MARCH 2021

Argonne NATIONAL LABORATORY

# CFM:
# CYBER FED MODEL

**DAN HARKNESS, CISSP**
Group Lead, CORSA
dharkness@anl.gov

**SCOTT PINKERTON**
Program Lead, Cyber Threat Sharing
pinkerton@anl.gov

Argonne National Laboratory's work was supported by the U.S. Department of Energy, Office of Science, under contract DE-AC02-06CH11357.

# INTRODUCTION

- The Cyber Fed Model (CFM) is a system built to connect organizations in community to combat cyber threats through near real-time automated sharing of actionable information
- Community approach increases relevance and skin-in-the-game for participants
- Technology-agnostic design enables broad compatibility
- Flexible distribution supports 1-1 (direct) or 1-many (broadcast) distribution

# CYBER FED MODEL: THE ORIGINS

- Cyber Attacks in 2004
  - Targets included Argonne, NASA, and others
  - Attacker leveraged shared trust relationships
- Can we leverage our trust relationships for defense?
  - Needs to be automated (human response can be slow)
  - Data owners need to be in control
- Technological underpinnings
  - Traditional LAMP stack; custom PHP web service
  - Specialized Perl scripts as clients
  - Custom scripts for interacting with Cisco and Palo Alto
  - No standards for cyber threat data existed
    - Customized version of IDMEF looked promising

# CYBER FED MODEL: EVOLUTION

- Fast Forward to 2013
  - Key defense for multiple laboratories
  - Standards for cyber threat information beginning to emerge, but still competing
  - Greater implementation variability across participants
- TIME TO EVOLVE
- Updated Technology
  - Geographically redundant high availability
  - RESTful API
  - Envelope & Payload design provides data agnosticity
    - Allows support of multiple / evolving standards
  - Modular approach to client tools supports variability

# CYBER FED MODEL: NOW

- Over 75 Participating Organizations
  - Critical infrastructure
  - Government
- Daily Data Volumes
  - Uploads of 45K+ indicators
  - 500+ organization-specific reports
- Unique Capabilities
  - Support for both direct and broadcast distribution
    - And anything in between; customized per upload
  - Payload agnostic
  - Multi-platform connectivity
  - Last Quarter Mile Toolset (LQMT)

# CYBER FED MODEL: ADVANCING THE FUTURE

- Above the Water Line (Today)
  - Information sharing focuses on “final product” data
  - Collaborative analysis efforts are limited to central collection of subsets of organizational data
    - Public or known “safe” to share with others
    - Reasonable bandwidth and storage considerations
- Below the Water Line (Future)
  - Information sharing focuses on “pre-decisional” data
  - Collaborative analysis efforts have access to all organizational data where it resides
    - Local datasets; raw, unfiltered
    - Bandwidth, storage, sensitivity concerns alleviated through targeted queries

# CYBER FED MODEL: ADVANCING THE FUTURE

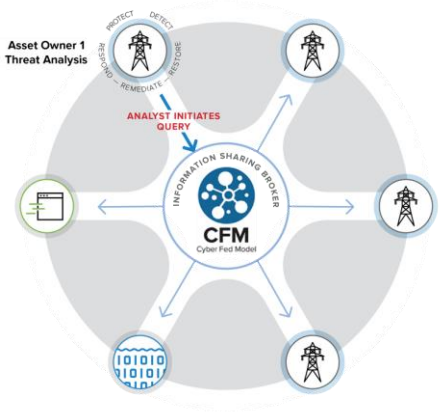

**What used to take months, now takes milliseconds**

- Information sharing pivots to become distributed cyber threat discovery
- A flexible query/response mechanism is added
  - On-demand
  - Allows for *tailored, relevant* collection from “below the water line”
- Becomes a force multiplier for cyber defenders
- Cyber threats are discovered more quickly; Cyber threat intel (CTI) is higher quality

# CYBER FED MODEL: ADVANCING THE FUTURE

## LOCAL DETECT
ANOMALOUS / SUSPICIOUS

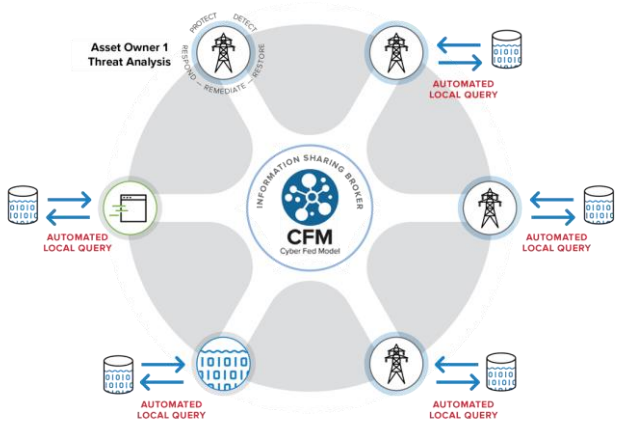
1




Site initiates request for information

## QUERY
ACROSS COMMUNITY PARTICIPANTS

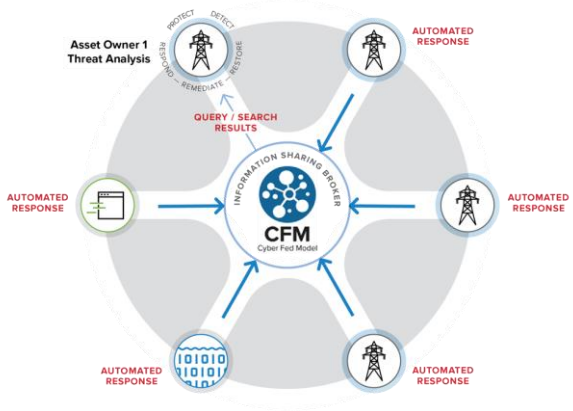
2




Community queries local dataset

## RESPONSE
DATA SHARING

3




Community responses are relayed

# CYBER FED MODEL: NEEDED FOR THE FUTURE

- Coalition of the willing for ‘local search’ trust communities
- Development of trust framework
  - Sharing agreements and parameter representation
  - What data will I (can I) share, and with whom?
  - Site obfuscation requirements
  - Redaction requirements
  - How can data be used (both query and response)?
- Development of query and response framework
  - Define queries for crawl, walk, run phases
  - Identify / develop query representation
- Identification of key technology integrations

# THANK YOU!

Dan Harkness
dharkness@anl.gov

Scott Pinkerton
pinkerton@anl.gov