

Heath Nieddu

CISSP | GSEC | GCIH | MBA

Summary of Experience

Enabling the success of organizations by simplifying the complex, cutting costs, and saving time while delivering cyber security services.

Information security leader with over 14 years of experience maturing information security programs for multiple medium and large organizations in various industries. Managed dozens of projects as a consultant and full-time employee designed to enhance program capability, securely deploy security solutions and integrate security practices into IT and business processes.

Areas of specialization

- Threat and vulnerability management
- Information Security Architecture
- Security program assessment and development
- Facilitation, coaching, and mentoring
- Security tool rationalization
- Business intelligence and security metrics development
- Executive reporting
- Identity and access management (IAM) program development
- Data governance and privacy
- Threat intelligence and threat management
- Incident response and security operations

Experience

Sept 2020 – Present

Senior Advisor, Security Operations & Risk | Cask NX, LLC | San Diego, CA

- As a Senior Security Consultant for Cask, Heath leads projects that require information system governance to be streamlined and a natural part of service delivery. Leveraging his diverse background in the military, federal government, healthcare and retail, he focuses on helping clients deploy security and GRC applications while considering a wide range of requirements.
- Interim Global Risk Manager for industry-leading security logistics firm
- Information Security Program Developer, BISO
- Senior Advisor for the implementation of ServiceNow Risk Management
- Senior Advisor for the implementation of ServiceNow Security Incident Response
- Senior Advisor for the implementation of ServiceNow Vulnerability Management

Apr 2019 – Present

Adjunct Professor | Point Loma Nazarene University | San Diego, CA

- Heath works with students to explore what it means to manage information systems in environments where business and technology activities are increasingly overlapping.

Apr 2018 – Aug 2020

Security Architect Consultant | EVOTEK, Inc | San Diego, CA

- Shapes the company's overall security services, leveraging industry-recognized security controls and advanced technologies to address today's most critical security threats.
- Leads security service delivery teams to conduct security program assessments and tools rationalization efforts for marquee clients. These efforts are designed to optimize security investment under budgetary constraints.
- Focus areas are program assessment, policy development, vulnerability management, security metrics, insider threats, access management, and governance frameworks.
- Advises clients on emerging compliance and privacy regulations.

2017 – Apr 2018

Vulnerability Management Program Lead | DXC, Inc | San Diego, CA

- Vulnerability Management lead supporting the County of San Diego and DXC.
- Used vulnerability scan data and external data sources to: 1) make severity adjustments to CVSS scores, as well as 2) work with the rest of IT to prioritize, monitor and complete remediation steps. Interacted with application owners, architects, Wintel teams, infrastructure teams and third-party vendors to reduce exposure.
- Monitored and alerted management about emerging vulnerabilities. Creating executive dashboards summarizing exposure.
- Assessed Metasploit Express pen testing results and coordinating remediation.

2016 – 2017

Information Security Metrics Lead | Nike, Inc | Beaverton, OR

- Developed program to illustrate Nike's risk posture to the board of directors, CISO, and senior managers.
- Led a five-person security metrics team. Team members conducted metric design discussions, performed data extraction and transformation from multiple security tools, and developed a front-end dashboard in Tableau. Worked with developers to wrap the Tableau dashboard in java script for integration with broader intranet experience.

- Data analysis covered the following topics: vulnerability management, end-point protection, pen testing, secure code and network security. These efforts included evaluating the coverage and effectiveness of security controls.

2015 – 2016

Senior Information Security Research Principal | Optiv, Inc | Denver, CO

- Interviewed CISOs across the country to create program blueprints. These program blueprints illustrated effective ways to build insider threat and identity and access management (IAM) programs.
- Produced trade articles and presented at national conferences.

2012 – 2015

Senior Information Security Analyst | Providence Health | Beaverton, OR

- Provided reporting and analysis to the Board of Directors and senior management regarding information security threats facing this large healthcare organization.
- Created a set of six key performance indicators for the CISO. Aggregated over 100 base measures of security controls to create these six indicators.
- Used Qualys vulnerability scan data to prioritize the top 5000 workstations that needed enhanced policies, controls, and asset tracking.

2009 – 2012

Business Process Engineer, Information Security | Providence Health | Beaverton, OR

- Established research models, analytic standards, and training for information security analysts. Created a knowledge base of over 160 analytic products that distilled our collective knowledge into one analytic voice.
- Authored multiple pieces of analysis and provided briefings on emerging threats.
- Leveraged other experiences in finance, economics, and the intelligence community to enhance communication about security risks.

2007 – 2009

Economic Intelligence Officer | CIA | Langley, VA

- Created economic analysis for the Presidential Daily Brief (PDB) on multiple occasions. Focused on international finance. Result: POTUS questions answered in roughly six memos for the morning brief. Presented in Oval Office for delivery of analysis.

2001 – 2007

Cryptographic Technician, Interpretive | US Navy | Spain/Georgia

- Served as a highly deployable, Arabic linguist for the US Navy. This required not only linguistic skills, but also many technical skills related to communication technologies. Provided support for military and national agencies.

Education

Portland State University, Portland, Oregon

Master of International Management | 2014

Pacific Rim Economies

University of Central Florida, Orlando, Florida

Bachelor of Science | 2000

Finance

Professional Skills

- CISSP (2015)
- GSEC (2018)
- GCIH (2019)
- Splunk query and dashboard development to display tenable.io data
- Vulnerability scanners, including Nexpose/InsightVM, Qualys and tenable.io as well as vulnerability prioritization platforms such as Risk Sense and Kenna.
- Python/Anaconda and R Studio for data analysis, transformation, and modeling
- Git and BitBucket for version control
- Microsoft PowerView and Tableau for front-end dashboard development
- Used data from Symantec, zScaler, SentinelOne, Nessus, Qualys and Nexpose to enhance security program assessments
- Familiar with capabilities of IAM solutions such as SailPoint, Lieberman, Cyberark, Ping, and Okta and how those tools fit into overall program needs
- Personal use of Ubuntu, KVM, and Kali for wireless surveys.

Presentations

- Portland InfraGard Speaker: "Threats Inside and Out" Optiv, Inc, 2016.
- Palo Alto Ignite Speaker: "Four Steps to an Intelligence-driven Security Program" Optiv, Inc, 2016.