Jacob Kosidowski

(507)458-1295
JakeKos21@outlook.com
https://www.linkedin.com/in/jtk21-cybersec/

Summary

Cybersecurity Professional with 10 years of experience institutionalizing operational rigor through policy, ensuring critical information flows through Knowledge Management, implementing security and hunting solutions, and developing cybersecurity training and range environments. Highly proficient in network threat hunting, SIEM toolkits, log ingestion, forensics, and cyber defensive actions. Driven and motivated to implement my skill set within a rapidly-evolving cybersecurity domain.

Certifications

CompTIA Security+

SANS GIAC Network Forensic Analyst (GNFA)
SANS GIAC Certified Detection Analyst (GCDA)
SANS GIAC Defending Advanced Threats (GDAT)

Skills

ELK Stack, Beats, Vulnerability Analysis, Network Traffic Analysis, Cyber Threat Hunting, Security Onion, Data Collection/Enrichment/Aggregation, Arkime, Malcolm, Reverse Engineering, Critical Thinking, Windows, Linux, Kubernetes, Helm, AWS, HTML, Python

Clearence

Top Secret / Sensitive Compartmented Information (TS/SCI)

Professional Experience

Cybersecurity Tech Lead
United States Air Force
Various Locations — Dec'21 - Present

- Technical Lead in traffic analysis, SIEM management, and threat hunting overseeing the development, testing, and employment of new TTPs and tools to advance SOAR operations.
- Authored technical documentation outlining standard operating procedures, best practices, and presented training & toolkit deficiencies to senior leaders to enhance and improve team operations.
- Oversaw planning, root cause analysis, and maintained after action reviews from all training, exercise, and operations enabling continuous improvement across twelve 39-member teams.
- Developed and provided training for Network Analysts on Threat Hunting within Kibana utilizing the Discover, Visualizations/Dashboards, and Detections features.
- Managed ELK stack deployment in a containerized environment leveraging Helm, Kubernetes, and cri-o across a distributed rapidly deployable server cluster.
- Configured the integration of MISP, Attack Navigator, thehive, Wikijs, and internal C2 tools within a containerized environment to allow fluid team operations and analysis.
- Administered Elastic Index Lifecycle Management policies and implemented backups with Minio for a deployable SIEM toolkit with constrained data storage to facilitate response operations.

Cyber Threat Hunting Team Lead
United States Air Force
Various Locations — May'19 - Dec'21

- Led cross-functional defensive cyber operations conducting data collection/analysis, identification/hunt of adversarial techniques leveraging threat intelligence, and network hardening actions.
- Directed 9-member team response to 3 incidents, rapidly scoped potential intrusions/issues, made critical decisions to execute response plans, and ensured the safety and security of assets.
- Planned & Executed Phishing Campaign targeting 1300 personnel - attack vector, email content, and delivery - provided remedial training on how to identify potential malicious indicators.
- Team Instructor & Evaluator responsible for ensuring personnel are properly trained and can demonstrate required skills in accordance with documented procedures during operations.
- Developed and implemented twelve data ingest pipelines utilizing Logstash mutate plugins and grok parsing, enriching 24 TB of raw customer logs into actionable data for analysis.
- Leveraged elastic beats Filebeat, Auditbeat, and Winlogeat for log collection and forwarding across critical customer networks in addition to Metricbeat for internal cluster monitoring.

Jacob Kosidowski

(507)458-1295
JakeKos21@outlook.com
https://www.linkedin.com/in/jtk21-cybersec/

Knowledge Management Center/Requirements Lead
United States Air Force
Various Locations — Jul'13 - Sep'18

- Responsible for directing and supervising a 10-member team to provide services to 47 Organizations and 6000 personnel across the installation.
- Led Records Management program and ensure proper records maintenance and end-of-year staging actions in accordance with NARA/DoD standards.
- Oversaw $3M SharePoint platform hosting 670 sites and built visual dashboards for Installation Programs which increased visibility for senior leaders and highlighted critical gaps in operation effectiveness and/or capabilities.
- Managed, tracked, and ensured timelines were met for 1100 Communications projects and oversaw the lifecycle management for 300 local policies aiding space launch operations.
- Installation Freedom of Information Act (FOIA) & Privacy Act program lead ensuring federal program compliance, Personal Information protection, & proper information release/redaction.

Education

AAS - Cyber Warfare Operations
Community College of the Air Force, Maxwell AFB, AL — 2019

AAS - Knowledge Management
Community College of the Air Force, Maxwell AFB, AL — 2016

Additional Training

SANS GIAC Reverse Engineering Malware
Currently Enrolled — 2023

Undergraduate Cyberspace Training
333rd Training Squadron, Keesler Air Force Base, MS — Sep'18 - Apr'19

Defensive Cyber Operations - Network and Host Analysis
39th Information Operations Squadron
Hurlburt Air Force Base, Florida — Aug'19-Nov'19

Elasticsearch Engineer 1 & 2
Certification Not Attempted — May'20