Joseph Autorino

CSN 190

Professor Edwin Reed Sanchez

10/14/25

## 4.1 Feasibility Assessment and Final Topic Decision

In Operational security there are many skills needed in the field such as threat modelling and risk management. Using tools such as MITRE ATT&CK, STRIDE/DREAD, risk matrices, spreadsheets, OWASP Threat Dragon. Endpoint protection and hardening tools like CrowdStrike, Defender for Endpoint, HIPS, disk encryption, app whitelisting, OS baselines. This stops detects and contains endpoint compromise. Network security and segmentation skills are important using such tools like firewalls, VLANs, egress filtering, SDN controls IDS/IPS packet capture tcpdump and Wireshark. This limits lateral movement and reveals C2/abuse. Logging, detection and SIEM using tools such as ELK/Wazuh, Splunk, Chronicle, OSQuery, Fluentd/Vector, SIEM rules, correlation logic. Used for Centralized visibility and detections and ability to find intrusions early. Incident response and forensics are skills needed with such tools as Volatility, Autopsy/FTK Imager, Redline, FTK, X Ways, chain of custody practice. To triage preserve evidence and recover with confidence. Also threat hunting and intel operationalization is commenced using tools like MISP, YARA, Sigma rules, threat feeds, OpenCTI, hunting notebooks. For proactive detection to find what automated rules miss. Web browser and supply chain security using tools such as CSP, SRI, Subresource integrity, Secure build pipelines, SCA runtime, sandboxing for third party JS/ad supply chain is a massive attack vector. Cloud and container security is a must. Such tools that are needed is Cloud IAM, CloudTrail/CloudWatch/Stackdriver, K8s RBAC, kube-bench, runtime security, IaC scanning. This is necessary because the cloud is where most infra lives now different patterns, same adversary. Offensive fundamentals for defenders using tools like Nmap, Burp, Metasploit, BloodHound CTF platforms to think like attackers and harden accordingly. Secure communications and OPSEC tradecraft using tools like Signal, GPG, WireGuard, compartmentalized VMs, password managers protect sensitive investigation data and personal identity leakage. Automation and tooling skills using tools like Python, PowerShell, Bash, Terraform, Ansible, CI/CD GitHub Actions. Why because app layer vulnerabilities are often exploited for footholds. Legal, compliance and policy awareness using tools like NIST, GDPR/CIPP basics, IR playbooks, notification processes. You must operate within legal contractual boundaries during incidents.

Prioritize starter toolset minimum viable OpSec kit using visibility, Network, Endpoint, IR/Forensics, Hunting/Intel and Automation.

The reason why this is achieving yet challenging is because the tools, playbooks, standards and training exist but pulling them together keeping everything working scale, people, legacy systems, evolving attackers, and budget/legal limits. You can do it but it takes sustained effort, priorities and trade off. This is meaningful to me because it is in the field of something I enjoy doing and fun. This balances well with growth because it challenges you to think and evolve in your thought process.

Why it's achievable mature tooling and frameworks open source and a commercial tools, plenty of learning paths and labs with hands on training, docs, templets, community play books. Repeatable processes IR playbooks, detection engineering, laC, and automation. Incremental wins possible. You can prioritize high impact controls and see measurable results quickly.

Why it's challenging is complexity and heterogeneity like networks, cloud legacy systems, and IoT create a messy attack surface one size defense don't fit. Evolving adversaries such as attackers adapt new malware, obfuscation, P2P C2, supply chain attacks. Detection rules age quickly. Human factor such as misconfiguration, weak passwords, and phishing remain primary failure points. Training and culture change are slow. Scale and noise at enterprise scale, telemetry volume explodes, tuning to reduce false positives while catching real threats is hard. Resource constraints skilled people, budget for tooling, and access to production telemetry are limited for many orgs. Legal/organizational friction such as evidence collection, privacy laws and coordination across teams/legal slow detection and response. Legacy debt and operational risk replacing or isolating old systems is costly and risky so compromises remain.

Ambitious goal would be to achieve an operationally mature detection and response capability for your environment that reliably detects and contains advanced threats and demonstrates measurable improvement in metrics.

Realistic Target is to create reliable visibility and triage capability and one validated detection and one IR playbook.

Minimum viable outcome is to demonstrate basic visibility and the ability to perform a decisive triage on a suspicious host.

What skills you'll develop is visibility and telemtry engineering learning skills like Sysmon/osquery, log collection, log parsing, shipping to ELK/Wazuh. Detection engineering writing Sigma/ELK/Splunk queries, suricata/Zeek rules, tuning alerts to reduce noise. Network monitoring and packet analysis learning Zeek/Suricata basics, reading pcaps, using tcpdump/Wireshark. Incident response and forensics isolation, evidence capture basic volatility plugins, chain-of-custody basics. Automation and scripting with PowerShell/Python scripts to automate log parsing, evidence collection and simple triage.

Detection validation and tabletop exercises running drills red and purple team basics measuring MTTD/MTTR. Threat modeling and prioritization use ATT&CK to map threats prioritize controls by impact and likelihood. Communication and reporting clear IR reporting evidence packaging stakeholder communication. Cloud and container basics cloud logs IAM hygiene, basic k8s observability.

This is valuable progress is compounding and every small win makes later tasks faster and safer. Tools, configs, and scripts and build are reusable. You create demonstrable artifacts working detection, a pcap a volatility report on an IR playbook are concrete proof of ability and great for a resume. Risk reduction now not later even partial deployment closes high impact gaps. You learn decision-making under constraints as security is about trade offs. Attempting the project trains you to prioritize high-impact actions with limited time ans budget. You accelerate learning through feedback drills and real tests reveal real world assumptions and teach faster theory than alone.