Joshua Padilla

Golden, CO | 720-231-7411 | https://www.linkedin.com/in/padilla-joshua

---

Threat Detection & Response Management | SOC Operations | Incident Response | MDR Leadership

Cybersecurity leader with 10+ years of Cybersecurity experience and 2+ years in building and managing **SOC and MDR operations**, including global teams and enterprise-scale detection programs. Proven track record in **incident response leadership, threat detection strategy, and operational excellence**, with deep expertise in **EDR (Carbon Black Cloud), and MITRE ATT&CK–aligned detection frameworks**. Known for developing high-performing teams, reducing analyst turnover, and improving detection fidelity and response efficiency.

PROFESSIONAL EXPERIENCE

Broadcom (Formerly VMware Carbon Black)

Working Manager/Senior Threat Analyst, MDR
Broomfield, CO
April 2019 – July 2025

- Led day-to-day operations of a global **SOC/MDR team** responsible for **24/7 threat monitoring, triage, and incident response**, ensuring consistent service delivery and high-quality investigative outcomes.
- Managed analyst workflows, escalations, and **SLA adherence** while mentoring team members, resulting in the **lowest analyst turnover rate in company history**.
- Designed and implemented a **follow-the-sun operating model** that enabled **24/7 global coverage** and improved response times by **approximately 25%**.
- Oversaw investigations involving **endpoint and cloud-based threats**, guiding analysts through **hundreds of security incidents** across customer environments.
- Directed the development and standardization of **incident response playbooks**, improving triage efficiency and investigative consistency.
- Collaborated with **Detection Engineering** to improve **alert fidelity** and visibility, contributing to a **30–40% reduction in false positives**.
- Helped lead the transition from **Managed Detection (MD)** to **Managed Detection and Response (MDR)**, contributing to **go-to-market strategy**, service design, and operational readiness.

- Partnered with product and UI/UX teams as a **Carbon Black Cloud (CBC) super user** to influence feature enhancements that improved platform usability and customer adoption.
- Standardized **customer notification and reporting processes**, improving clarity, consistency, and **executive communication** during high-severity incidents.
- Provided escalation support for **critical incidents**, delivering **executive-level summaries** and remediation guidance to internal and customer stakeholders.
- Served as a **trusted technical advisor** to sales teams and customer stakeholders, conducting **health checks** and strategic consultations that supported **proof-of-concept success, customer retention, and contract renewals**.
- Received multiple **VMware "At Our Best" awards** for contributions to the successful **MDR launch** and ongoing operational excellence.

InteliSecure

Data Protection Analyst, Team Lead
Greenwood Village, CO
November 2018 – April 2019

- Monitored and investigated security alerts across **endpoint, email, and cloud environments**, focusing on **data loss prevention (DLP)** and insider threat activity
- Analyzed suspicious behaviors including **unauthorized data transfers, policy violations, and anomalous user activity**
- Conducted investigations using **log analysis, endpoint telemetry, and email artifacts** to determine risk and impact
- Collaborated with cross-functional teams (including HR and leadership) to support **insider threat investigations**
- Tuned detection rules and policies to improve signal-to-noise ratio and reduce alert fatigue
- Documented investigation findings and contributed to the development of **incident response procedures and playbooks**

EDUCATION

Master of Science: Information & Communication Technology (Cybersecurity Emphasis)
University of Denver
Denver, CO
August 2016 - August 2018
GPA: 3.97

Bachelor of Arts: International Relations (European Union Emphasis)
University of Colorado Boulder
Boulder, CO
August 2012 - December 2014
GPA: 3.28

CORE COMPETENCIES

Security Operations & Incident Response: Security Operations Center (SOC), Managed Detection and Response (MDR), Extended Detection and Response (XDR), Incident Response, Threat Hunting, Threat Detection Collaboration, Root Cause Analysis, Triage, Escalation Management, Containment and Remediation

Detection Engineering & Analytics: Detection Tuning, Alert Logic Optimization, False Positive Reduction, MITRE ATT&CK, Cyber Kill Chain, Playbook Development, Threat Intelligence, Detection Coverage Analysis

Platforms & Tools: VMware Carbon Black Cloud, Jira, Confluence, Symantec DLP, Proofpoint DLP/CASB, ForcePoint DLP/CASB

Frameworks & Standards: MITRE ATT&CK, ISO 27001

Leadership & Advisory: Team Leadership, Analyst Development, Operational Readiness, Service Delivery, Stakeholder Management, Executive Communication, Cross-Functional Collaboration, Technical Advisory, Customer Success, Health Checks, Proof of Concept (POC) Support, Customer Retention, Renewals, Go-to-Market Strategy