Jasper Woods

(630) 555-0148 jasper.woods@email.com linkedin.com/example/jasperwoods Naperville, IL 60540

SUMMARY

Senior SOC Analyst and **incident response** professional with 15 years supporting **security monitoring**, **threat hunting**, **alert triage**, remediation, and incident leadership across complex enterprise and public-sector environments. Leads investigations across EDR, SIEM, endpoint, identity, network, cloud, and protected operational telemetry. Uses Python and PowerShell for detection engineering, enrichment, investigation automation, and reporting. Coordinates containment, eradication, recovery, evidence handling, and remediation with infrastructure, application, identity, compliance, and business stakeholders. Mentors analysts through case reviews, tabletop exercises, shift coaching, and practical threat-hunting guidance. Holds CISSP, CySA+, and Security+ certifications alongside a Bachelor of Science in Cybersecurity. Ready to help Redwood Public Safety Technologies strengthen monitoring, response consistency, detection quality, and CJIS-aware security operations.

EXPERIENCE

Senior SOC Analyst & Incident Lead

March 2024 - Present

CivicShield Security Services

Chicago, IL

Directs monitoring and incident response across cloud workloads, endpoints, identity systems, and protected operational networks. Leads high-severity investigations, improves detection content, coordinates remediation, maintains CJIS-aware records, and mentors six analysts.

- Correlated **EDR**, SIEM, identity, network, and **threat intelligence** data during high-severity investigations.
- Created **Python** enrichment scripts and **PowerShell** rules, reducing repetitive investigation work for analysts.
- Coordinated containment, eradication, and recovery with infrastructure, application, identity, and compliance stakeholders.
- Maintained CJIS-aware evidence timelines, executive summaries, and **remediation** records for post-incident reviews.
- Mentored six analysts through case reviews, tabletop exercises, shift coaching, and threat-hunting guidance.
- Refined **detection logic** after incident reviews, improving context available during alert triage and escalation.

SOC Operations Manager

July 2021 - February 2024

BlueHaven Digital Defense

Evanston, IL

Managed a 24/7 SOC model for regulated customers, aligning alert operations, escalation paths, response playbooks, analyst quality, customer reporting, and remediation verification with contractual security requirements.

- Managed 24/7 alert queues and escalation paths across multiple regulated customer environments.
- Guided investigations involving credential abuse, malware, PowerShell, lateral movement, and anomalous administration.
- Established threat-hunting sprints using endpoint telemetry, authentication data, and adversary tradecraft.
- Prioritized remediation with customer security leaders and verified closure of incident actions.
- Automated indicator lookups, case enrichment, and operational reports with Python and PowerShell.
- Delivered service reviews that improved severity assignment, evidence capture, and stakeholder **reporting** consistency.

Lead Security Operations Analyst

January 2018 - June 2021

Northstar Communications Group

Oak Brook, IL

Served as senior escalation point for monitoring across corporate, hosted, and field environments supporting sensitive communications services. Directed complex investigations, detection tuning, incident bridges, automation, and analyst development.

- Combined process trees, command lines, DNS, identity, and network evidence into defensible findings.
- Built detection content for scripting, privilege misuse, persistence, and unusual remote access.
- Documented testing criteria and known limitations before releasing tuned detection rules.
- Directed incident bridges with network, systems, cloud, and legal **stakeholders** during containment.
- Developed **PowerShell** and **Python** utilities that shortened monitoring-to-response handoffs.
- Trained junior analysts on investigative reasoning, escalation thresholds, reporting, and artifact handling.

Security Operations Analyst

September 2014 - December 2017

IronGate Managed Security

Rosemont, IL

Monitored SIEM and endpoint alerts across commercial and public-sector environments. Investigated phishing, malware, account compromise, and policy events while supporting **threat hunting**, remediation coordination, automation, and customer reporting.

- Monitored **SIEM** dashboards and endpoint alerts across commercial and public-sector environments.
- Analyzed phishing, malware, account compromise, and policy events using security telemetry.
- Developed search queries and validated suspicious indicators during assigned threat-hunting investigations.
- Applied PowerShell collection and Python enrichment during recurring security investigations.
- Coordinated remediation requests with administrators and application owners, confirming closure evidence.
- Prepared incident summaries and shift briefings covering scope, risk, and next steps.

Junior SOC Analyst September 2011 - August 2014

Lakefront Technology Partners *Downers Grove, IL*

Supported centralized monitoring for enterprise customers under senior responder guidance. Applied playbooks, collected evidence, tested SIEM rules, developed introductory scripts, and presented case findings during team reviews.

- Monitored centralized security events and endpoint notifications using documented response playbooks.
- Triaged authentication anomalies, suspicious processes, attachments, and network indicators with senior guidance.
- Collected host and log evidence while preserving timestamps and investigative notes.
- Compared sample events against expected SIEM alert behavior and documented false positives.
- Created introductory PowerShell collection scripts and Python exercises for event parsing.
- Presented selected case findings during reviews, improving escalation notes and incident timelines.

PROJECTS

CJIS-Aware Detection Improvement Program 2025

Reviewed incident patterns, alert context, and evidence requirements across public-safety operations. Improved detection review practices, reporting consistency, and remediation tracking for high-security investigations.

Automated SOC Investigation Enrichment 2023

Built Python and PowerShell utilities for indicator lookups, case enrichment, and recurring reports. Gave analysts faster context while preserving audit-ready investigation records.

Threat-Hunting Sprint Framework 2020

Created repeatable hunting sprints around endpoint telemetry, authentication data, and adversary tradecraft. Helped teams uncover monitoring gaps beyond alert-driven workflows.

LEADERSHIP & AWARDS

- SOC Excellence Award, CivicShield Security Services, 2025. Recognized for dependable incident leadership and practical improvements in security operations.
- Incident Response Mentorship Recognition, BlueHaven Digital Defense, 2023. Honored for helping analysts build stronger investigation and escalation habits.
- Security Operations Quality Award, Northstar Communications Group, 2020. Recognized for clear evidence, detection tuning, and response coordination.

EDUCATION

Bachelor's Degree in Cybersecurity 2011

Illinois Institute of Technology GPA: 4.0 *Chicago, IL*

Coursework: *Incident response, network security, digital forensics, security operations*

CERTIFICATIONS

- CISSP 2022
- CompTIA CySA+ 2018
- CompTIA Security+ 2012

TECHNICAL SKILLS

- **Security Monitoring:** EDR, SIEM, alert triage
- **Incident Response:** Containment, eradication, recovery
- **Threat Hunting:** Endpoint telemetry, authentication data, adversary tradecraft
- **Detection Engineering:** Analytic rules, detection logic, rule testing
- **Scripting:** Python, PowerShell, automation
- **Security Analytics:** Log analysis, event correlation, evidence timelines
- **Threat Intelligence:** Indicator lookups, enrichment, adversary indicators
- **Endpoint Security:** Process trees, command lines, endpoint collection
- **Identity Security:** Authentication monitoring, credential abuse, privilege misuse
- **Network Security:** DNS records, firewall telemetry, proxy telemetry
- **Governance and Compliance:** CJIS policy, audit records, remediation tracking
- **Response Operations:** Playbooks, tabletop exercises, incident bridges

SKILLS

- Threat hunting
- Incident response
- Incident command
- EDR
- SIEM
- Detection engineering
- Alert triage
- Remediation coordination
- Python
- PowerShell
- Security analytics
- Threat intelligence
- Malware investigation
- Identity monitoring
- Log analysis

PROFESSIONAL AFFILIATIONS

- Chicago Cybersecurity Professionals Association, Incident Response Working Group, 2022 - Present.
- ISACA Chicago Chapter, Volunteer Workshop Facilitator, 2019 - 2023.

LANGUAGES

- English (Native)
- Spanish (Intermediate)

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST