

Luke Johnson

Threat Hunter & Purple Team / Active Defense Engineer

Fort Worth, TX | luke@cyberresearch.us

linkedin.com/in/the-luke-johnson | github.com/cyberresearch-us | credly.com/users/-lukej-/badges | luke.cyberresearch.us

PROFESSIONAL SUMMARY

Security engineer with 9+ years across threat hunting, detection engineering, and incident response, focused on purple teaming and active defense. I emulate adversary TTPs in controlled environments to measure detection efficacy, close coverage gaps, and ship ATT&CK-mapped detections—turning attacker behavior into measurable defensive improvements. Incident-commander experience brings an assumed-breach mindset. Seeking Active Defense / Purple Team roles where emulation-driven validation strengthens detection and response.

CORE SKILLS

Adversary emulation & purple team · MITRE ATT&CK (emulation plans, Navigator) · Detection engineering (Sigma, Splunk SPL; YARA-L drafts for MSSP) · Detection validation & gap analysis · Threat hunting · Incident response / incident command · SIEM (Splunk admin & SPL; QRadar/QRoC; Google SecOps / Chronicle — UDM hunt & cases) · EDR (SentinelOne, Trend Vision One, Defender, Huntress) · Threat intelligence & IOC enrichment · Host IR / artifact analysis (Aftermath, ESFPlayground, MonitorUI; EnCase, Autopsy, LogMD) · PCAP / network analysis · Cyber deception (honeypots, canaries) · SOAR (Cortex XSOAR / Demisto — Mosaic era; not XSIAM) · NGFW (Palo Alto Networks — Mosaic era) · AWS security (GuardDuty, CloudTrail, Athena) · Scripting — Python, Bash, PowerShell (familiar)

PROFESSIONAL EXPERIENCE

Staff Pro-Active Threat Hunter & Detection Engineer — Undisclosed

Remote | Oct 2022 – Present

- Run purple team and adversary-emulation exercises across cloud and on-premises environments—researching attacker TTPs, emulating them in controlled windows, and measuring whether they are prevented, logged, or alerted to validate and improve detection coverage.
- Plan and execute structured, hypothesis-driven threat hunts using MITRE ATT&CK across SIEM, EDR, and cloud telemetry to surface activity consistent with sophisticated attacker methodologies and close visibility gaps.
- Investigate and hunt in Google SecOps (UDM search, cases/alerts, retrohunt) alongside daily Splunk SPL investigations; keep PII/fraud work in Splunk; draft YARA-L/detection logic for the MSSP SOC to deploy.
- Splunk administrator: onboard log sources, write/fix parsers and knowledge objects, and track log-source count, collection rate, parse issues, and platform health; author SPL correlation and detections.
- Author vendor-agnostic detection-as-code (YAML/Sigma) with Splunk as the mature implementation path and additional SIEM/IR targets in the catalog; validate against emulated techniques; ship campaign-aware rules for supply-chain and credential-abuse activity.
- Lead cloud IR using CloudTrail, Athena, and SSM; take EBS snapshots for a retained IR firm; reconstruct IAM/CI credential abuse and contain by rotating implicated keys and tightening IMDS/aws-auth controls.
- Lead incident response as incident commander in cloud and hybrid environments; drive intrusion and root-cause analysis and convert findings into new detections.
- Host IR on Windows, macOS, and VMware Horizon: collect/analyze with Aftermath and Mitten Mac tooling (ESFPlayground, MonitorUI), plus Huntress/EDR and logs for persistence — not enterprise DF platforms (Magnet/Cellebrite/Recon).
- Built and continue to operate a multi-source alert-triage and IOC-enrichment pipeline that informs emulation prioritization and feeds attacker-behavior context into detections and hunts.
- Built and operate an internal attack-surface / network-reconnaissance monitoring program to identify external exposure and prioritize remediation.
- Promoted to Staff (Jan 2025) for closing security gaps with engineering solutions; mentor junior analysts and brief technical and non-technical stakeholders with fact-based, BLUF findings.

Cyber Security Consultant — PacketWatch

Remote | Nov 2020 – Oct 2022

- Developed structured threat hunts from active threat intelligence aligned to the cyber kill chain—external exposure, lateral movement, and data exfiltration on clients' existing SIEM and EDR stacks.
- Delivered managed detection and response: continuous monitoring, daily threat hunting, and verification of anomalous activity across client networks.
- Built detections from TTPs and client-relevant threat intelligence; reviewed findings with stakeholders and implemented preventive controls.

- Led incident response using EDR and network evidence; performed threat and intrusion analysis and remediation planning with client teams.

Security Operations Engineer — PayPal

San Jose, CA | Jul 2019 – Nov 2020

- Participated in incident response; investigated malware, intrusion, brute-force, and denial-of-service activity to determine scope.
- Partnered with the bug-bounty program to recreate exploits, extract IOCs, and implement mitigations (rate limiting, WAF policies, correlation rules).
- Reviewed abuse patterns against API endpoints and developed mitigation strategies with business units to close security gaps.

Sr. Cyber Security Analyst — Mosaic451 (MSSP)

Remote | Sep 2017 – Jul 2019

- Investigated security events across Splunk, QRadar/QRoC, FortiSIEM, McAfee ESM, and ELK; added log sources and parsers to the existing QRoC and tuned SIEM correlation rules.
- Used Palo Alto NGFW telemetry and Cortex XSOAR (then Demisto) to build detections and IR playbooks — case create/assign workflows with other tools (investigation/response automation, not Cortex XSIAM).
- Curated threat-intelligence IOC lists (IP, hash, domain) and built IDS/IPS and SIEM detection content from threat data.
- Performed malware triage with EnCase, Autopsy, and LogMD; correlated Nessus/Nexpose vulnerability data during investigations.
- Conducted network traffic and PCAP analysis with Wireshark; authored regex parsing logic for QRadar and Splunk log ingestion.

Information Security Operations Analyst — University of Phoenix (Apollo Education Group)

Phoenix, AZ | Oct 2016 – Sep 2017

- Developed Splunk detections for escalated privileges and deception (“honey”) profiles; performed threat modeling and use-case development.
- Tuned McAfee SIEM products (ESM, ePO, DLP, MWG); implemented Check Point firewall and web-proxy changes; monitored and responded to security events.

SELECTED PROJECTS

- **Multi-Source Alert Triage Platform:** Internal platform: ingest cloud/exposure findings, normalize events, enrich with TI sources and attribution, apply YAML disposition (FP/BTP/TP), automate SOC triage with close-loop updates.
- **IOC Enrichment Platform:** Pluggable TI enrichment (VirusTotal, Shodan, GreyNoise, AbuseIPDB, OTX, ThreatFox, and others) with parallel execution and caching — reused across exposure scans, triage, and investigations.
- **Detection Engineering Catalog:** Vendor-agnostic detection-as-code catalog (YAML + Sigma) mapped to MITRE ATT&CK — CloudTrail, GuardDuty, Linux audit, DNS, and multi-source correlation — with Splunk implementations and additional SIEM/IR targets; campaign-aware rules.
- **CloudTrail Threat Hunting (Athena):** Athena hunt library and MITRE-mapped hunt catalog; Python orchestrator for multi-account, date-bounded hunts with structured output for SOAR.
- **Security Platform & SOC Program:** Multi-repository security automation unifying triage, enrichment, detection-as-code, and hunting for day-to-day SOC work; program docs cover IR gap analysis, log-source inventory, and ATT&CK coverage.

CERTIFICATIONS

- CompTIA Security+ — CompTIA (2015)
- CompTIA CySA+ — CompTIA (2018)
- Systems Security Certified Practitioner (SSCP) — (ISC)² (2016)
- eLearnSecurity Junior Penetration Tester (eJPT) — INE Security (2022)
- SentinelOne Incident Response — SentinelOne (2021)

Verify: credly.com/users/-lukej-/badges

EDUCATION

B.S. Information Technology, Concentration in Information Systems Security — University of Phoenix (2011)