CHAD HATALA

SECURITY ENGINEER SR, THREAT ANALYST
Google Certified Cybersecurity Professional,
IBM Certified Cybersecurity Professional

Knoxville, Tennessee, United States
+1-865-809-8214
chad.hatala@gmail.com
https://linkedin.com/in/chad-hatala

Summary

Dynamic cybersecurity professional with a successful background in assisting executive management and implementing robust security programs. Equipped with a comprehensive toolkit encompassing analysis, reporting, threat hunting and research, intelligence collection, email security, process optimization, creation, and policy development. Adept at providing consultancy to diverse groups and actively participating in security-focused working groups. Skilled in multiple industries, including e-commerce, law, and healthcare, with a proven ability to create metrics dashboards and reports that executives value.

Key Skills

Public Trust • Leadership • Security Consulting • Log Analysis • Presentations • Cyber Kill Chain Framework • Source Intelligence • Vulnerability Assessment and Penetration Testing (VAPT) • Microsoft Defender • Project Management

Additional Skills

Cybersecurity Incident Response · Digital Forensics · Threat & Vulnerability Scanning · OSINT · Data Protection Manager · Access Control · IT Risk Management · Threat Analysis · Cyber Kill Chain Framework · Problem Solving · Technical Documentation · Technical Support · Business Process Automation · Incident Response · Threat Hunting · Cloud Computing · MITRE | ATT&CK · Cybersecurity · Information Security · Analytics · PCI-DSS · Data Visualization · Office 365 · Computer Hardware · Russian · Russian Politics

Software Experience

Microsoft Office · Office 365 · Sentinel · Defender · HP SureClick · Aternity · ServiceNow · Qualys · SailPoint · Splunk · Apple, Linux, and Android OS · Microsoft Windows · Kali Linux · ParrotOS · Ubuntu· Azure · SharePoint · PowerBI · PowerApps · PowerAutomate · Maltego · IBM QRadar · Adobe CS · Nmap · Wireshark · Shopify · WordPress · Squarespace · Volusion · ProofPoint · KnowBe4 · VSCode · Tenable Nessus ·Chronicle · Cyber Weapons · Snowflake

Industry Experience

Sr. Security Engineer | Provisions Group | Franklin, TN | Nov 2022 - Jun 2023
Served as a security engineer and information security consultant responsible for:

- Evaluating network vulnerabilities
- Identifying security gaps
- Collecting both intelligence and operational data

Leveraged SharePoint as a central platform for:

- Data management
- Reporting on information security operations

Utilized metrics provided by Sentinel and Defender.

Additionally, I:

- Generated best-in-class intelligence reports and presentations for top-level executives
- Actively participated in the Security Working Group, contributing to the identification and resolution of security weaknesses throughout the organization
- Consulted to Security Operations Center
- Served as Tier II and III incident handler.
- Served as ProofPoint liaison.
- Researched Organizational and Healthcare related threats
- Created security awareness training materials.
- Conducted vulnerability scans on web applications and servers.
- Partnered with CISO on program improvements and needs.
- Created CISO presentations for the rest of C-Suite.
- Provided weekly Threat Landscape and Health related intelligence reports to stakeholders.

Director, Information Security | Threds, Inc | Knoxville, TN | Jun 2019 - Oct 2022
Led organizational efforts in:

- Protecting information assets
- Managing cybersecurity risks
- Ensuring compliance
- Developing a secure environment

Provided:

- Security awareness training
- Strategic direction

- Policy development
- Procedures
- Incident management

Collaborated with stakeholders to establish a security program that aligns with business objectives.

Cloud Administrator and Architect | Threds, Inc | Knoxville, TN | July 2014 - Jun 2019

- Lead and implement process improvements that reduce costs and increase efficiency and security.
- Through several ongoing projects, process changes, marketing implementations, and more, helped reach the company's first million-dollar-a-year store in 2019.
- Flagship store is projected to cross the $2 million dollar mark+ for the second time in 2022, showing consistent and steady growth.
- Maintained and Secured 30+ ecommerce-based fulfillment stores across the enterprise.

Licenses and Certifications

Google

- **Google Cybersecurity Professional #RKJ7L58SMVZR**
- **Google Cloud Digital Leader #AE6K8XKPFWTN**

MITRE ATT&CK Defender™

- **Cyber Threat Intelligence Certification Training -** CC-7a0c50e8-648e-4e76-bf95-34636a316a64
- **Aversarial Emulation Certification** CC-42be3de1-a99b-4104-a57e-1787f400f0e1
- **Threat Hunting Certification** CC-19f25ca3-f638-4393-9672-ecdb680cf7cf
- **Cyber Kill chain Certification** CC-1b5e3445-d039-42d5-a0af-9878838d9734
- **OSINT Certification** CC-9089369d-ee49-439a-bb6f-dd2a72921997

$(ISC)^2$

- **Systems Security Certified Practitioner (SSCP) #UFD2HVE7HB3Y**
- **Cyber Security Certified (CC) #YRVV7WU8Y93K**

EC-Council

- **Ethical Hacking Essentials (EHE) #9SHBQ9CCPW3C**

INFOSEC Institute

- **Cybersecurity Leadership and Management #42YLMPR4PHUK**
- **Cyber Threat Hunting #MUSXKKV8S7VE**
- **Blockchain Security #M8BNVUEK9KE2**
- **Python Automation**

US Department of Homeland Security

- **101 Critical Infrastructure Protection (Public)**
- **101 Reverse Engineering (Public)**

Cybersecurity Infrastructure and Security Administration

- **Cloud Computing Security**
- **Cyber Intelligence (Public)**

Splunk, Inc

- **Splunk Search Expert Certified #L6NUT4LY5SGP**

IBM

- **Certified Professional Cybersecurity Analyst #NAHWKNDAJK5A**
- **Certified Data Scientist #QNVUC8UPV3D3**
- **Tools for Data Science V2 #QNVUC8UPV3D3**

IBM Skill Badges

- **Cybersecurity Compliance and Framework Certified**
- **Network Security and Database Certified**
- **Penetration Testing, Incident Response and Forensics Certified**
- **Malware Analysis Certified**
- **Threat Intelligence Certified**
- **Data Visualization w/ Python**
- **Python for Data Science and AI**
- **Machine Learning w/ Python**
- **Data Visualization and Dashboards**
- **Data Science Methodology**
- **Excel for Data Analytics**
- **Data Analytics**

https://www.credly.com/users/chad-hatala/badges

Education

Pellissippi State Community College

- **Cyber Defense (2020-2022)**
- **Media Technology and Web Development (2008-2013)**

University Certifications (ACE Credited)

University of Colorado, Colorado Springs - Specialization(s)

- **Homeland Security and Cybersecurity**
- **Computer Security and Systems Management**

Tomsk State University - Certification

- **Beginner Russian Language #5EGHTFFCTY3T**

University of California, Santa Cruz - Specialization

- **Russian History (1900 - Present) #8N9QSR35M93E**

Hands-On Skills

Cybersecurity Program Implementation — Assisted executive management in implementing robust security programs, ensuring optimal protection for critical assets as well as the creation of the Security Working Group for Quorum Healthcare.

Threat Hunting and Research — proactively identifying and mitigating potential risks and vulnerabilities.

Cybersecurity Subject Matter Expert (SME) — to diverse groups, advising on best practices and tailored security solutions.

Security Working Group — contributing to the development of industry-standard processes and protocols.

Cross-Functional Collaboration and Leadership — Collaborated with cross-functional teams to create metrics dashboards and reports, enabling executives to make informed decisions and prioritize security initiatives.

Intelligence Collection — Applied intelligence collection techniques to gather actionable insights and support proactive security measures.

Threat Intelligence — Applied comprehensive threat intelligence practices to gather, analyze, and interpret cybersecurity data to identify potential threats and vulnerabilities. Utilized threat intelligence feeds, open-source intelligence, and internal data to proactively enhance the organization's security posture. Familiar with industry-leading frameworks and methodologies such as MITRE ATT&CK and STIX/TAXII.

Threat Hunting — Proficient in proactive threat hunting techniques to detect and respond to advanced cyber threats that evade traditional security measures. Leveraged advanced security tools and analytics to hunt for signs of malicious activity within the network and endpoints. Demonstrated expertise in creating custom threat hunting queries and using behavioral analytics to uncover hidden threats.

Threat Research — Conducted in-depth threat research to analyze emerging cyber threats, zero-day vulnerabilities, and advanced attack techniques. Leveraged a wide range of sources, including security blogs, forums, dark web monitoring, and threat intelligence platforms, to gather valuable insights. Collaborated with internal security teams and external partners to develop timely and relevant threat advisories, providing actionable recommendations for mitigating risks and enhancing the organization's overall cybersecurity resilience. Published research findings to contribute to the cybersecurity community and stay at the forefront of evolving threat landscapes.

Attack Simulation — Implemented email security solutions, effectively mitigating phishing and malware threats.

Process Optimization — Streamlined processes through optimization and creation, enhancing overall operational efficiency and security posture.

Policy Development — Developed comprehensive security policies and ensured compliance with industry regulations and standards.

Risk Assessments — Conducted Assessments with the assistance of the CISA in identifying potential vulnerabilities in company infrastructure.

Emergency Incident Response — Responding to emergency situations in a timely and professional manner.

Access Control — Implemented and administered user accounts, permissions, and access controls across cloud services and networks. Implemented password management applications to enforce cyber policy.

Ecommerce Applications — Highly experienced in designing and maintaining most well-known applications not limited to setup, customer management, and automation. Clients include Mercury Marine, Mellow Mushroom, University of Tennessee- Knoxville, ZimVie Biomet, Mortgage Investors Group, Fat Brands, Brunswick Boat Group and more.

2FA Adoption — Implemented Two-Factor Authentication on all critical systems and implemented the use of Google Authenticator.
Executed a 2FA sprint to align all stakeholders and parties with access to critical systems.

Policy Assessments & Updates — Provided guidance and implemented solutions for updating policies and applications in order to comply with GDPR, CCPA and other regulations. Assumed leadership on projects with developers to insure websites were ADA compliant where required by law, and proactively working with clients in areas of concern where laws are still taking shape.

Cyber Security Training — Provided cybersecurity and computer usage training to employees. Built an internal web application for testing and training employees.
Created course materials and curriculum. Demonstrated hacking tools and techniques to illustrate key takeaways.

Digital Asset Management — Implemented an internal web application for the use of Digital Asset Management including Asset Security, Version Control and Permissions Usage.
Built a company sharepoint application to share news, events, cyber training and alerts, as well as a database for systems and application documentation. Maintained records of domains, servers and services.

Continuity & Redundancy — Created a database covering all aspects of our cloud network, applications and service providers. Created and maintained backups of digital properties and assets. Created backups for web applications and internal servers responsible for our cloud-based workflow.

Automation — Worked with employees to identify problem areas in order to process and automate tasks where available. Created a company intranet with various department portals, and an online ticketing system for IT to manage support requests.
Process design, database design, artificial intelligence.

Data Handling — Handled company and customer data with integrity and care with special attention to processes and access control. Versed in data handling processes and legal requirements regarding customer rights, CAN-SPAM, Sarbanes-Oxley and more.

Investigations — Conducted open source intelligence and reconnaissance investigations on alleged bad actors or cyber threats. Developed and implemented measured responses to eliminate threats.

References

Trent Draughon
(Supervisor) Director, Client Development Provisions Group
tdraughon@provisionsgroup.com

Stephen Ladner
Director, Corporate Sales, Threds Inc.
sladner@threds.com

James Evans
Creative Director, Threds Inc.
wevans@threds.com

Mike Mitchell
President, CTG Knoxville
Director, Information Technology, Threds Inc.
mmitchell@ctgknox.com