Matt Linton (matt@mattlinton.com)

Incident Response, PSIRT, & Crisis Management Leader

https://www.linkedin.com/in/mattlinton/

Key Skills

I am a **recognized leader in security**, including the PSIRT and DFIR communities. I've managed a team of 20 very experienced (Senior and Staff Eng) employees, mentored dozens more, & overseen other managers

I am a **DFIR domain expert, formally trained in crisis management**, with extensive experience in both information security & real-world disaster response

I have prepared & run **contingency plans and risk mitigation** projects to prevent cybersecurity incidents and map out optimal responses if they do occur

I have field and operational experience filling multiple IT and cybersecurity positions, including (but not limited to) **system administration, digital forensic analysis, incident response, compliance, and security engineering,** and I work hard to maintain technical proficiency

I am an **experienced technical communicator** and comfortable working with auditors, regulators, lawyers, & and executive leadership in addition to technical staff

Google *(2014 → Present)*

Manager, Security Response Americas Region & **Global Technical Lead**, Security Response discipline

Impacts:

Grew, trained, & professionalized a mixed-discipline on-call team of crisis managers & forensic experts, from 4 to 20 full-time employees (FTE). My focus on burnout prevention resulted in **improved retention of key staff**

Developed procedures and operational paradigms and **oversaw operations of 300+ Engineers & Analysts** to ensure fast, reliable 24/7 coverage of potential incidents

Represented Google in CISA/JCDC's cross-industry **"AI Incident" Response planning effort**, providing insight into Artificial Intelligence (AI) as it relates to practical security risks

Co-created IMAG & led training of thousands of engineers to successfully execute a unified response model for Availability, Security, & Privacy incidents

Published & communicated in many venues about my professional and technical work

Led global-scale security and privacy responses, including pre-embargo coordinated disclosure of Spectre & Meltdown, response to log4j, the Frameshift DDOS vulnerability, Active attacks by APT threats, and more

NASA Ames Research Center *(2000 → 2014)*

Security Engineer → Deputy CISO of a $600M, 4,000+ employee research lab with a top-3 supercomputer & numerous unique, challenging security environments

Impacts:

Designed and implemented secure environments for: a National wind tunnel complex, the world's largest interactive flight and air traffic control simulators, a SCADA environment, a Mission Control center, NASA's Advanced Supercomputing environment, the general administrative and wireless IT environments, a private Government Cloud service, & many other diverse computing environments

Provided community service as a **DNS Root Server operator** for the "E" Root server

Performed CSIRT functions as an on-call responder, investigating crimes against the government, IT fraud and abuse, and policy violations

Served as liaison between Scientists, Engineers, Management, and Policymakers, ensuring alignment between varied stakeholders with opposing needs & experiencing resource scarcity - **operating at low cost with high resourcefulness**

Performed security oversight for USGov classified information systems as a Designating Approval Authority