john@thedelay:~$ whoami

John DeLay

Head of Information Security and IT

Chicago area / john@thedelay.com / linkedin.com/in/john-delay / thedelay.com

I run IT and information security, and for 20+ years I've done this work at organizations ranging from scrappy startups to enterprise environments. I came up through IT and systems engineering, building data centers and running thousands of servers, and I never left IT behind when I moved into security leadership.

CAREER	PACKBACK	PACKBACK	PACKBACK	PACKBACK	HOME PARTNERS
20+	**$160K+**	**95%**	**2.5x**	**139**	**1,400+**
years in IT and security	a year in run-rate savings, no added headcount	reduction in HECVAT response effort, using AI	InfoSec and IT tickets resolved, year over year, while bringing IT in-house	vulnerability tickets closed	devices in a company-wide rollout, completed in eight weeks

Experience

Packback · Head of Information Security and IT

Aug 2024 – Present

RUNNING IT

- Replaced the company's managed IT provider by taking over day-to-day IT myself, on top of security, saving $160K+ a year in run-rate with no added headcount and a specialist partner for overflow.
- Run IT day to day: help desk, onboarding and offboarding, laptops, device management, endpoint protection and the asset register.
- Ran the migration hands-on: moved the laptop fleet to company-owned device management and endpoint protection using my own migration script, bought licensing direct and right-sized it (76% lower), and stood up an asset register and a single intake for IT requests.
- Grew InfoSec and IT tickets resolved 2.5x year over year while bringing IT in-house.

SECURITY OPERATIONS

- Built vulnerability management from scratch into a weekly operation, closing 139 vulnerability tickets and merging 50+ of my own security fix PRs.
- Cut SIEM alert noise 73% through tuning. Built a threat-detection program with 70+ detections, alerts routed by severity, and automated health checks on the detection pipeline itself.
- Own identity and access management across the SaaS portfolio, including SSO and SCIM, as the company's sole expert. Run quarterly access audits. Lead incident response end to end, including blameless postmortems.
- Took DMARC to full enforcement in about six weeks with a 98.5% pass rate and zero delivery incidents.

COMPLIANCE AND AI

- Built and shipped a production AI compliance assistant for security questionnaires and RFI/RFQ responses, cutting HECVAT responses from a multi-week, multi-person effort to hours, a 95% reduction. It answers from official documentation only, with source citations and confidence levels.
- Wrote the company's employee AI guidance, which serves as its AI policy: which AI tools and data connections are approved, limited to certain teams, or need a review first.
- Run the SOC 2 Type 2 program end to end, including auditor fieldwork, and the TX-RAMP recertification. Handle customer security reviews and RFPs for 22+ institutions. Serve as Data Protection Officer.

Home Partners of America · Information Security Officer

Mar 2022 – Aug 2024

- Deployed Kandji for Macs, Microsoft Intune for Windows and Automox for patching across both, from scratch, across a geographically dispersed fleet of 1,400+ devices, completing the company-wide rollout in eight weeks.
- Got an overseas laptop fleet PCI-compliant within six weeks, a first for the organization, with minimal employee friction.
- Owned ServiceNow and worked across the wider IT stack, including Workspot VDI, Azure AD, Keycloak and Zscaler.
- Built the business cases and executive presentations behind Automox, Kandji, 1Password, SentinelOne and other major platform investments. Negotiated six figures in savings across three security vendors.
- Led incident response across multiple events, coordinating with parent company stakeholders. Earned trust through transparent communication and demonstrated competence, to the point that leadership stepped back and let the team operate independently.
- Reduced audit violations and improved control effectiveness. Performed regular risk assessments of likelihood and impact, giving the business clear justification for risk reduction.

Salesforce · Product Security Lead

Jan 2022 – Mar 2022

› Joined through Salesforce's acquisition of Narrative Science and kept managing the same environment. Led the security workstream for M&A integration, and managed the security team responsible for SOC 2 certification, customer contracts, incident response and risk assessment during the transition.

Narrative Science · Lead Information Security Engineer

Oct 2017 – Dec 2021

› Ran all of IT for the company while building its security program, from the network to the laptops to the AWS servers.

› Built out the company's information security program, establishing best practices, governance and compliance frameworks that kept SOC 2 reports clean and passed client security audits.

› Evaluated and implemented AlienVault USM as the company's SIEM after conducting quantitative risk assessments and presenting the findings to executive management.

› Developed the Computer Incident Response Methodology. Managed the company's Apple devices with Jamf. Served as primary contact for customer security engagements, from basic security practices to complex contract negotiations.

Systems Administrator

Jun 2015 – Oct 2017

› Ran all of IT for the company. Led the effort to obtain the company's first SOC 2 Type 2 letter, received clean in 2017.

› Created the company's first system for responding to customer security inquiries, significantly reducing RFI effort and establishing contract tracking.

› Designed and built enterprise-grade AWS infrastructure using CloudFormation, EBS, EC2, Route 53, S3 and VPC, with disaster recovery and business continuity capabilities.

Nokia · Systems Administrator → Senior Systems Administrator → Senior System Engineer

Aug 2007 – Mar 2015

› Led the design and construction of a new data center, coordinating with business leaders to complete the migration without serious business interruptions.

› Implemented high-availability Xen clusters with rapid failover using Hitachi storage frames and redundant fiber-optic networks. Designed, implemented and supported thousands of servers running Red Hat Linux and Windows.

› Conducted security vulnerability assessments, monitored SIEM and IDS/IPS systems (Splunk), and provided Tier 3 support as the escalation point for hardware, OS and application troubleshooting.

Aegon · Senior Network Analyst → Lead Network Analyst → Lead Server Engineer

1999 – 2007

› Ensured Sarbanes-Oxley compliance policies and systems were effectively and consistently enforced. Deployed and provisioned racks, PDUs, data centers and thousands of servers across geographically dispersed environments.

Personal projects and writing

`jaid-observability-platform`: self-hosted observability for AI coding sessions (context, cost, subagents).

`project-management-plugin`: a planning skill for coding agents; done only on evidence.

`claude-context-starter-kit`: role-based context templates and a security program starter pack.

`video-transcriber`: download, transcribe with Whisper, and outline a YouTube video.

30+ articles on security, AI and homelab at thedelay.com.

Education

Kirkwood Community College: courses toward a degree in Criminal Justice

Skills

SECURITY AND COMPLIANCE Information Security, SOC 2, TX-RAMP, PCI DSS, Sarbanes-Oxley, FERPA, HECVAT, Incident Response, Vulnerability Management, Risk Management, Vendor Management, DMARC

IT AND ENDPOINTS IT Management, ServiceNow, Microsoft Intune, Kandji, Jamf, Automox, SentinelOne, Microsoft Defender, Workspot, Okta, Auth0, Microsoft Entra ID (Azure AD), Keycloak, 1Password, Single Sign-On, SCIM

INFRASTRUCTURE AWS, Microsoft Azure, Google Workspace, Cloudflare, Zscaler, Red Hat Linux, Windows Server, VMware, Virtualization, Network Administration, Data Center Design, Ansible