Justin Walters

Security practitioner - DFIR, incident response, threat intelligence

verdantpro@proton.me | github.com/verdantpro | linkedin.com/in/justin-walters-36a579256 | verdantprotocol.com

Hands-on security practitioner experienced in incident response and digital forensics across 30+ ransomware and BEC engagements as a primary responder. Root-cause analysis from EDR telemetry, logs, and forensic artifacts; remediation across Windows and Linux. SIEM (Splunk, Zeek), malware analysis, threat hunting, MITRE ATT&CK; Python/Bash automation; federal continuous monitoring (CMS / FISMA).

EXPERIENCE

Ransomware Recovery Consulting Specialist - Halcyon.ai

July 2024 - March 2026

- Primary responder on 30+ ransomware and BEC intrusions; RCA from EDR, logs, and forensic artifacts (Windows/Linux).
- Malware analysis (Any.run, VirusTotal); M365/Azure compromise investigations; TLSH + MITRE ATT&CK correlation.
- Velociraptor on 700+ endpoints; Timesketch IR infrastructure; Python automation; counsel/insurance coordination.

Security Engineer - ECS Federal (supporting CMS)

February 2023 - July 2024

- Splunk SIEM and Gurucul GRA UEBA in FISMA / NIST 800-53 environment; Ansible hardening and patching.
- Primary engineer for Gurucul GRA at CMS; Splunk server admin; stakeholder communication under change pressure.

Implementation Engineer - DataBank

March 2020 - February 2023

- Cisco ASAv, VMware, VLANs; ASA + Duo + AD for AnyConnect; migrations; Cloudflare API scripting in Python.
- Escalation for Tier 1/2; customer-facing delivery through full engagement lifecycle.

National IT Service Desk Coordinator - RadNet

May 2018 - February 2020

- National IT front door; AD administration; software support; eRad RIS/PACS; infrastructure monitoring.

PROJECTS & COMMUNITY

Homelab: OpenCTI + MISP; Proxmox NSM (Suricata, Wazuh, Zeek->Splunk, OPNsense, Nebula); Terraform VMs on five Dell servers.

SKILLS

DFIR & IR: IR, triage, RCA, EDR/artifacts, Velociraptor, Timesketch, KAPE, EZ Tools, malware analysis, MITRE ATT&CK
SIEM: Splunk, Zeek, Suricata, Snort, Wazuh, Security Onion, Gurucul GRA, threat hunting
Threat intel: OpenCTI, MISP, IOC enrichment, TLSH, TTP correlation
Offensive: Nmap, Metasploit, Burp Suite, SQLMap
Engineering: Python, Bash, Git, Ansible, Terraform, Docker, hardening
Systems: Linux/Windows, ESXi, Proxmox, AD, homelab
Cloud/net: M365, Azure, AWS, GCP, Cisco ASA, OPNsense, TCP/IP, DNS, VLANs

EDUCATION

Coursework toward B.A. in English - University of Baltimore, 2008-2011