Patrick Hunt

443.652.7069 | huntpatrickjames@gmail.com

Experience

IT SPECIALIST (SECURITY) | CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS) | JUNE 2019 – PRESENT

- Translates business and mission-oriented objectives into technical requirements to author and revise information security vendor contracts, statements of work (SOW), and statements of objectives (SOO), and other procurements.
- Conducts regular incident response and security operations collaboration engagements with CMS Cloud Security Operation teams to determine areas of improvement in CMS Cloud and CMS SOC monitoring and detection.
- Directs and plans ISPG activities and deliverables in support of Marketplace Open Enrollment, including tabletop exercises, the Marketplace Report with POA&M tracking and escalation, and readiness briefings to CCIIO.
- Briefs external stakeholders and program leadership on incident response, control implementation, and general information security best practices defined by NIST and CMS policy.
- Successfully identities gaps in the CMS cloud security posture and coordinates with IUSG and ISPG leadership to address and remediate gaps, examples include prioritization and implementation of Cisco Umbrella, Cloud VPN log visibility, and the implementation of Guard Duty to address ADO level configuration issues and security weaknesses.
- Oversees the drafting and implementation of automated workflows which have resulted in a reduction for CMS SOC response times to incidents and improved response rates by supporting firewall teams.
- Identifies use cases for machine learning and to improve security operation detection capabilities.

Incident Response Lead | June 2019 - Present

- Prioritized projects and initiatives which have allowed CMS to demonstrate the effectiveness and maturity of its incident response program during IG FISMA Metric evaluations and audits.
- Developed and coordinated processes to allow the SOC to support the Insider Threat program.
- Coordinates incident response activities with the HHS Office of the Inspector General (OIG), FBI, HC3, and other federal partners.
- Implemented a risk management and quality control review process through daily standups with leadership elements across multiple security teams. Interprets and translates OMB, DHS, & HHS policies into written procedures to enable consistent and repeatable breach response capabilities.
- Manages relationships with cross functional teams at component and program levels, supporting CMS enterprise incident response functions.
- Advises on and coordinates the procurement and implementation of security tools used across the CMS enterprise.
- Provides oral and written guidance to CMS business owners and program leadership on corrective action plans and strategies to meet NIST SP 800-53 and Acceptable Risk Safeguard (ARS) requirements.
- Conducts and directs incident management capabilities including developing incident response plans, trend analysis, tracking, and reporting.
- Serves as the primary escalation point for major incident reporting and coordination for CMS.
- Directs and oversees planning phase and execution of security awareness exercises to promote collaboration between security, operations, and business components of CMS.

IT SPECIALIST (SECURITY) | CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS) | CONTINUED

Product Owner/Manager ServiceNow Security Incident Response (SIR) Module | June 2021 - Present

- Defines and prioritizes technical and functional requirements for the SIR module.
- Manages relationships with stakeholders with workflows onboarded to the SIR module, ensuring stakeholder current and future needs are documented during monthly capture sessions. .
- Identified areas of optimization and automation to reduce manual processes and provide value to stakeholders.

Government Task Lead CMS SOC | June 2019 – Present

- Directs and prioritizes investigation objectives for incidents of significant risk or ambiguity.
- Integrates Agile principles into task and project management to ensure work products are created iteratively and efficiently.
- Implements quality and risk management controls over stakeholder interaction and processes to ensure customer and stakeholder concerns are addressed appropriately.

Government Task Lead CMS Incident Management Team | June 2019 – Present

- Defines and oversees implementation of escalation procedures.
- Integrates Agile principles into task and project management to ensure work products are created iteratively and efficiently.
- Reviews and approves standard operating procedures, training exercises, and proposed process improvements.

Government Task Lead Forensics & Malware Analysis Team | June 2019 – August 2020

- Directed and set forensic investigation objectives in support of enterprise incident response efforts.
- Served as liaison between Office of Human Capital (OHC) and the Forensic & Malware Analysis Team (FMAT) in support of human resource investigations.
- Translated technical findings into actionable insights for stakeholders.
- Monitored team case assignments, conducted case reviews as well as reviews of report findings.
- Established working relationships with external groups to enhance forensic capabilities, specifically the use of eDiscovery tools such as Druva.

Information System Security Officer – OCIO SSM | June 2019 – August 2020

- Oversaw change control procedures, reinforced ITIL standard and nonstandard change request process.
- Reviewed and approved security impact assessments (SIAs).
- Conducted contingency planning exercises to ensure training for key personnel and the ability to meet established recovery time objectives (RTOs).

INCIDENT MANAGEMENT TEAM LEAD | IRON VINE SECURITY LLC | MAY 2017 – JUNE 2019

- On-boarded previously out-of-scope processes and refined them; most notably the privacy ticketing process for ISPG, reducing privacy ticket volumes by 50%
- Managed potential risks discovered by the Penetration Testing Team; provided guidance on potential impact to CMS businesses and beneficiaries.
- Provided quality assurance, and approval of task area contract deliverables before being presented to the customer.
- Directed and recommended plans of action during breach responses with the CMS Security Operations Center (SOC) and the Forensics Malware Analysis Team (FMAT) and external federal agencies during major security incidents to drive analysis and remediation efforts.
- Designed strategic goals for the incident management functional task area to meet operation and business needs.
- Recommended a course of action on each incident while ensuring investigation objectives and actions taken were documented, served as initial point of escalation for potential incidents reported by internal and external entities.

- Synthesized complex and technical information to written and oral situation reports to ISPG leadership, including Division Directors, CISO, and CIO, HHS, and DHS; information typically consisted of multiple vulnerability scans across thousands of hosts and/or multiple system logs from disparate sources.
- Provided project support and subject matter expertise to various in support of CMS initiatives and priorities.

ASSOCIATE | MORGAN STANLEY | SEPTEMBER 2013 – SEPTEMBER 2015

- Identified, triaged, escalated, and coordinated the response to high frequency electronic trading events and incidents which posed reputational, legal, and business risk.
- Budgeted headcount and capacity planning for the fiscal year through Managed Time Driven Activity Based Costing (TDABC) process.
- Drafted topical business and technical reports and presentations to inform leadership decisions.
- Planned and managed web application enhancement projects.
- Solicited customer requirements from brokers, worked with application development teams to deliver customer requirements and performed QA/UAT review prior to release.

FSI CRISIS MANAGEMENT TRAINING |U.S. DEPARTMENT OF STATE | AUGUST 2010 – DECEMBER 2010

- Researched and planned table-top exercises to prepare U.S. embassies and missions for natural disaster and terrorism-based events.
- Functioned as interim Program Officer during staff absence, performing the duties of a full-time Foreign Service Officer (FSO) by coordinating exercises with U.S. embassies and missions, consulting with Diplomatic Security Services personnel, and researching threats to embassies and missions in disparate areas of the world.

SMALL UNIT OPERATIONS SUPERVISOR | U.S. MARINE CORPS | MARCH 2003 – SEPTEMBER 2007

- Achieved ILR Level 1+/1+ in Iraqi Arabic through self-study.
- Successfully completed advanced leadership and technical occupational training.
- Organized, planned, and executed small unit operations during three combat deployments.

Education

- M.S. Information Security |2024| Champlain College
- B.A. Economics & International Studies | 2011 | Towson University

SKILLS & TOOLS: Python Scripting, Linux Administration, Nmap, Wireshark, Open-AudIT, SANS SIFT Workstation, Wireshark, ServiceNow, Splunk, Autopsy, CrowdStrike Falcon, RSA Archer GRC, Anomali, Tenable.sc

CERTIFICATIONS: Security Essentials Certification (GSEC), Certified Incident Handler Certification (GCIH), ITIL® v3 Foundations Certification

SECURITY CLEARANCE: ACTIVE Top Secret (2023-Present)

COURSES & CONFERENCES: CMS Workforce Resilience Cloud Awareness Cohort, Product Management Training Cohort, FOR500: Windows Forensic Analysis, SEC488: Cloud Security Essentials, SEC510: Public Cloud Security: AWS, Azure, & GCP, Splunk Core, Splunk Phantom (SOAR), SEC406 Linux for InfoSec Professionals