CYBER THREAT INTELLIGENCE · THREAT HUNTING · DARK-WEB RESEARCH

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

LAB INDEX // LIVE

INVESTIGATIONS PUBLISHED	02
ATTACK TECHNIQUES MAPPED	40+
ACTIVE RESEARCH	I2P Mapping
DISCIPLINE	CTI · DFIR · OSINT

01 — CAPABILITIES

What I do

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

01 · INTEL CYCLE
Cyber Threat Intelligence
Collect, analyze, and report structured intelligence on threat activity, tradecraft, indicators, and investigative findings.

02 · KQL — ATT&CK
Threat Hunting
Hypothesis-driven hunts across endpoint and network telemetry using KQL and the ATT&CK framework.

03 · DFIR
Threat Investigations
End-to-end intrusion reconstruction — timelines, evidence, IOCs, and defensible assessments.

04 · I2P · TOR
Dark-Web Intelligence
Research into anonymity networks, hidden services, and underground infrastructure.

05 · SATS
Intelligence Research
Structured analytic methods, source evaluation, and confidence-based judgments.

06 · METHOD
Security Research
Tooling, measurement, and methodology that extend how threats are studied.

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

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.

14 TECHNIQUES · 27d DWELL TIME

READ INVESTIGATION →

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

Solvi Systems: A Tale of Supply Chains and ICS

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.

18 TECHNIQUES · ICS DOMAIN

READ INVESTIGATION →

CASE-2026-003 · APT CAMPAIGN · INFRASTRUCTURE TRACKING

Valdoria Votes: Advanced Persistent Threat Analysis

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

◐ IN PROGRESS — COMING SOON

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 ("eepsite") 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 →

FIG. 01 — EEPSITE RELATIONSHIP GRAPH

04 — LAB ACTIVITY

Recent intelligence activity

◐ CURRENTLY WORKING ON

I2P Hidden Service Ecosystem Analysis — IN PROGRESS
PhD research on hidden-service discovery, application-layer crawling, infrastructure mapping, and graph-based relationship analysis.

KC7 Cyber Investigation Portfolio — IN PROGRESS
Public portfolio of scenario-based investigations — evidence analysis, KQL, IOC pivoting, ATT&CK mapping, and structured reporting.

Practical Detection Engineering — IN DEV
Studying detection workflows; published only once rules and validation reports are complete and defensible.

CTI Research & Writing — IN PROGRESS
Public-facing investigation reports, research notes, and technical articles documenting analytical reasoning.

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

PORTRAIT — 32C.JPG

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.

SOC Analyst — FINANCIAL SECTOR · 2021–22

Security Engineer Intern — INTUIT · 2023

Bug-Bounty Hall of Fame — MULTIPLE PROGRAMS

PhD Researcher — INFORMATION TECH · 2025–

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 ↗
RESUMÉ	View / download CV →