Deterring Cybercrime via a Global CyberGrid

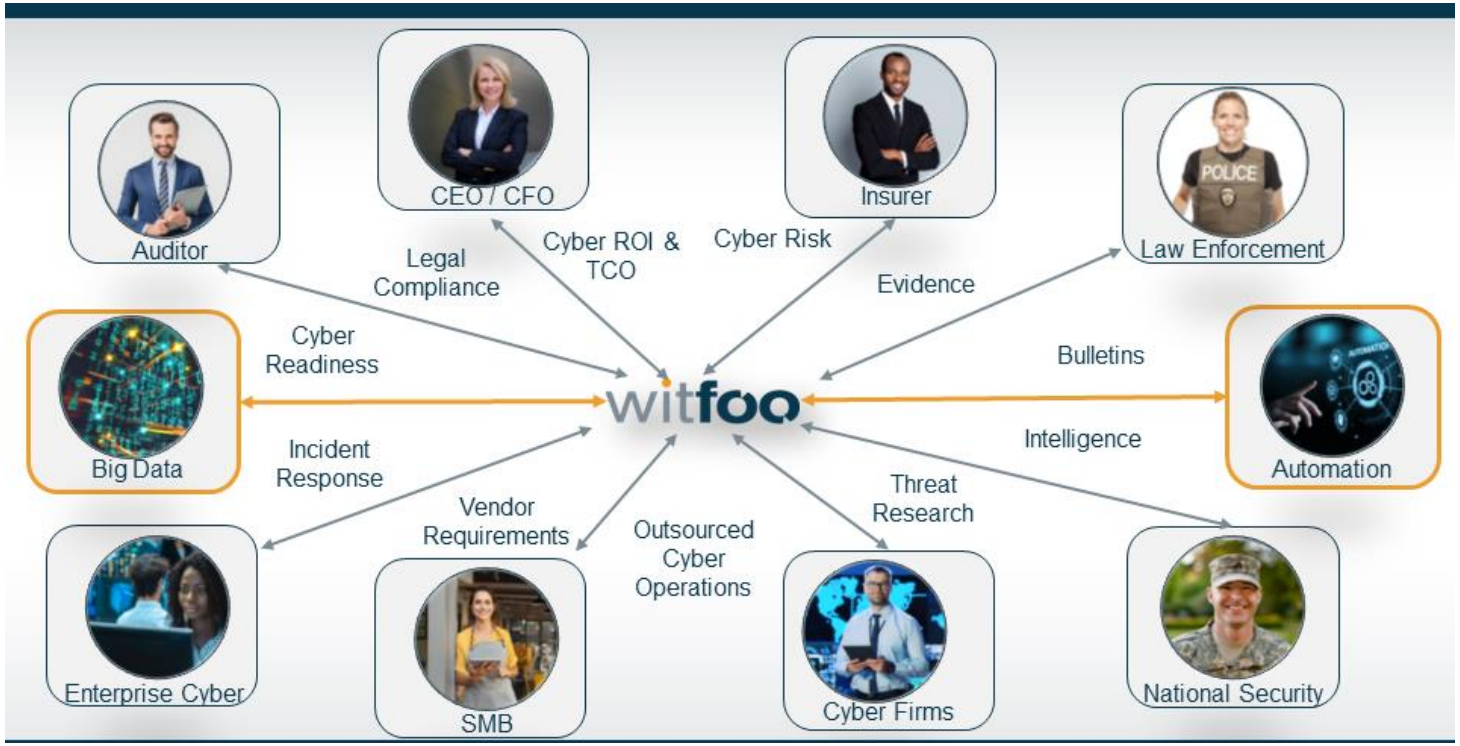
Charles D. Herring, WitFoo co-Founder & CTO
Charles@WitFoo.com
CharlesHerring.com
@charlesherring

About Charles

- WitFoo co-Founder and Project Lead (2016-)
- Cisco & Lancope Security Architect (2012-16)
- DoD Security & Data Consultant (2005-12)
- InfoWorld Test Center (2003-2008)
- US Navy Cyber Security (2002-2005)
- US Navy F/A 18 Hornet Avionics (1995-2002)

WitFoo Research

- Founded by Veterans of the US Military, Law Enforcement & Cyber
- Research began in 2016 across 20+ private & public organizations
- Goal to create a CyberGrid across the Cyber Community



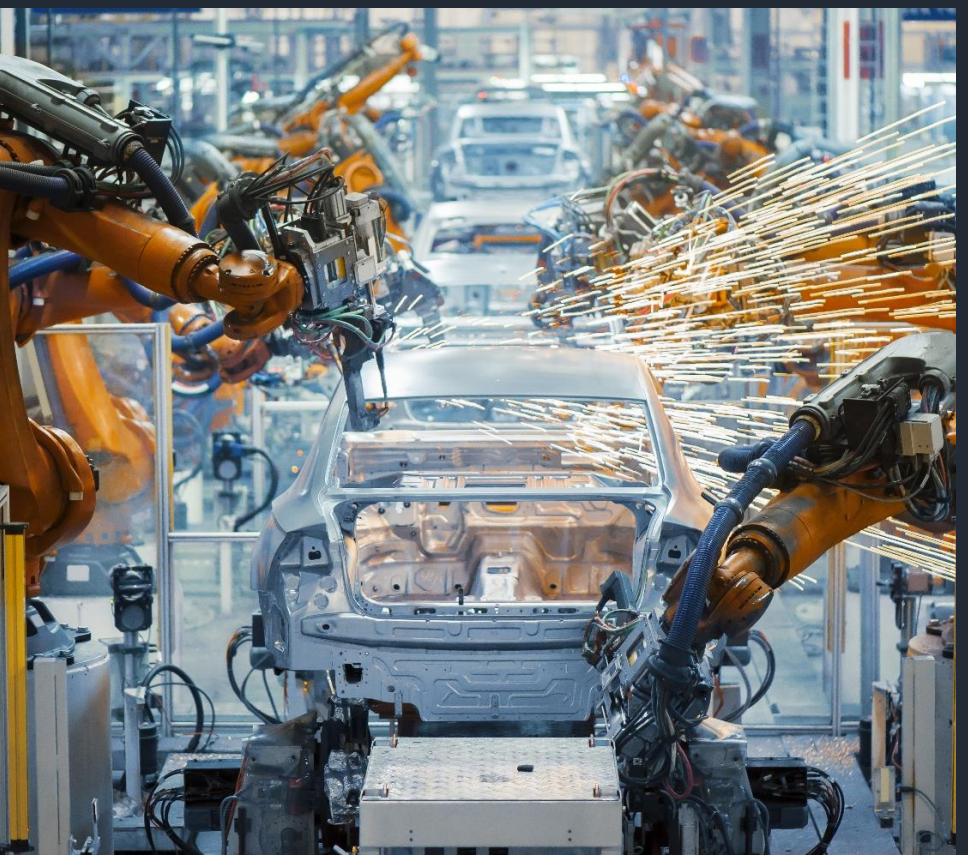
Agenda

Theory & Philosophy

Benefits of Community Deterrence

Implementation & State of Research

IT Evolved from Manufacturing



- Harvest Raw Materials
- Assemble New Units
- Ship & Store Units
- Linear Workflows
- Transactional/Unit Based

SECOPS is not IT

- Stop criminal activity
  - Prevention
  - Detection
  - Response
  - Remediation
- Non-linear workflows
- Based on Law Enforcement

IT Outcomes in SECOPS

Blacklist / Block

Reimage / Restore

Reset / Lock

No Impact to Criminal Activity

Legal Outcomes in SECOPS

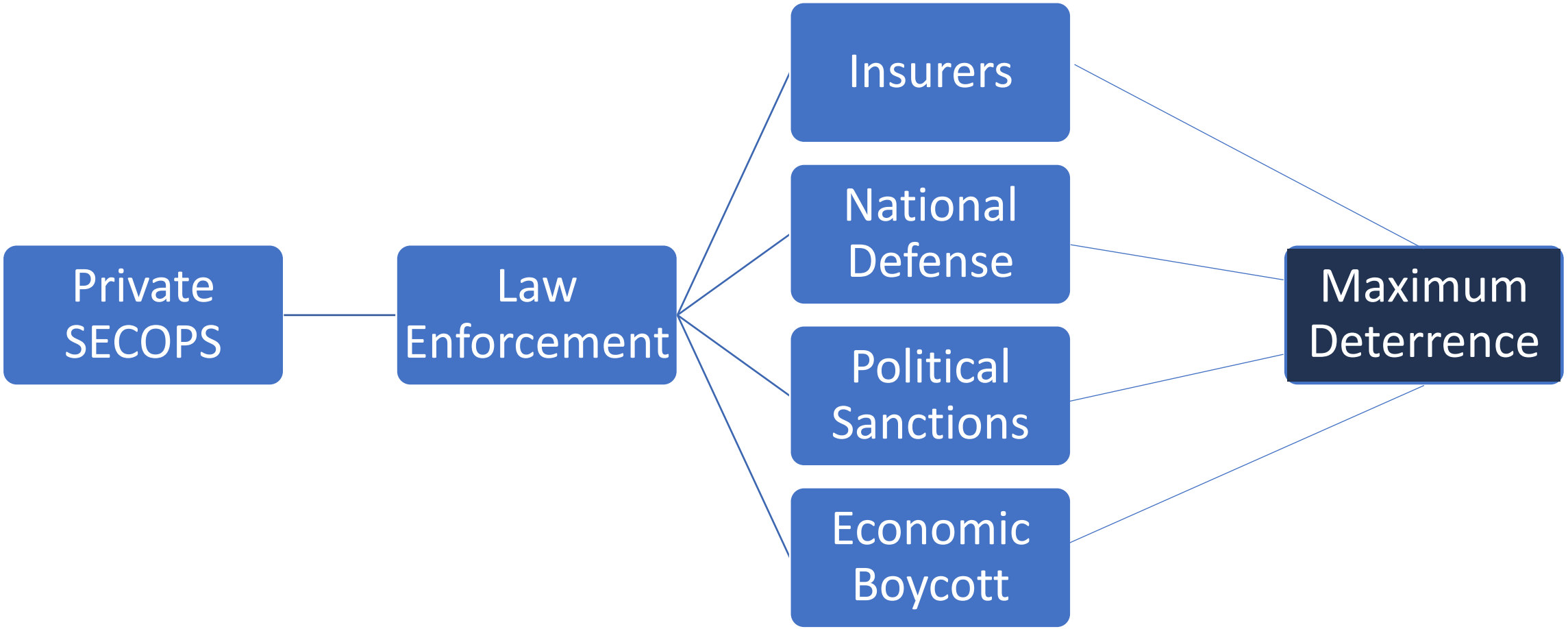
Incarceration

Financial Recovery

RICO Arrests

Increases Criminal Deterrence over Time

Optimized Cyber Community

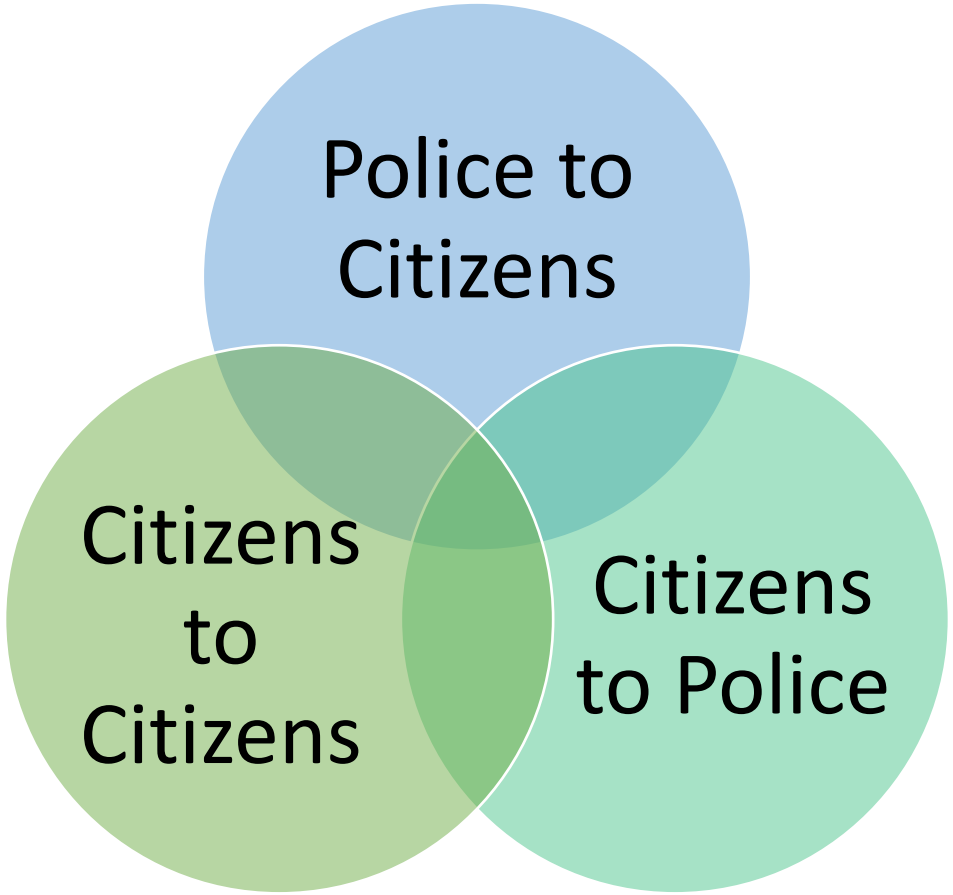


Power of Deterrence

"…the certainty of being caught is a vastly more powerful deterrent than the punishment."

- "***Five Things About Deterrence"*** **–** DOJ 2016

Safe Communities Communication



Short-term Benefits of Coordination

Recovery

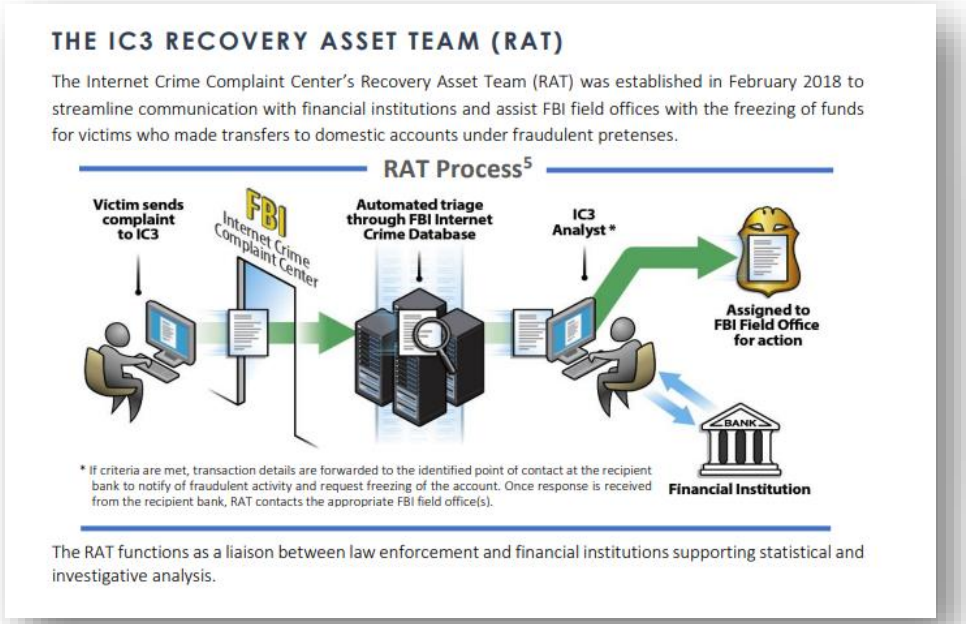
Attribution

Root Cause

Reduce Future Risk & Near-Term Recovery

Recovery

- Insurers coordinate with Law Enforcement
- Law Enforcement Recovery Success is High



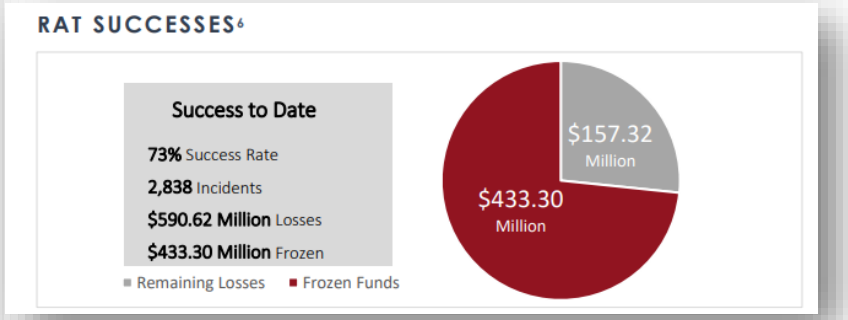
THE IC3 RECOVERY ASSET TEAM (RAT)

The Internet Crime Complaint Center's Recovery Asset Team (RAT) was established in February 2018 to streamline communication with financial institutions and assist FBI field offices with the freezing of funds for victims who made transfers to domestic accounts under fraudulent pretenses.

RAT Process[5]

* If criteria are met, transaction details are forwarded to the identified point of contact at the recipient bank to notify of fraudulent activity and request freezing of the account. Once response is received from the recipient bank, RAT contacts the appropriate FBI field office(s).

The RAT functions as a liaison between law enforcement and financial institutions supporting statistical and investigative analysis.



RAT SUCCESSES[6]

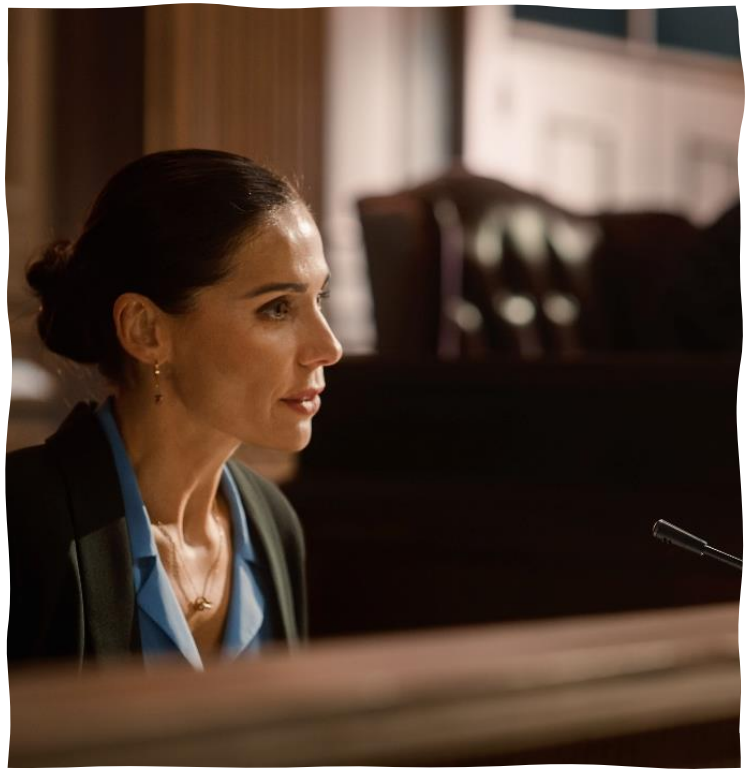
Success to Date

73% Success Rate
2,838 Incidents
$590.62 Million Losses
$433.30 Million Frozen

** 2022 FBI Internet Crime Report*

Attribution

- Human Intelligence (HUMINT) is required for legal attribution
- Legal attribution is required for civil litigation
- Civil Litigation leads to expanded recovery of damages



Root Cause

Physical, financial & third-party evidence

Medium-term Benefits of Coordination

Reduced Costs

Improved Insurance

Quality Threat Intel

Reduce Costs & Improve Protection

Barriers for Law Enforcement

- Missing Evidence
- Disorganized Data
- Poor Non-repudiation
- Insufficient Loss/Damages

Barriers for Private SECOPS

- Over-disclosure risks (legal & brand)
- Law Enforcement over-reach
- Understaffed
- Lack of expertise

Barriers to SECOPS Craft

- Multi-Petabyte Data
- Narrow-focus Tools/Controls
- Poor Collaboration Options
- Data Linguistics Complexity

WitFoo Research Principles

Predestination of Data

Non-repudiation

Low Cost for Big-Data

Data Comprehension

Object Oriented Organization

Sharing Levels akin to Physical Security

Sharing Grid/Mesh across community

Predestination of Data

The entire lifespan of a datum must be established at its birth. Comprehension of syntax, source and intent must be extracted. Inference and potential impact of the datum must be established. Nature of creation and transmission must be preserved. All expected evolutions and iterations of the data need to be established for processing. The death (TTL) of the datum must be established at persistence.

Non-repudiation Approaches

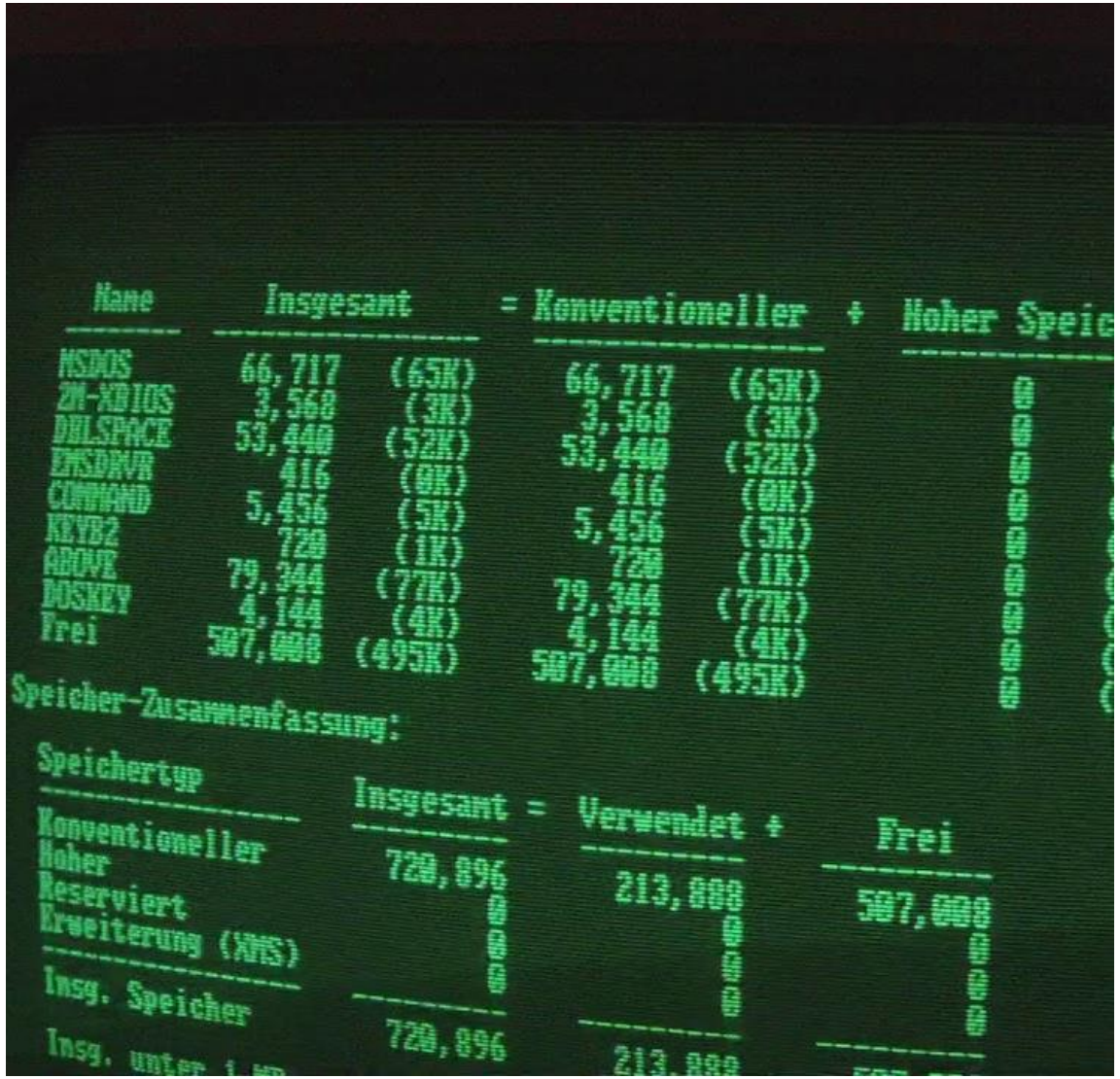
- Block-chain
- Signal Time Hashing
- Object Time Hashing

- Azure Confidential Locker
- AWS Blockchain
- Hash.WitFoo.com
- HyperLedger.org (Freemium)
- Corda (Apache 2.0)


```
                                    sha1sum /tmp/evidence.bin
b6cf99ed08a03eac26e82ffb1908f5eaf361526d  /tmp/evidence.bin
```

Big-Data Total Cost of Ownership

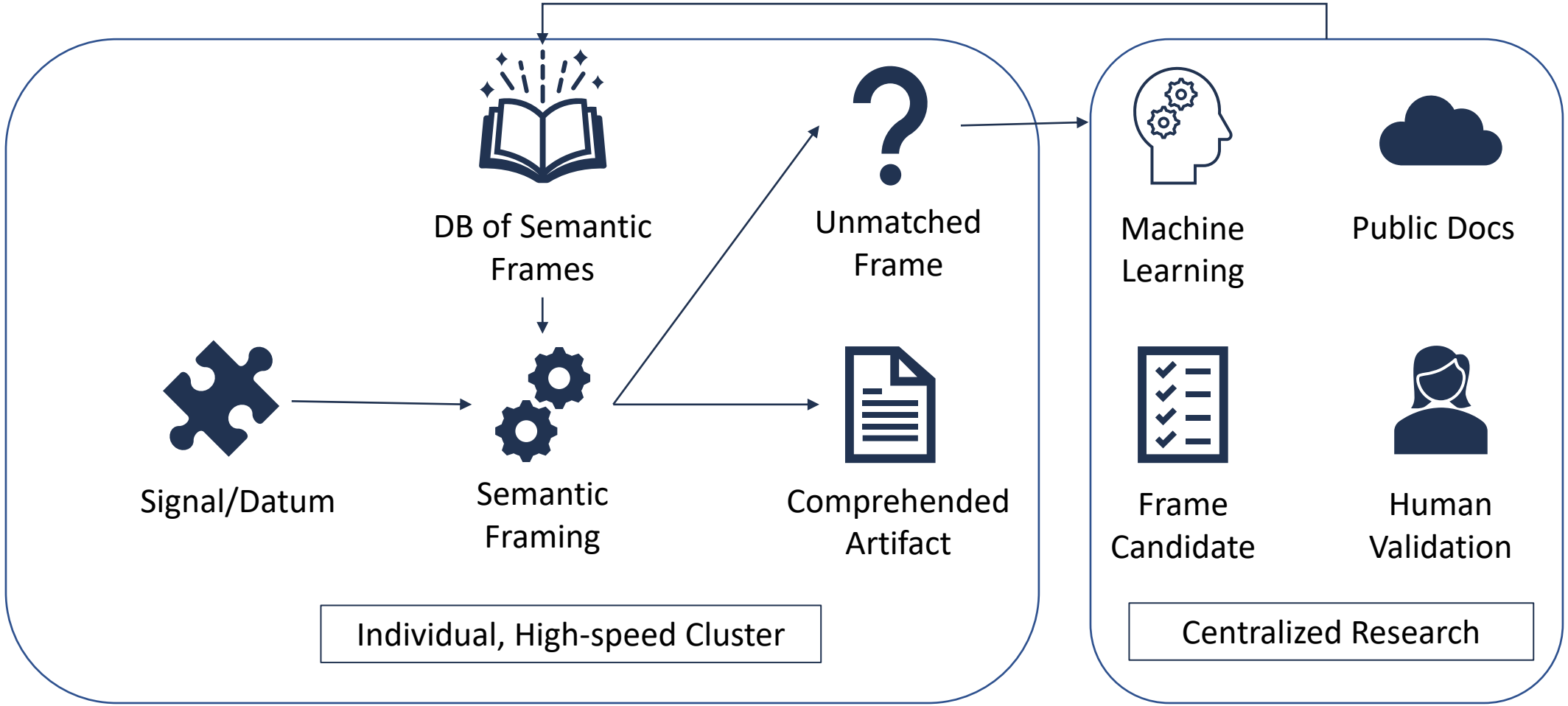
- *“Resource Sensitive Coding”* – IOPS, RAM, Storage & Compute
- *Avoid “Data Triage Licensing”* – Vendor-centric ingest/storage
- Labor Costs of Parsers, Engineering & Logic



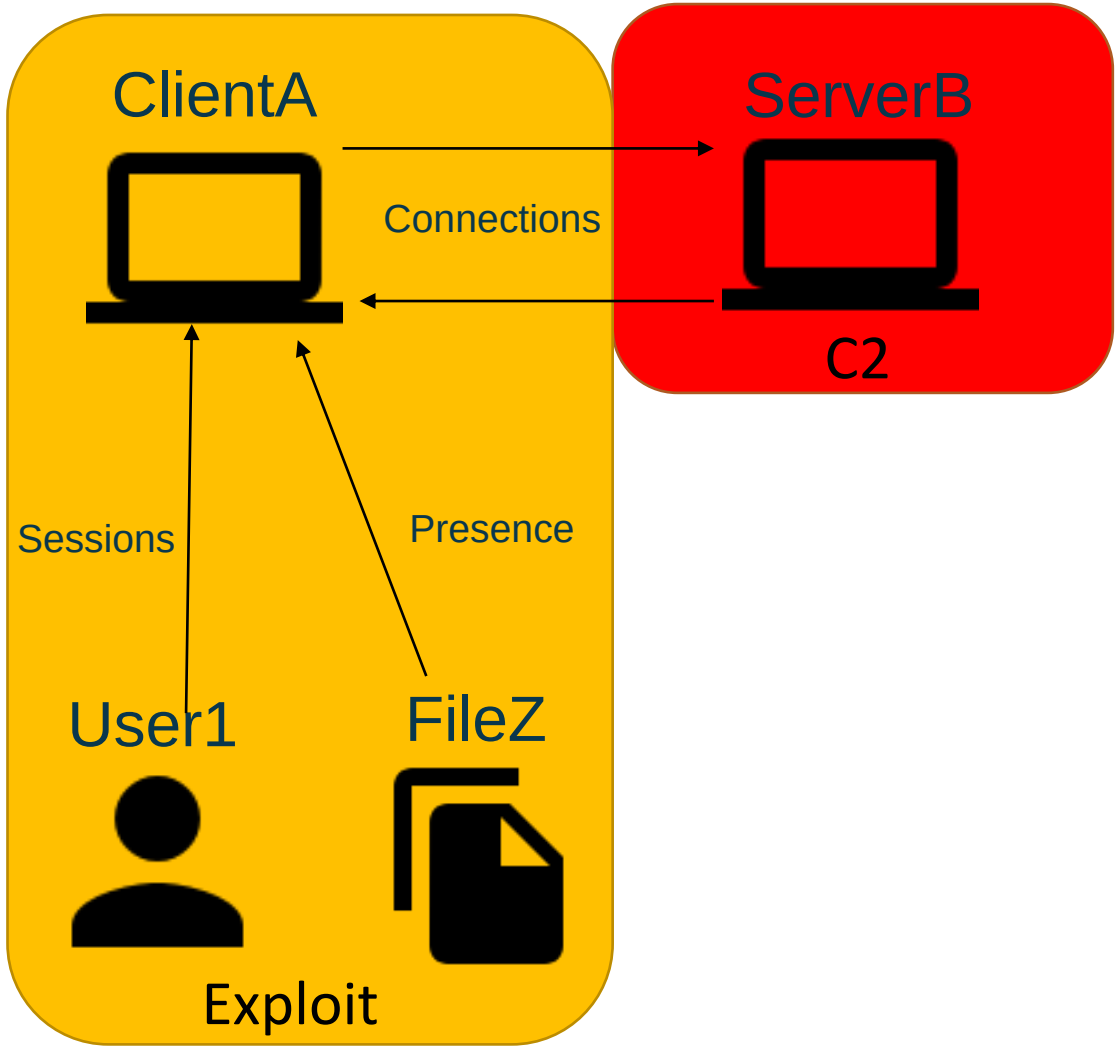
Data Comprehension

- Sematic Framing (Grammar)
  - Framing Validation
  - Illogical Computer Formats
- Data Validation
  - Data Context (Encyclopedia)
  - Data Inference (Chatter)
- Low Compute Cost at High Rate

Consolidated Human Asst. Learning



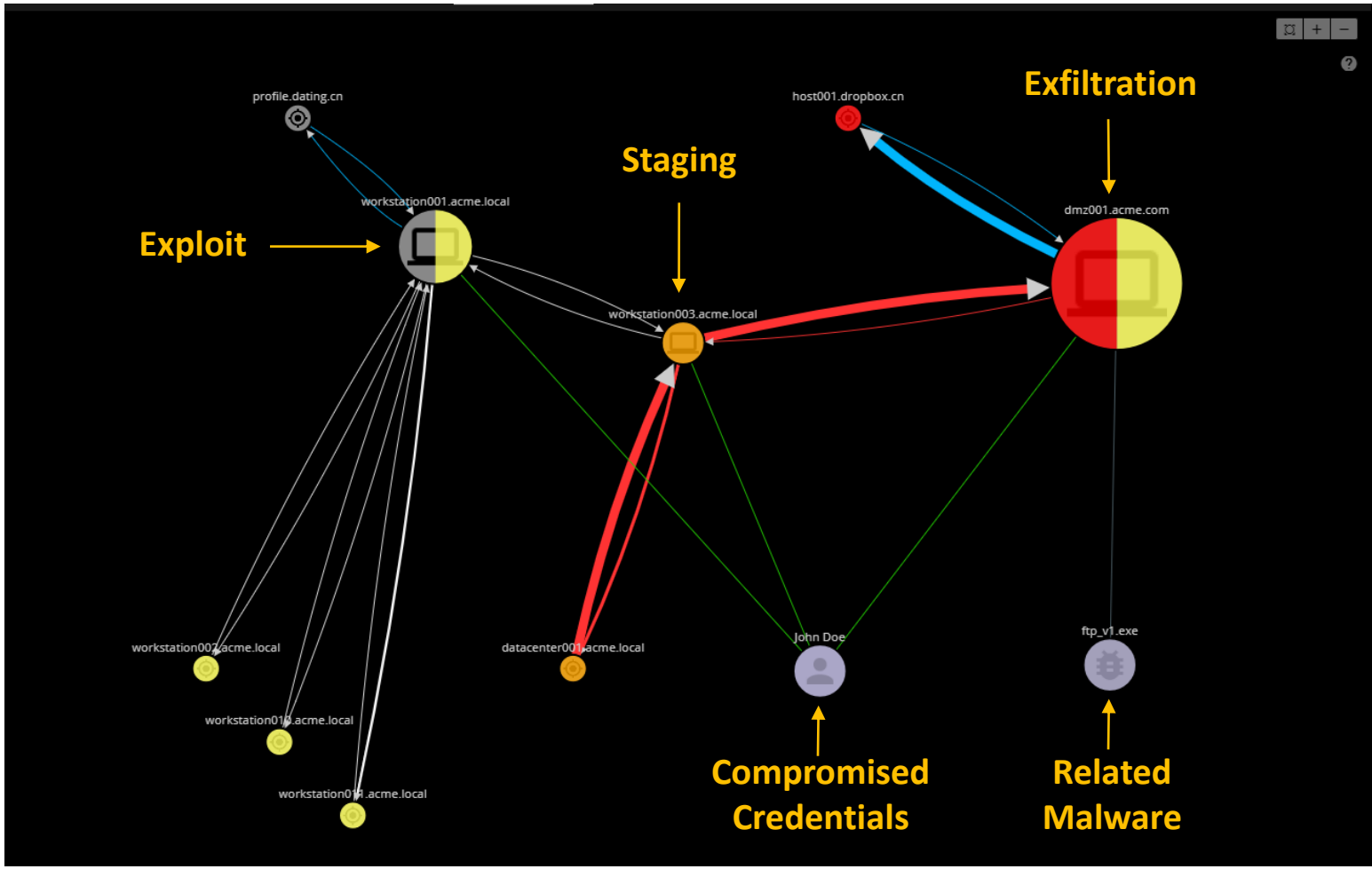
Object Oriented Organization



Artifacts
• ClientName: ClientA • ClientIP: 10.10.10.43 • ClientMAC: 00-DC-EF-23-15-12 • Product: MS DHCP • MessageType: DHCP Lease • Intent: Asset Info
• ClientName: ClientA • User: User1 • File: FileZ • Product: Crowdstrike Falcon • MessageType: Malware Detected • Intent: Exploit Detection
• ClientIP: 10.10.10.43 • ServerName: ServerB • Product: Cisco Firepower • MessageType: C2 Detected • Intent: C2 Detection

Graph vs. Crime Theory

- Meaningful Graph Relationships
- Modus Operandi of Attacker
- Combines, standardizes diverse data
- Hierarchical JSON
- *SECOPS & LE* ***Unit of Work***



Power of JSON

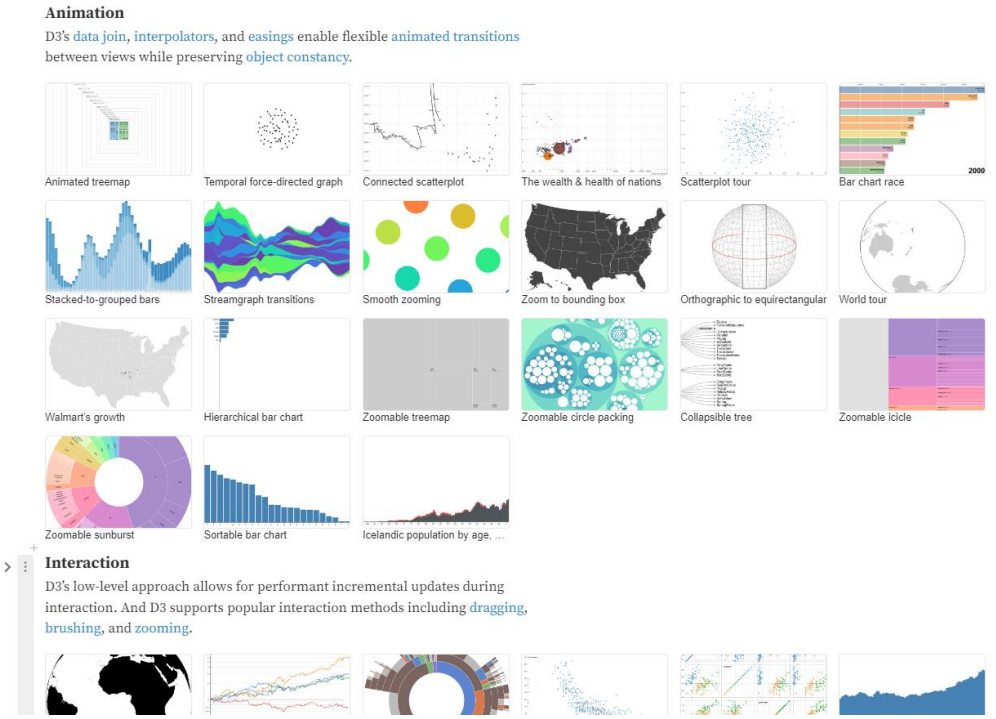
- High Compression (net & disk)
- REST Powered Transmission
- Easy to Hash & Version
- Hierarchical Structures

Incident JSON View


```
id: "53ba6ed0-ed35-11ed-8a89-053651253e65"
partition: "53babcf0-ed35-11ed-8a89-053651253e65"
nodes: Object {"52801a10-ed35-11ed-8a89-053651253e65":{"id":"52801a10-ed35-11ed-8a89-053651253e65","partition":"53b89a10-ed35-11ed-8a89-0536512
  52801a10-ed35-11ed-8a89-053651253e65: Object {"id":"52801a10-ed35-11ed-8a89-053651253e65","partition":"53b89a10-ed35-11ed-8a89-053651253e65"
    id: "52801a10-ed35-11ed-8a89-053651253e65"
    partition: "53b89a10-ed35-11ed-8a89-053651253e65"
    ip_address: "10.10.10.3"
    ip: "10.10.10.3"
    org: ""
    orgId: 1
    mac: ""
    guid: ""
    internal: true
```

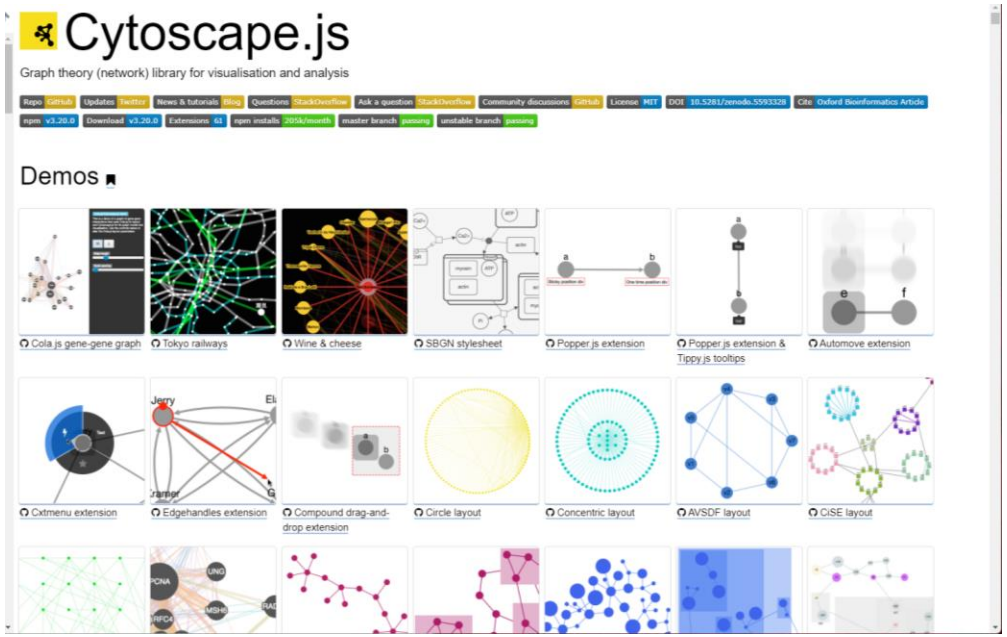
JSON Visualization - d3js

- MIT License
- JSON Data
- Dozens of easy JSON to chart visualizations

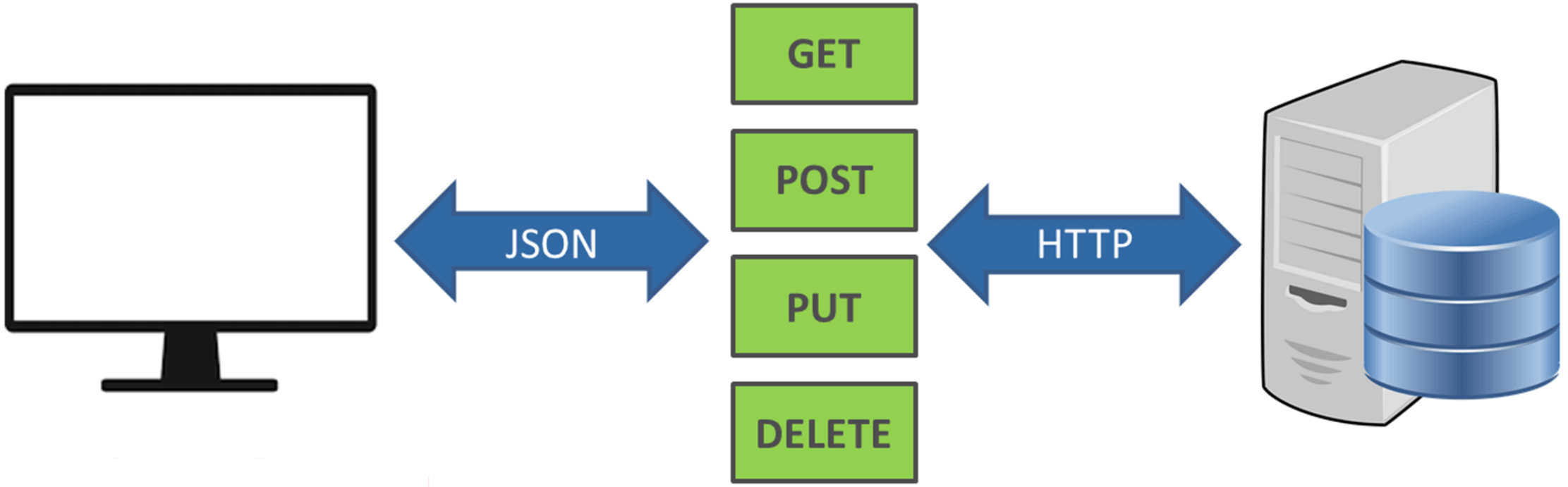


JSON Graph Visualization - Cytoscape.js

- MIT License
- JSON Data
- Graph Relationship interaction
- Bioinformatic Research



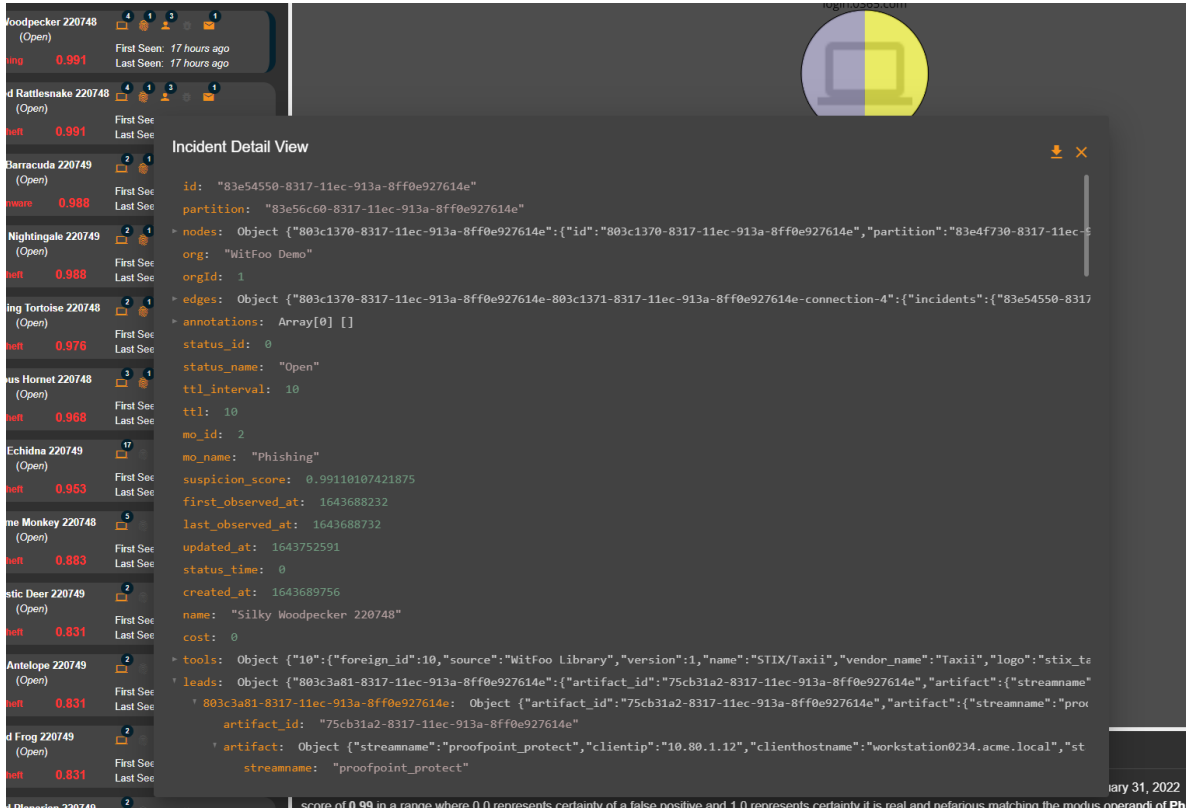
REST Basics



Client sends a **request**

HTTP methods

Server sends a **response**



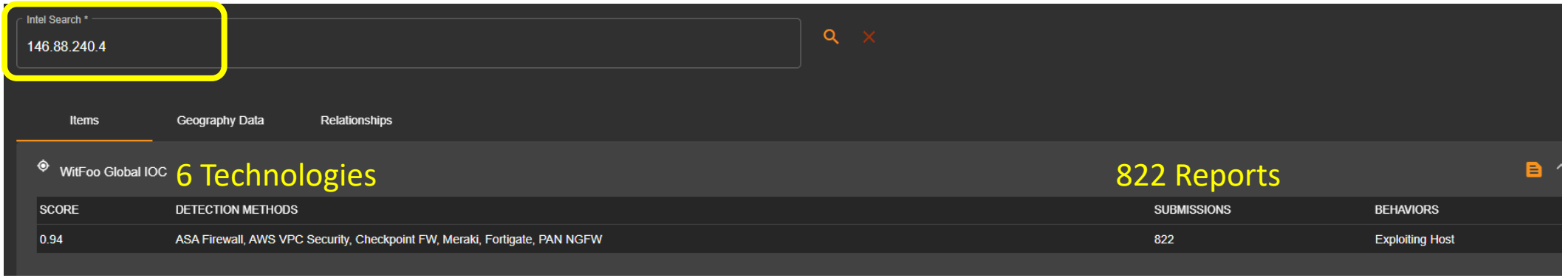
Package All Data – “Murderbook”

JSON Sharable Objects

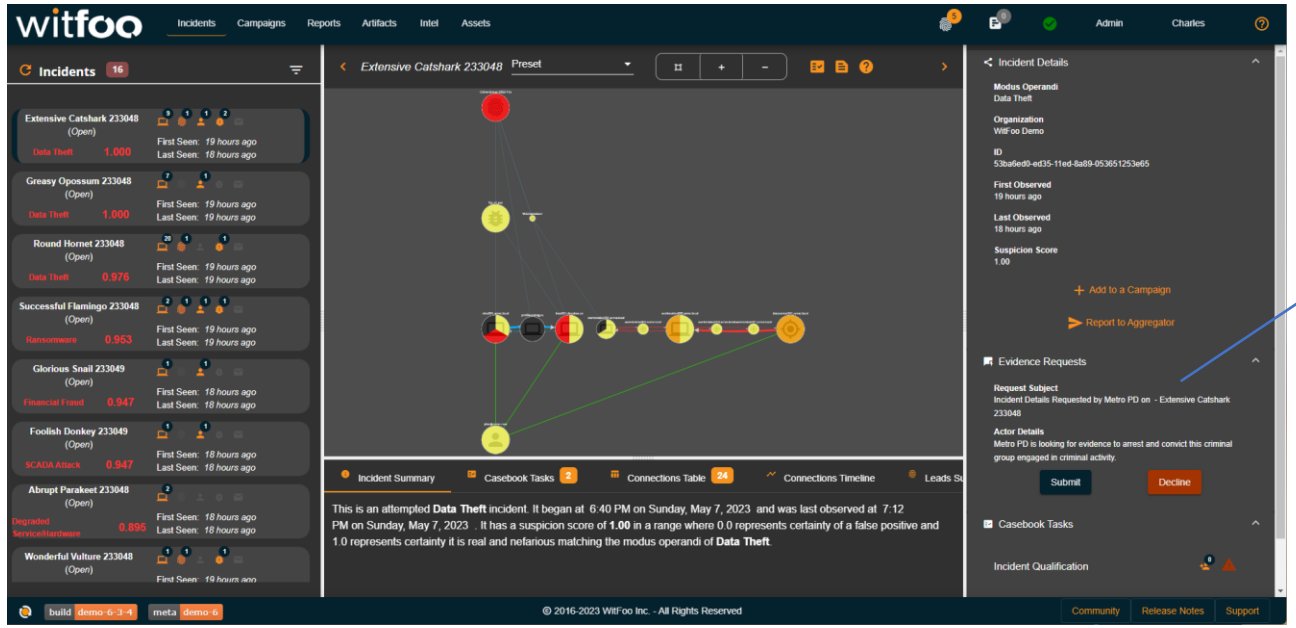
- Incident Collections
- Threat Intel
- Bulletins
- Job Execution
- Reports

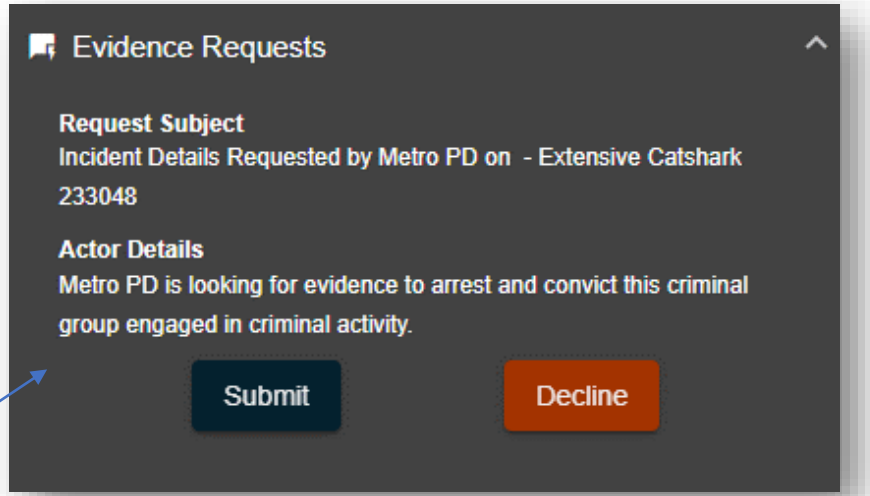
Anonymous Tips

- Automatically & Anonymously Submitted Across CyberGrid
- Corroboration types: Technology & Victims

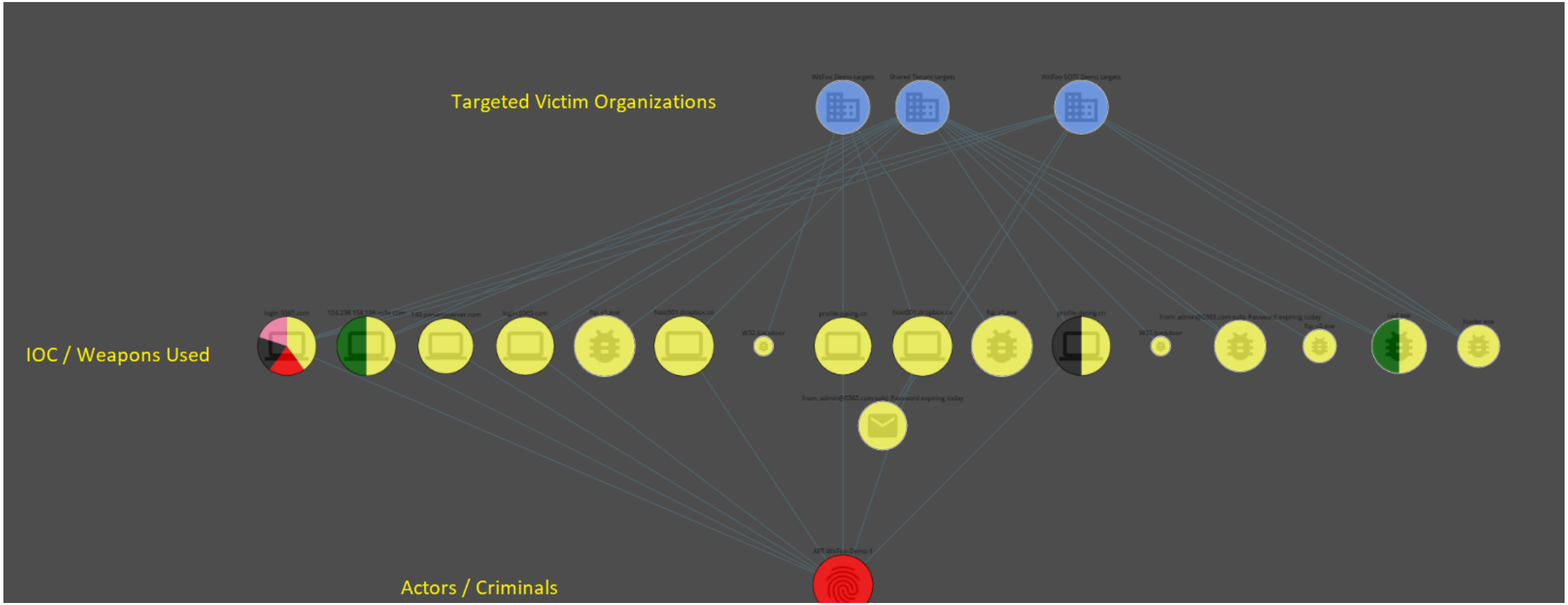


Law Enforcement Requests



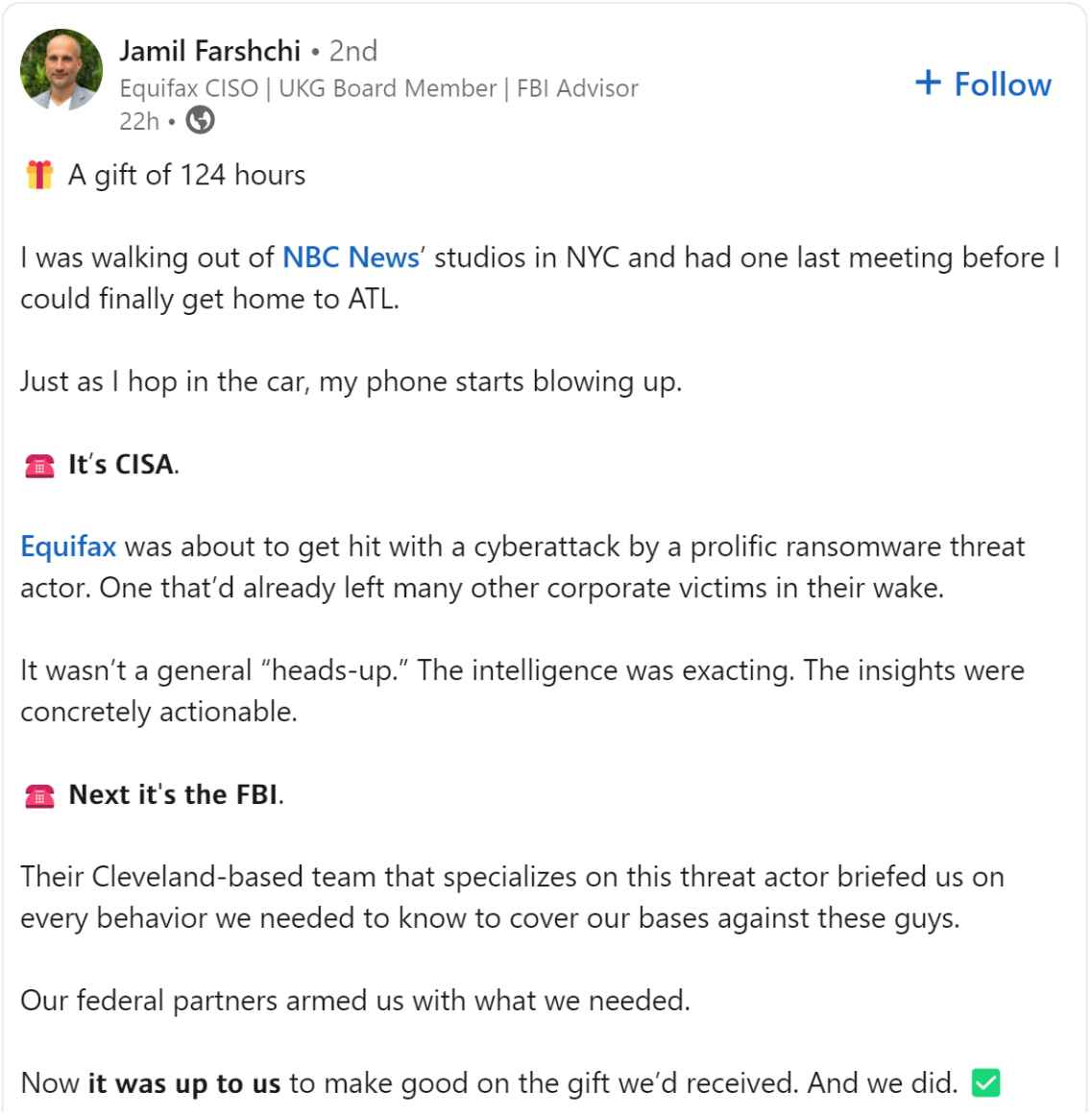


Incidents to Campaigns



Law Enforcement Resources

- Infragard
  - FBI and Private Critical Infrastructure
- Cyber Fraud Task Forces
  - Secret Service on Financial Fraud
- IC3
  - FBI Cybercrime Reporting
- CISA Critical Infrastructure Areas



Jamil Farshchi • 2nd
Equifax CISO | UKG Board Member | FBI Advisor
22h •

+ Follow

🎁 A gift of 124 hours

I was walking out of NBC News' studios in NYC and had one last meeting before I could finally get home to ATL.

Just as I hop in the car, my phone starts blowing up.

☎️ **It's CISA.**

Equifax was about to get hit with a cyberattack by a prolific ransomware threat actor. One that'd already left many other corporate victims in their wake.

It wasn't a general "heads-up." The intelligence was exacting. The insights were concretely actionable.

☎️ **Next it's the FBI.**

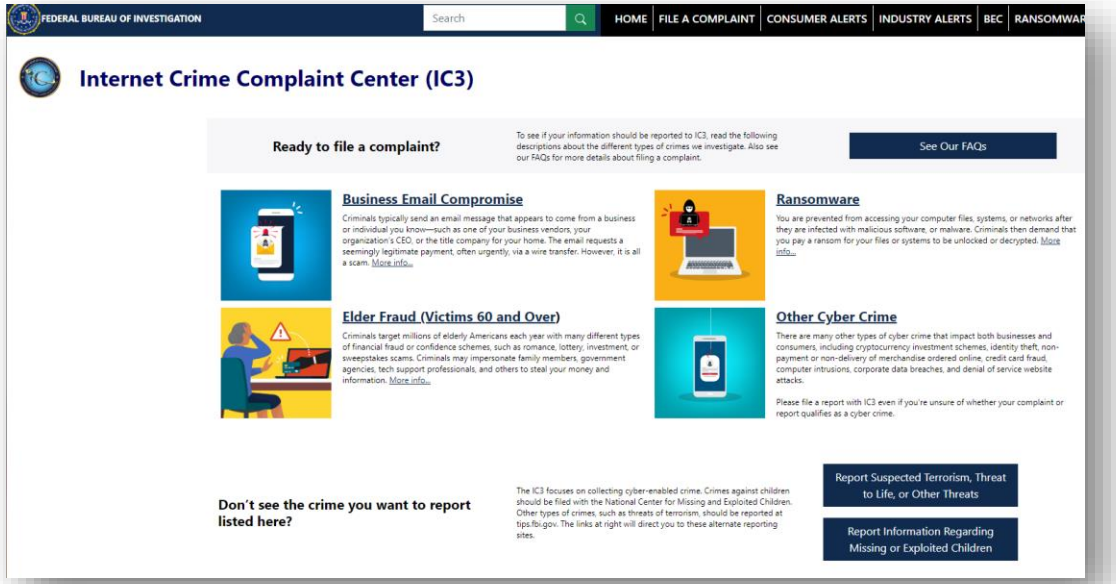
Their Cleveland-based team that specializes on this threat actor briefed us on every behavior we needed to know to cover our bases against these guys.

Our federal partners armed us with what we needed.

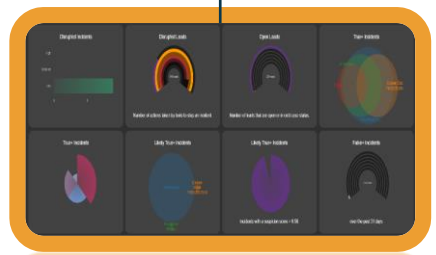
Now **it was up to us** to make good on the gift we'd received. And we did. ✅

Transmitting to Law Enforcement

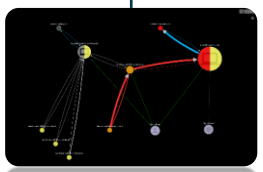
Manual or Automatic



https://IC3.gov



Law.WitFooCloud.com



"Powered by WitFoo" Technology

“Powered by WitFoo” Resources

vmware
Hyper-V
ubuntu
amazon web services
Microsoft Azure
Google Cloud
cyrvant
RIMSTORM
rogos
ardalyst

witfoo
PRECINCT
Certified User

- Free Training on WitFoo Community
- Free Educational Licensing
- Free Licensing to US Law Enforcement
- Free RaspberryPi4 (WitFooPi) licensing for training
- www.WitFoo.com or Charles@WitFoo.com