CHRISTIAN CARRASCO

IT OPERATIONS MANAGER | SERVICE DELIVERY | INCIDENT COMMAND | TEAM LEADERSHIP

Ocala, FL | (954) 806-6715 | christiancarrasco@myyahoo.com | linkedin.com/in/cybercc

PROFESSIONAL SUMMARY

IT Operations leader with 10+ years of experience commanding P1/P2 incidents, managing a five-person engineering team, and owning SLA performance across enterprise production managed services accounts. Maintains after-hours and on-call operational coverage, owns escalation matrices and incident runbooks, and coordinates geographically distributed technical teams through restoration while driving post-incident root cause analysis and corrective action under ITIL/ITSM problem management. Brings hands-on depth across AWS infrastructure, Dynatrace and PagerDuty monitoring, ServiceNow, and Linux environments backed by direct managed services delivery experience at the world's number one automotive brand by global sales.

CORE COMPETENCIES

Incident Response & Major Incident Command • SLA Management & Performance Reporting • Team Leadership & People Management • Disaster Recovery & Business Continuity • Continuous Process Improvement • Process Documentation & Training • Root Cause Analysis • Budget & Vendor Contract Management • Cloud Security & AWS Auditing • SIEM Engineering & Administration • Organizational & Prioritization Skills • Analytical Problem Solving & Root Cause Investigation

TECHNICAL PROFICIENCIES

Monitoring & Observability: Dynatrace, PagerDuty, AWS Shield, Syslog, dashboard and metrics reporting, alert threshold tuning

SaaS, ITSM & Endpoint: ServiceNow (ticketing, CMDB, control correlation), ITIL v4, SCCM, KACE, Office 365 Security & Compliance

Cloud & Infrastructure: AWS (EC2, S3, Lambda, CloudFormation, CloudFront, Route 53, Elastic Beanstalk, IAM, Security Groups, Shield), Azure AD, VMware, Hyper-V, Windows Server, Linux (Ubuntu, Debian)

Automation & Delivery: Jenkins, AWS CloudFormation, ServiceNow

Identity & Access: Active Directory, Azure AD / Microsoft Entra ID, conditional access, MFA, SSO, AWS IAM, Group Policy, RBAC, joiner-mover-leaver lifecycle

Compliance & Frameworks: NIST 800-53, NIST CSF, ISO 27001, SOX, PCI DSS, HIPAA, CMS, control mapping, audit evidence and documentation

Security & Threat Response: SIEM (LogRhythm), correlation rule and alarm development, phishing and IOC analysis, vulnerability scanning and remediation, MITRE ATT&CK mapping, Cylance, Sophos, Checkpoint, Cisco Umbrella

Networking: TCP/IP, DNS, DHCP, BGP, OSPF, VLAN, NAT, ACL, SSH, Bastion, VPN

PROFESSIONAL EXPERIENCE

Beyondsoft Consulting Inc. - Remote

Operations Manager 03/2021 - 08/2026

Started as Senior Lead Systems Analyst; promoted to Operations Manager in late 2022, retaining technical and operational responsibilities while adding people leadership, budget, and training ownership. Was embedded on assignment at Toyota Motor North America.

- Command P1/P2 incident management end to end across enterprise production environments, assigning severity against business impact, coordinating technical response across teams, driving restoration, and owning customer escalation and executive communication through resolution.
- Lead and manage a five-person engineering team across operations management responsibilities, owning hiring from requirements definition through selection, performance management, one-on-ones, and development conversations, sustaining minimal turnover with one hire in the past three to four years.

- Maintain incident response runbooks, escalation matrices, and on-call rotation coverage for after-hours and weekend operational continuity, standardizing how a five-person team responds to major events and technical escalations across managed services accounts.
- Lead post-incident reviews and root cause analysis, translating recurring failure patterns into corrective actions and runbook improvements consistent with ITIL/ITSM problem management, feeding systemic issues into continuous improvement tracks rather than treating symptoms repeatedly.
- Coordinate change management activity including maintenance windows, change requests, and release work across internal and client enterprise production systems, communicating scope and risk to stakeholders so planned service delivery work does not become unplanned downtime.
- Balance workload and capacity planning across competing client priorities for a geographically distributed team while serving as the escalation point for technical and customer escalation issues the team cannot resolve alone, including after-hours and on-call coverage.
- Own SLA performance oversight across enterprise production teams by identifying breaches and underperforming areas, investigating root causes, and driving corrective action plans with the owners responsible for closing them and restoring service delivery targets.
- Identify and implement continuous improvement across recurring operational workflows, authoring the runbooks and standard operating procedures that make them repeatable and aligned with ITIL/ITSM practices rather than dependent on individual tribal knowledge.
- Administer Dynatrace and PagerDuty across enterprise production client workloads in a managed services environment, onboarding new applications into monitoring coverage, tuning alert thresholds to cut noise, and maintaining escalation and routing policies.

TelevisaUnivision - Remote

Information Security Analyst 10/2019 - 10/2020

Scope spanned SOC analysis, security engineering with tool enhancement, and security architecture including SIEM migration planning and server restructuring.

- Tracked incident findings and remediation activity in ServiceNow, correlating findings against the CMDB to assign ownership to the right infrastructure and application teams, driving items to closure, and capturing closure evidence for compliance stakeholders as corrective action documentation.
- Managed log retention and storage configuration against compliance requirements, documenting detection logic, tuning rationale, and operational runbooks for continuity so that procedures remained reviewable, repeatable, and available to any analyst inheriting the work.
- Led root cause analysis of security incidents by interpreting tool data to form and test hypotheses, identifying contributing factors, and documenting response decisions and corrective action so the same issue did not recur unexamined across the production environment.

Cigna HealthCare - Doral, FL (Hybrid)

System Administrator 10/2014 - 10/2019

Five years supporting a HIPAA-regulated healthcare environment.

- Served as lead technician and Level 3 escalation point for a support team of three technicians and one supervisor, owning customer escalation resolution across identity, endpoint, application, and connectivity issues that lower tiers could not close in an enterprise production environment.
- Mentored and provided technical guidance to junior technicians, authoring knowledge base articles and troubleshooting documentation that functioned as runbooks for repeat issue patterns, reducing escalations reaching Level 3 through continuous improvement of team procedures.
- Assisted in the development and testing of disaster recovery technology plans with key users, participating in exercises that validated recovery procedures and documenting results for continuity review in a HIPAA-regulated enterprise production environment.

Commonwealth-Altadis - Fort Lauderdale, FL (Contract)

IT Support Specialist 10/2013 - 06/2014

EDUCATION

B.S. Network Operations and Security, Western Governors University | Oct 2017 - Jan 2021

CERTIFICATIONS

Certified Ethical Hacker (CEH), EC-Council | CompTIA Security+ | AWS Certified Cloud Practitioner | ITIL v4 Foundation | Cisco CCNA Routing & Switching

CERTIFICATION IN PROGRESS

ISC2 Certified Information Systems Security Professional (CISSP) | In Progress

Focus: Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, Software Development Security