Anthony Bandaras

Email: Anthony.Bandaras@gmail.com | Phone: 720-346-8549 | LinkedIn: www.linkedin.com/in/anthony-bandaras-a4400135

Professional Summary

Cybersecurity leader with over 15 years of experience in Security Operations Center (SOC) management, Incident Response (IR), and Security Information and Event Management (SIEM) solutions. Recognized Subject Matter Expert (SME) in QRadar deployments and integrations, threat detection, SOC optimization, and advanced automation. Proven track record in leading teams, improving operational efficiency, and strengthening organizational security posture across public and private sectors.

Core Competencies

- QRadar Specializations: Deployment, integration, upgrades, HA/DR, use case development, parsing, and tuning
- Incident Response: Threat detection, containment, remediation, and post-incident analysis
- SOC Operations: SOCaaS implementation, team training, gap analysis, and continuous improvement
- Deep expertise in incident response and threat detection
- Strong knowledge of cloud and on-prem security
- Experience with SIEM, SOAR, EDR, and identity systems (AD/Azure AD)
- Degree or certifications in cybersecurity, or equivalent experience
- Excellent communication and collaboration skills
- SIEM Technologies: IBM QRadar, Splunk, LogRhythm, Exabeam, Logz.io, TSIEM
- Threat Management: Vulnerability assessments, threat intelligence, and mitigation strategies
- Compliance & Standards: HIPAA, PCI DSS, SOX, HITECH, ISO 17799
- Automation & Orchestration: IBM SOAR, custom parsers, advanced workflows
- Cloud Security: SIEM migrations across on-prem and cloud environments

Professional Experience

IBM QRadar SIEM Deployment Engineer

Alacrinet | Aug 2024 – Apr 2025

- Deployed and configured IBM QRadar across multiple client environments

- Developed custom parsers and advanced use cases to support unique logging requirements
- Performed QRadar tuning and ingestion optimization across 15,000+ log sources
- Led upgrade cycles and implemented HA and Disaster Recovery solutions

Project Delivery Senior Manager – Cyber & Strategic Risk

Deloitte | Dec 2023 – Aug 2024

- Managed full-lifecycle incident response for state-level government agencies
- Directed the deployment of QRadar across 15 agencies with 90+ appliances and 15,000+ data sources
- Developed custom dashboards and security configurations for Windows/Unix systems
- Conducted security gap analyses and delivered vulnerability remediation plans
- Designed and implemented a crisis response plan, reducing downtime by 15%

Director of Information Security / CTO

Alacrinet | Jul 2021 – Nov 2023

- Oversaw SOCaaS delivery and IR workflows, utilizing IBM SOAR for automation
- Led enterprise deployments of QRadar and Exabeam for large government entities
- Designed SOC training programs, improving analyst readiness and efficiency

Professional Services Manager – ASOC / SOCaaS

NTT Security | Jul 2017 – Jul 2021

- Directed global SOC operations, including threat hunting and SIEM architecture
- Developed and deployed SIEM integrations and SOAR workflows
- Customized dashboards and parsers tailored to specific client needs

Senior Security Consultant

NTT Com Security | May 2015 – Jul 2017

- Executed QRadar deployments and tuning for managed services clients
- Performed SOC health assessments and improved escalation procedures
- Built use cases, wrote parsers, and optimized log source collection

Senior Security Consultant – Managed Security Systems

CDI Corporation | Jun 2013 – May 2015

- Migrated clients from legacy platforms to IBM QRadar with minimal service disruption
- Configured HA and DR environments, and developed advanced threat detection rules
- Created UBA content, custom reports, and tailored use cases

Senior Consultant – Security & Privacy

Deloitte & Touche LLP | Jan 2013 – Jun 2013

- Developed security frameworks and incident handling protocols for healthcare exchanges
- Ensured regulatory compliance through advanced monitoring and control implementation

Security Consultant – Managed Security Systems

IBM | Oct 2008 – Jan 2013

- Provided managed security services, focused on triage, compliance, and log management

Information Security Analyst / Auditor

Triad Consultants, Inc. / IBM | Jul 2006 – Oct 2008

- Conducted security audits and risk assessments, significantly improving incident detection

Education

M.S. in Information Systems Management (Information Security)
Colorado Technical University, Colorado Springs, CO | 2005

B.S. in Electronics Engineering Technology / Computer Science
Metropolitan State University of Denver, Denver, CO | 1996

Certifications

- IBM QRadar SIEM Foundation
- IBM Security XDR Technical Sales Intermediate
- IBM Security Guardium Sales Foundation
- IBM Cloud Pak for Security Sales Foundation
- Microsoft Sentinel
- Splunk User
- LogRhythm Admin
- Exabeam Admin
- AWS Certified Cloud Practitioner
- AWS Certified Solutions Architect – Associate

Additional Expertise

- SOC Optimization: Health checks, analyst training, workflow improvements
- SIEM Migrations: Seamless platform transitions with minimal disruption
- Incident Management: Forensics, RCA documentation, and continual improvement initiatives