# Dan Jones

dan@shadowanalytics.net • (801) 336-8100
www.linkedin.com/in/danieldjones • Northern Virginia

**Demonstrated ability to solve difficult security problems while protecting businesses from cybersecurity threats.**

Detail-oriented and decisive security leader with broad and extensive experience managing all facets of cybersecurity programs for high-growth organizations. Repeated success overseeing and directing management of information security function to ensure the development and advancement of the information security program. Solid education with multiple industry certifications and active TS/SCI security clearance. Poised to build productive relationships with internal and external stakeholders to effectively manage high-severity privacy and network incidents and offer further opportunities for growth.

## Areas of Expertise

- Program Management
- Incident Response
- Risk Analysis & Mitigation
- Cross-Functional Leadership
- Stakeholder Engagement
- Regulatory Compliance
- Threat Intelligence
- Configuration Monitoring
- Penetration Testing

## Accomplishments

- Recruited by U.S. Army Reserve to provide civilian perspective needed to bolster defensive cyber security practices.
- Succeeded in securing MX Technologies with no findings during due diligence activities for Series B and Series C.
- Built two successful security organizations for startup organizations in a capital constrained environment that met or exceeded compliance and customer contractual expectations.
- Made significant contributions to a cloud security program and customer identity strategy at Zions Bancorporation.

## Career Experience

### Amazon.com, Arlington, VA [JAN 2021 – Present]

Sr Security Engineer (JUL 2023 - Present)

Member of the AWS Cloud Security Response team managing the security and availability of AWS Cloud services. Operate on the 'AWS' side of the AWS “Shared Responsibility Model” to ensure the "Security of the Cloud" and to protect our customers. This role required working tactically with both internal and external stakeholders to solve security challenges at massive scale, and to think strategically to develop and implement changes to drive automation, scalability, and continuous progress for the organization. 40+ hours/week, salaried.

- Triage/assess security issues and engage with internal service teams to ensure prompt remediation of issues, escalating internally as necessary to ensure the right level of urgency and engagement.
- Participate in efforts to promote security throughout the Company and build good working relationships within the team and with others across Amazon.
- Demonstrate high ability and tolerance for extreme context switching and interruptions while staying productive and effective.
- Develop pragmatic solutions that achieve business requirements while keeping an acceptable level of risk.
- Mentoring junior staff and proactive knowledge sharing within the team and across the company.
- Fulfill regular on-call responsibilities.

Security Engineer (JAN 2021 - JUL 2023)

Develop actionable intelligence on a variety of threats ranging from e-commerce crime groups, insider threats as well as other advanced cyber threats for all Amazon CDO (commercial, digital, and other) and AWS teams. Collect indicators and intelligence from a variety of internal and external sources to develop an understanding of threat actors and their tactics, techniques, and procedures. Use that understanding to proactively identify and mitigate malicious activity through OSINT and internal data sources. 40+ hours/week, salaried.

- Developed framework for the intelligence lifecycle at Amazon including coordination with incident response, detection, vulnerability management, red team, and threat hunting teams at Amazon.
- Build the intelligence management platform that coordinates collection efforts across the Amazon ecosystem at tactical, operational, and strategic levels.
- Created a novel approach to quantifying the threat that ransomware presents across Amazon. This approach was presented to the EVPs of Amazon and used to reprioritize security initiatives at various levels of the organization.
- Provided customer-facing reports where customer impact was possible or known in coordination with AWS Legal and the Office of the CISO. Provided data-driven analysis of findings along with next steps for customers based on industry best practice.

**LiveView Technologies, Lehi, UT [JUL, 2021 – AUG 2023]**
VP of Information Security

Built a cybersecurity team focused on digital and physical security for the company as well as the platform and customer hardware devices. Secure physical hardware devices with significant bandwidth restrictions that exist in public spaces as well as a SaaS based platform and API framework that connects with customer security and physical access control systems. 40+ hours/week, salaried.

- Provided a 2-year roadmap for team development to achieve SOC 2 Type I verification and FedRAMP moderate readiness. Achieved this goal 6 months earlier than anticipated.
- Implemented all fundamental domains of cyber security including acquisition of essential technology to properly secure all vital areas of the business including security architecture, penetration testing, security operations, threat intelligence/hunting, identity management, risk and governance.
- Introduced the Executive Leadership Team to the concept of a risk appetite. Facilitated the identification, tracking and management of business risks using a framework that demonstrated risks as they related to company OKRs. Enabled the business to take more risk in strategic areas due to increased awareness of strength/weaknesses.

**MX Technologies, Lehi, UT [AUG 2018 – JUL 2021]**
Director of Information Security

Serve as subject matter expert across all information security domains while holding concurrent responsibility for leading end-to-end design of all technical security measures. Apply advanced knowledge of enterprise architecture, security fundamentals, and strategic technologies to build a highly effective cybersecurity program. Define policies, guidelines, and procedures concerning the handling of intellectual property. 40+ 40+ hours/week, salaried.

- Valued by senior management teams for continually developing unique and cost-effective solutions in response to complex security problems.
- Proved highly effective in allocating a broad workload amongst cross-functional team members including security architecture, penetration testing, security operations, identity management, threat intelligence/hunting, risk and governance.
- Succeeded in growing the cybersecurity team by 2.5 times each year of tenure.

### Zions Bancorporation, Salt Lake City, UT [OCT, 2010 – AUG 2018]

Enterprise Architect (MAR 2018 – AUG 2018)

Responsibility and accountability for designing customer and workforce IAM solutions. Owned responsibility for planning, designing, reviewing, and facilitating implementation of IAM initiatives to support core security functions with a specific emphasis on fraud detection and prevention. 40+ hours/week, salaried.

- Played an integral role in supporting the creation and deployment of a cloud security solution and a customer identity strategy.
- Entrusted to develop and maintain information security standards and processes that aligned with industry best practices and regulatory statutes.

Senior Threat Intelligence Engineer (JAN 2013 – MAR 2018)

Tasked with identifying security events and incidents threatening organization's IT function. Analyzed large datasets using efficient and scalable processes that support data reliability and integrity. Built relationships with external stakeholders to gain additional intelligence about malware authors and other similar fraud actors. 40+ hours/week, salaried.

- Transformed capacity vulnerability management and security operation functions with development and implementation of an initial threat intelligence program.
- Recognized as computer forensics expert in execution of fraud, human resources, legal, and security investigations.
- Performed threat hunts for threats relative to the organization based on relevant threat intelligence from both public and private intelligence.

Information Security Engineer (OCT 2011 – JAN 2013)

Coordinated administration of vulnerability management program for banks across nine states. Conducted in-depth risk assessments of vulnerabilities across corporation and communicated readily with system owners to ensure full understanding of pending risks and probable solutions. Designed and managed procedures for reporting systems. 40+ hours/week, salaried.

- Pioneered establishment of a root cause-based vulnerability management program that featured state of the art hunting practices.
- Led automation of key systems to perform data discovery of potential security issues, building customer software tools, as needed.
- Promoted to position after successful one-year tenure as Information Security Analyst.

## Additional Experience

### US Army Reserve, Cyber Warfare Officer
### CPT(P) O-3, SEP 2020 to Present

Developed and validated a concept of operations that enables the proactive use of Army Reserve Cyber Operators to be on mission during normal training cycles. Lead numerous defensive cyber operations in Europe working with NATO partners to develop complementary defensive practices and information sharing where appropriate. Provided strategic and operational briefs to US and NATO partner general officers. Training multinational forces on effective threat hunting and intelligence strategies.

- Leading the efforts to establish an Army Reserve Intelligence unit focused on Cyber Threat Intelligence for DCO/OCO operations as the Chief of Cyber Intelligence for the Military Intelligence Readiness Command.
- Developed SOPs for threat hunting that were adopted for all threat hunting related missions taken on by ARCPB. Also built out the operational framework used to scope, size, align and contract with new mission partners.

- Part of a team working on developing a continuous ATO DevSecOps pipeline for rapid deployment of Army capabilities in Cloud Environments.

## Education

**Master of Business Administration**
Western Governors University, Salt Lake City, UT – DEC 2016 to NOV 2018

**Master of Science in Information Security & Assurance**
Western Governors University, Salt Lake City, UT – FEB 2010 to DEC 2012

**Bachelor of Science in Information Technology**
Western Governors University, Salt Lake City, UT – JUN 2009 to DEC 2010

## Certifications

Active TS/SCI
CIW Associate, Database Design Specialist, JavaScript Specialist & Professional
CompTIA A+, Network+, Project+, Security+
EC Council Certified Ethical Hacker (CEH) & Certified Hacking Forensics Investigator (CHFI)
GIAC 27000 Specialist – G2700, GIAC Certified Incident Handler - GCIH, GIAC Reverse Engineering Malware - GREM, GIAC Cyber Threat Intelligence - GCTI, GIAC Certified Forensics Analyst - GCFA, GIAC Certified Penetration Tester - GPEN
MS Certified Technology Specialist

## Technical Proficiency

| | |
|---|---|
| **Data Analytics:** | Apache Hadoop; Hive; NoSQL; Elasticsearch/ELK; Jupyter/Sagemaker; MongoDB; MySQL; PostgreSQL |
| **Languages** | Java; JavaScript; Python; Ruby |
| **Networking Tools:** | Checkpoint; Citrix Access Gateway; Cisco; Juniper; Palo Alto; Wireshark |
| **Security Tools:** | BlackBag Suite; Carbon Black; Crowdstrike; Ghidra, Ida Pro; Logicube Forensics Falcon; Axiom/Magnet Forensics; Maltego; McAfee; MITRE ATT&CK Navigator; MISP; OpenCTI; OSQuery; Recorded Future; SentinelOne; Snort; Splunk; Suricata; X-Ways |

## Inventions and Patents

**Data Protection Query Interface** US 20220035943 A1 · Issued Feb 3, 2023