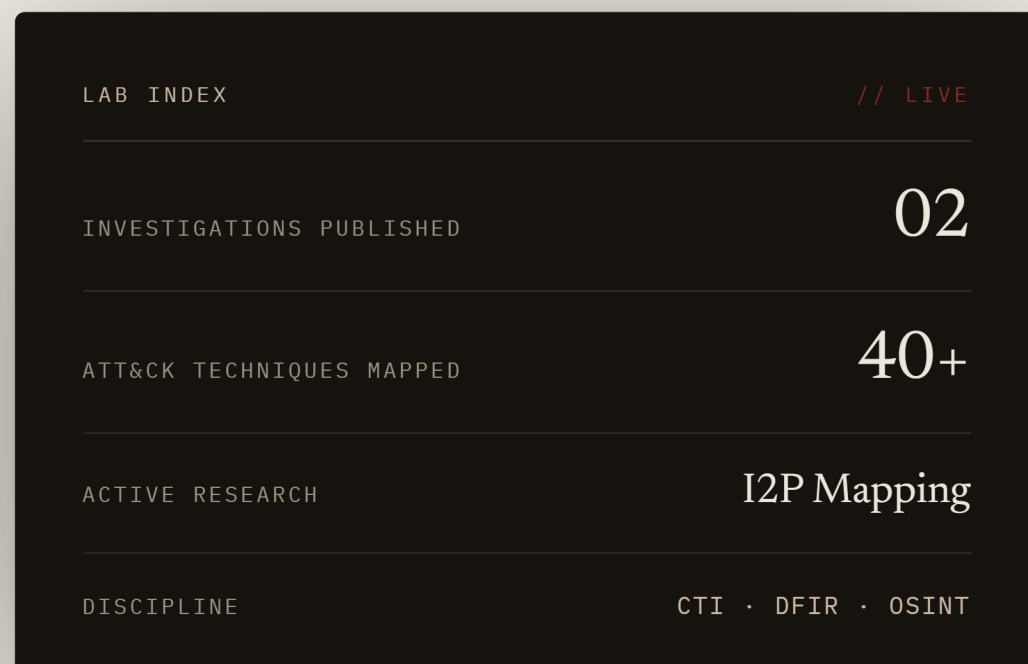


# Tracking adversaries. Hunting threats. Producing actionable intelligence.

I'm Joshua Berkoh — a cybersecurity professional and PhD researcher in threat investigations, threat hunting, and dark-web intelligence. I reconstruct intrusion activity, map tradecraft to MITRE ATT&CK, and turn raw telemetry into clear, defensible intelligence.

[View investigations](#) [Read research](#) [Download résumé](#)

MITRE ATT&CK KQL OSINT IOC Pivoting Python  
Graph Analysis



## 01 — CAPABILITIES

### What I do

Demonstrated competencies across the intelligence cycle — collection, analysis, and reporting — grounded in completed investigative and research work.

|                                                                                                                                                                                                                       |                                                                                                                                                                                      |                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>01</b> <span>INTEL CYCLE</span></p> <p><b>Cyber Threat Intelligence</b></p> <p>Collect, analyze, and report structured intelligence on threat activity, tradecraft, indicators, and investigative findings.</p> | <p><b>02</b> <span>KQL · ATTACK</span></p> <p><b>Threat Hunting</b></p> <p>Hypothesis-driven hunts across endpoint and network telemetry using KQL and the ATT&amp;CK framework.</p> | <p><b>03</b> <span>DFIR</span></p> <p><b>Threat Investigations</b></p> <p>End-to-end intrusion reconstruction — timelines, evidence, IOCs, and defensible assessments.</p> |
| <p><b>04</b> <span>I2P · TOR</span></p> <p><b>Dark-Web Intelligence</b></p> <p>Research into anonymity networks, hidden services, and underground infrastructure.</p>                                                 | <p><b>05</b> <span>SATS</span></p> <p><b>Intelligence Research</b></p> <p>Structured analytic methods, source evaluation, and confidence-based judgments.</p>                        | <p><b>06</b> <span>METHOD</span></p> <p><b>Security Research</b></p> <p>Tooling, measurement, and methodology that extend how threats are studied.</p>                     |

## 02 — INVESTIGATIONS

### Featured investigations

Threat-investigation case studies: full intrusion reconstructions with timelines, IOC analysis, and MITRE ATT&CK mapping — developed from KC7 scenarios and written to professional intelligence-reporting standards.

CASE-2026-001 INSIDER THREAT · ACTIVE DIRECTORY · RANSOMWARE

**Inside Encryptodera: An Insider Threat Scenario**

14 TECHNIQUES 27d SWELL TIME

[READ INVESTIGATION](#)

A dual-track insider-threat investigation at Encryptodera Financial: a contractor's 27-day FTP exfiltration of cold-storage wallet secrets running in parallel with a hijacked-identity intrusion that escalates to ransomware.

CASE-2026-002 CRITICAL INFRASTRUCTURE · SUPPLY CHAIN · ICS

**Solvi Systems: A Tale of Supply Chains and ICS**

18 TECHNIQUES ICS DOMAIN

[READ INVESTIGATION](#)

Triaging a complex supply-chain intrusion targeting regional energy distribution — from perimeter XSS probing and weaponized phishing documents to lateral movement and source-code compromise.

CASE-2026-003 APT CAMPAIGN · INFRASTRUCTURE TRACKING

**Valdoria Votes: Advanced Persistent Threat Analysis**

IN PROGRESS COMING SOON

Investigating a high-stakes, state-sponsored campaign targeting election infrastructure — attacker persistence, multi-hop C2 structures, and domain-registrar anomalies.

## 03 — RESEARCH

### Current research — dark-web intelligence

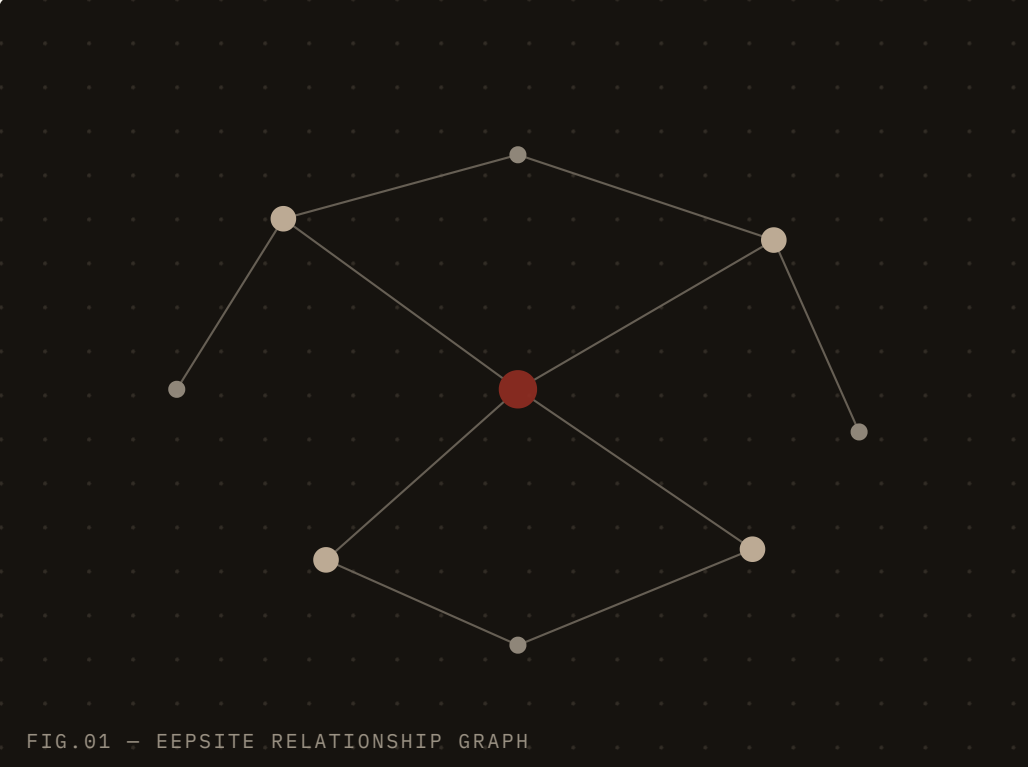
#### Mapping the I2P anonymous network

A cross-layer framework that fuses network-layer routing data with application-layer hidden-service ("beepsite") crawls into a single graph — making it possible to study anonymity infrastructure and the services riding on it as one connected ecosystem.

The work spans hidden-service discovery, infrastructure mapping, large-scale collection, and graph analysis.

Hidden-Service Discovery Infrastructure Mapping Graph Analysis

[EXPLORE THE RESEARCH](#)



## 04 — LAB ACTIVITY

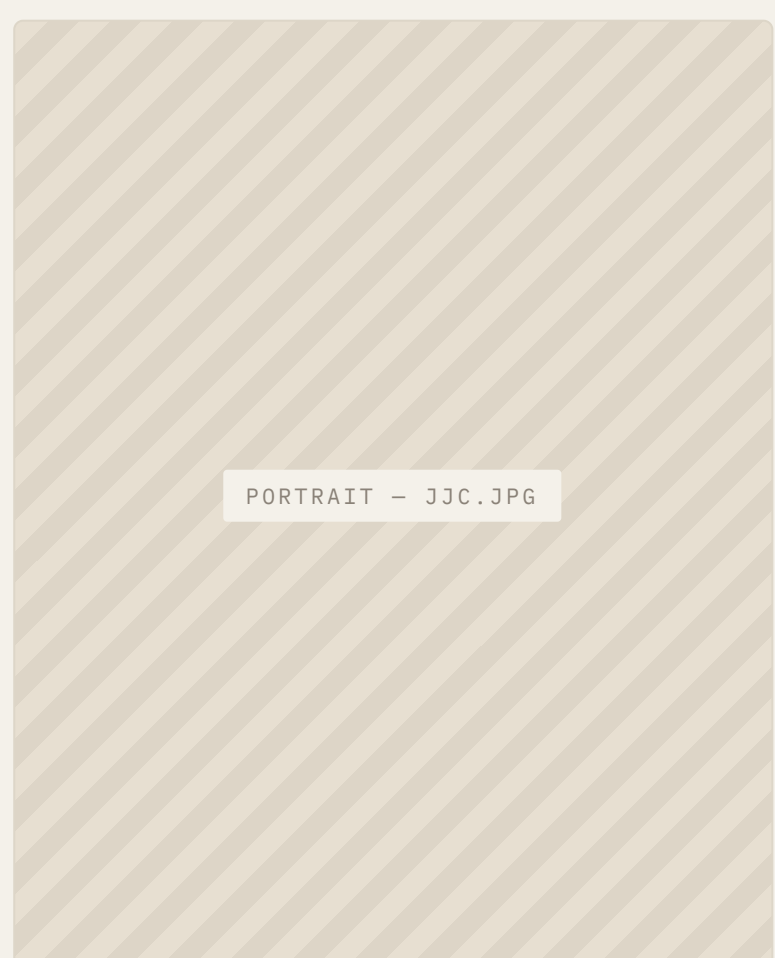
### Recent intelligence activity

#### CURRENTLY WORKING ON

|                                                                                                                                                                                                                          |                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>I2P Hidden Service Ecosystem Analysis</b> <span>IN PROGRESS</span></p> <p>PhD research on hidden-service discovery, application-layer crawling, infrastructure mapping, and graph-based relationship analysis.</p> | <p><b>KC7 Cyber Investigation Portfolio</b> <span>IN PROGRESS</span></p> <p>Public portfolio of scenario-based investigations — evidence analysis, KQL, IOC pivoting, ATT&amp;CK mapping, and structured reporting.</p> |
| <p><b>Practical Detection Engineering</b> <span>IN DEV</span></p> <p>Studying detection workflows; published only once rules and validation reports are complete and defensible.</p>                                     | <p><b>CTI Research &amp; Writing</b> <span>IN PROGRESS</span></p> <p>Public-facing investigation reports, research notes, and technical articles documenting analytical reasoning.</p>                                  |

#### TIMELINE

|         |                                        |             |
|---------|----------------------------------------|-------------|
| 2026    | Cyber Threat Intelligence Lab rebrand  | IN PROGRESS |
| 2026    | Inside Encryptodera investigation      | COMPLETED   |
| 2026    | Solvi Systems / Operation DockShock    | COMPLETED   |
| 2026    | Valdoria Votes investigation           | IN PROGRESS |
| 2026    | I2P Hidden Service Ecosystem Analysis  | IN PROGRESS |
| 2026    | Malware Reversing Lab environment      | COMPLETED   |
| 2025–   | PhD Research in Information Technology | IN PROGRESS |
| 2023    | Security Engineer Internship - Intuit  | COMPLETED   |
| 2021–22 | Security Operations Center Analyst     | COMPLETED   |



## 05 — ABOUT

### Researcher & threat investigator

I'm a PhD researcher in Information Technology and a practicing security professional. My work sits where intelligence analysis meets hands-on investigation: reconstructing intrusions, hunting adversary activity in telemetry, and researching the infrastructure that threats rely on.

I write every investigation to be defensible — evidence-first, mapped to MITRE ATT&CK, and honest about confidence. Detection engineering is an area I'm actively studying and will publish as the work matures.

|                                                                |                                                              |
|----------------------------------------------------------------|--------------------------------------------------------------|
| <p><b>SOC Analyst</b></p> <p>FINANCIAL SECTOR · 2021–22</p>    | <p><b>Security Engineer Intern</b></p> <p>ENVI · 2023</p>    |
| <p><b>Bug-Bounty Hall of Fame</b></p> <p>MULTIPLE PROGRAMS</p> | <p><b>PhD Researcher</b></p> <p>INFORMATION TECH · 2025–</p> |

## 06 — CONTACT

### Open to threat intelligence work

If your team works in cyber threat intelligence, threat hunting, or security research, I'd welcome a conversation.

LINKEDIN [Joshua Berkoh](#)

GITHUB [@joshberk](#)

RÉSUMÉ [View / download CV](#)