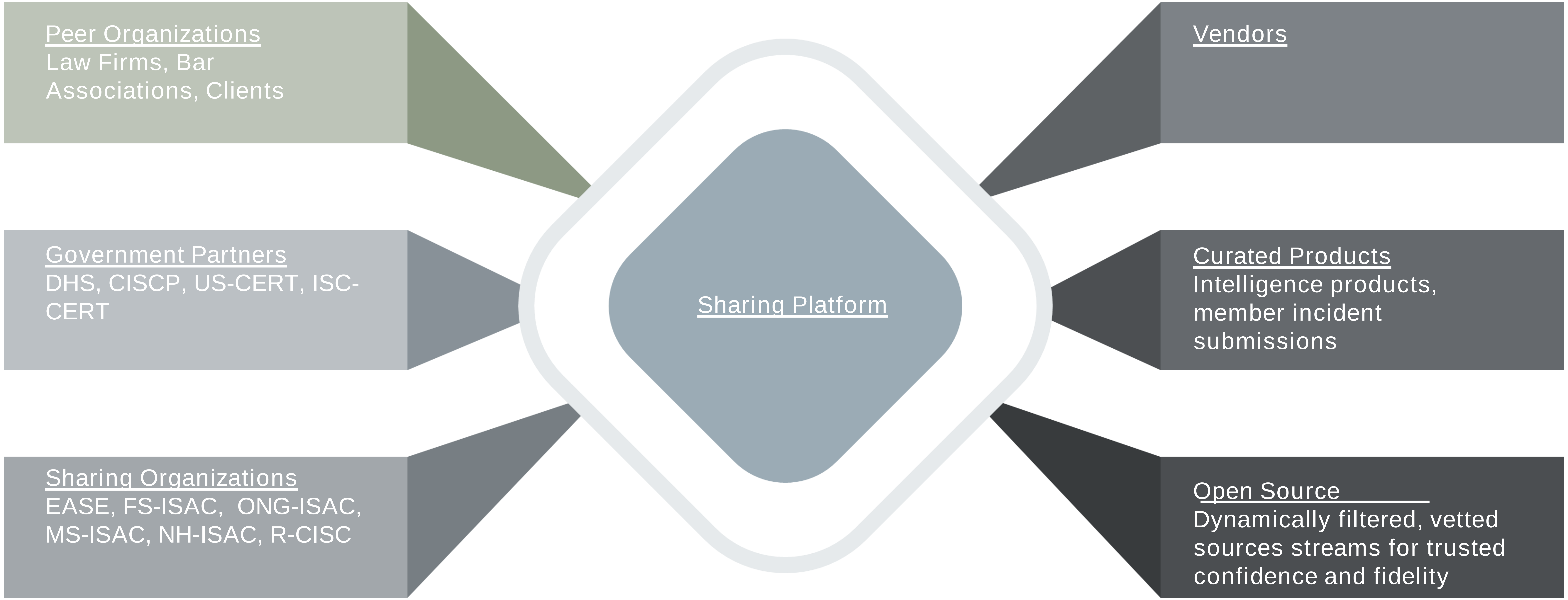
INTELLIGENCE DATA FLOW



OTHER OPTIONS

- LS-ISAO – Subscription to Anomali included
- Anomali STAXX (free)
- MineMeld (Open Source) from Palo Alto Networks
- GOSINT – Open Source Intel gathering and processing framework from Cisco
- MISP (Malware Information Sharing Platform)

LS-ISAO AUTOMATED THREAT INTELLIGENCE



Peer Organizations
Law Firms, Bar Associations, Clients

Government Partners
DHS, CISCP, US-CERT, ISC-CERT

Sharing Organizations
EASE, FS-ISAC, ONG-ISAC, MS-ISAC, NH-ISAC, R-CISC

Sharing Platform

Vendors

Curated Products
Intelligence products, member incident submissions

Open Source
Dynamically filtered, vetted sources streams for trusted confidence and fidelity

LS-ISAO AUTOMATED THREAT INTELLIGENCE

- Intelligence Source Integrations
  - AIS
  - Curated sources
  - Intelligence Partners
- Peer ISACs and Cross Sector Sharing
  - Feeds from – NH-ISAC, ONG-ISAC, FS-ISAC, MS-ISAC, EASE
- Volume vs Fidelity
  - Ingestion of 3.5 million Indicators
  - Leveraging Resources
- Sharing Value
  - Community sharing
  - Enrichment
  - Analysis

Questions????