Matt Linton - Cybersecurity & Response Expert

Matt is a recognized leader in cybersecurity, specializing in Digital Forensics & Incident Response (DFIR), Product Security Incident Response (PSIRT), and crisis management. He has extensive experience in both information security and real-world emergency response, managing and mentoring teams of experienced engineers and analysts.

Work Experience

Google - *Mountain View, CA*

Manager & Regional Lead, Security Response | (2020 – 2025)

Lead of the Americas (North/South AMER) region for the Google Cybersecurity Response team

- Grew, trained, & professionalized a mixed-discipline on-call team of crisis managers & forensic experts to 20 full-time employees (FTE). Focused on burnout prevention resulting in improved retention of key staff.
- Developed procedures and operational policy, oversaw operations of a broader team of 300+ Engineers & Analysts to ensure efficient, reliable 24/7 coverage of potential incidents via case reviews and "Virtual Security Operation Center" oversight.
- Represented Google in government and customer regulatory coordination to ensure compliance with law and contracts pertaining to incident response globally.
- Led the "Incident Management At Google" (IMAG) program as curriculum developer and owner, driving Google to unified incident response procedures companywide.
- Led incident response activities for complex security investigations of external attacks against Google and insider activity. Assisted with logs analysis and review, oversaw analyst work.
- Provided expert guidance on security best practices and emerging threats.
- Created & Led "Incident Response Council" - a cross-disciplinary review board aligning Security & Reliability senior staff on incident response practices.
- Created & Led "Tabletop trainings" for google-wide teams to ensure regular training and exercise for engineers, leaders, legal and others involved in response activities.

Staff Security Engineer | (2018 – 2020)

Senior Technical Lead for Detection & Response team.

- Designed and implemented advanced security solutions for critical infrastructure.
- Conducted in-depth security investigations and forensic analysis including logs and digital artifact analysis.
- Coordinated major incident response activity for attempted intrusions into Google by outside parties and suspected insider activity.
- Led PSIRT operations for complex supply chain vulnerabilities.
- Provided expert guidance on security best practices and emerging threats.
- Created & led "Tabletop exercise" program to ensure regular training and exercise for response staff.

Senior Security Engineer | (2015 – 2018)
Security Engineer III | (2014 – 2015)

Oncall incident responder and forensic analyst for the Detection & Response team

- Coordinated teams to assess, respond and fix large-scale and internet-scale security vulnerabilities such as the “DNSMasq” security bugs and the “Spectre & Meltdown” global CPU vulnerabilities.
- Developed and maintained security tools and automation scripts for use by the digital forensic team.
- Responded to security alerts and conducted initial incident triage.
- Performed forensic investigations, root-caused events and potential malware executions and compromises.
- Conducted in-depth security investigations and forensic analysis including logs and digital artifact analysis.
- Led incident response activities for large-scale incidents.
- Implemented Incident Management At Google (IMAG) ultimately training thousands of Google employees in a custom variant of the National Incident Management System’s Incident Command System (NIMS ICS) for performing incident response focused on system outages and cybersecurity investigations.

NASA Ames Research Center - *Moffett Field, CA*

Deputy CISO & Lead of Incident Response Team (GS-2210-14) | (2012 – 2014)

Technical lead of operational staff and direct assistant to the CISO, bridging policy and practice to ensure compliance with security policy in ways that allowed for the research and engineering community to perform their jobs with minimal disruption

- Assisted the CISO in developing and implementing agency-wide information security policies and procedures.
- Managed security compliance and risk assessment programs.
- Oversaw security awareness and training initiatives, including providing training to other NASA staff in cybersecurity and incident response.
- Served as secondary Designating Approval Authority (DAA) for classified information processing systems at NASA SOC.
- Led incident response team (2 Civil servants & 5 Contractors) staff to ensure effective IR on NASA Ames systems.
- Selected as a “Senior Expert” reviewer for United States Air Force “Cyber Vision 2025” planning and long-term strategy document.

Lead Engineer, NASA Security Innovation Laboratory (GS-2210-13) | (2012 - 2014)

Researched and implemented cutting-edge and low-cost security improvements for NASA Ames

- Experimented with, produced and operationalized new security tooling and techniques to protect research and mission systems at NASA Ames.
- Led security design of the NASA Ames Multi-Mission Operation Center (MMOC).
- Led security design and implementation of NASA ARC “SCADA Network”.
- Led security design and implementation of the NASA “Nebula” private computing cloud - one of the earliest private cloud deployments in the US Government.
- Provided technical and security support to the “E” internet root nameserver and the root-operations community.
- Provided training in cybersecurity to NASA staff and contractors, including cross-agency and public

speaking as needed.
- Winner: National Cybersecurity Innovation Award 2012 & 2013 for NASA IPOST and Nebula.

Information Security Specialist, Incident Response (GS-2210-13) | (2010 – 2012)

Performed internal security investigations and work alongside the NASA Office of Inspector General (OIG) to support evidence gathering for their ongoing investigations

- Led incident response efforts, including detection, analysis, containment, and eradication.
- Developed and refined incident response plans and procedures.
- Conducted post-incident reviews and identified lessons learned.
- Conducted penetration tests and security assessments of both network infrastructure and physical computing and processing infrastructure.
- Write scripts, programs and automation to facilitate performing tasks at scale.
- Created and executed automated programs to facilitate vulnerability discovery and asset management across the network.

Information Security Specialist (GS-2210-12) | (2008 – 2010)

Protective cybersecurity engineer for NASA mission-related IT systems

- Developed information security standards and implemented tooling to support the Constellation space missions.
- Administered security systems and tools.
- Monitored network traffic and system logs for security events.
- Provided technical support for security-related issues.
- Write scripts, programs and automation to facilitate performing tasks at scale.

Rescue Captain - NASA | (2000 – 2014)
Rescue Specialist - California Task Force 3 | (2008 – 2021)

Paid (As part-time duty at NASA and as on-call at CATF3) Rescue Specialist

- Trained, practiced and maintained skills as a deployable heavy USAR specialist.
- Deployed as needed to support emergency response duties, standby EMS and Rescue duties.
- Assisted in research and development of new mechanisms for advancing USAR (e.g., Shore testing and development, Rescue Robotics).
- Led others as Captain of NASA Dart “Water Rescue Specialist” unit.

ASANI Solutions, LLC - Contractor to NASA Ames Research Center

UNIX & Linux Information Systems Security Officer (ISSO) | (2003 – 2008)

System Administrator responsible for setting and ensuring security standards for research and engineering systems at NASA’s computer science and human factors research department

- Continued system administration duties from 2000 - 2003 and additionally was the main security point of contact for the “Code TI” research labs.
- Ensured compliance with federal security regulations and policies.
- Developed and maintained system security plans.
- Conducted security audits and assessments.
- Implemented tooling to secure and monitor research and operational computing systems for the NASA Ames computational sciences division.

- Write scripts, programs and automation to facilitate performing tasks at scale.

UNIX & Linux System Administrator | (2000 – 2003)

System Administrator responsible for the reliable performance of general computing systems

- Managed and maintained network infrastructure and server systems.
- Provided technical support to users.
- Implemented and troubleshot software and hardware.
- Wrote scripts, programs and automation to facilitate performing tasks at scale.

Onyx Networks, Inc

Junior UNIX System Administrator | (2000 – 2000)

Entry-level system administration assistant learning the trade under a senior network engineer

- **Account Management:** Created, modified, and managed user accounts on UNIX systems, including setting up home directories and permissions.
- **Access Control:** Managed access rights and permissions for files and directories to ensure proper security and data segregation.
- **System Monitoring:** Monitored system performance, resource utilization (CPU, memory, disk space), and network activity for anomalies or potential issues.
- **Helpdesk Support:** Responded to and resolved helpdesk tickets related to UNIX system issues, user access problems, and basic application support.
- **Troubleshooting:** Diagnosed and resolved common system problems, such as process failures, full disk partitions, or connectivity issues, under senior guidance.
- **Log Analysis:** Reviewed system logs to identify errors, security events, or other operational concerns.
- **Documentation Assistance:** Assisted the senior administrator in maintaining and updating system documentation, procedures, and troubleshooting guides.

Volunteer & Other relevant experience

Technical Director - Mickaboo Companion Bird Rescue (2001 – Present)

- Advised the organization on the best technical strategy for internet tooling and infrastructure to operate a 100% distributed volunteer animal rescue with no physical location.

Concert Emergency Medical Technician - RockMed (Rock Medicine) (2014 – 2020)

- Provided emergency medical services at rock concerts and other large public events.

Firefighter - Half Moon Bay Volunteer Fire Dept (2024 – Present)

- Trained regularly and responded to emergency calls and general alarms as a Firefighter on Engine 141 in Coastside Fire Protection District.

Internships & Part-Time work during College

Lifeguard & EMT - Maryland State Parks (1998 – 2000)

Lifeguard - Various pools in Frederick MD (1996 – 1998)

EMT & Firefighter (1996 – 2000)

- Elkridge Volunteer Fire Department
- Walkersville Volunteer Rescue Department
- National Park Service - Search & Rescue Intern
- UMBC EMT internship positions around Baltimore, MD

Security / Engineering Certifications

- **2016**: SANS FOR585: Smartphone forensic analysis in-depth
  - *Winner - Final course challenge competition, “Lethal Forensicator”*
- **2015**: SANS FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics
  - *Certification obtained: **GIAC Certified Forensic Analyst** - GCFA (Jun 2015) CN#11037*
  - *Winner - Final course challenge competition, “Lethal Forensicator”*
- **2014**: SANS SEC408: Windows Forensic Analysis
  - *Winner - Final course challenge competition, “Lethal Forensicator”*
- **2004**: SANS SEC504: Hacker Tricks, Techniques, and Incident Handling
  - *Certification Obtained: **GIAC “Certified Incident Handler”** credential*
- **2003:** SANS SEC503: Intrusion Detection In-Depth

Continuing Education

- **2014 - Present**
  - Provided and took annual internal training at Google on topics including:
    - Investigative mindset for forensics.
    - Incident Management at Google.
    - Digital forensics training to include log analysis.
    - Updated technical information about logging systems.

- Handling “Controlled Unclassified Information” for US Government customers
- Managing operational teams.

- Attended and spoke at Digital Forensics and Incident Response (DFIR) related conferences (e.g., SANS DFIR Summits)
  - Refreshed skills on host forensics investigations, cloud forensic investigations.
  - Performed experiments and research including “USB PWNY Express – Counterfeit USB Device AntiForensics.”
- Attended and spoke at industry conferences (e.g., Black Hat, DEFCON)
  - Networked with other professionals, traded tips on current investigative methods.
  - Attended talks to learn current investigative techniques and methods of obtaining digital artifacts.

Emergency Response Training

Course	***Most Recent Recertification date***
Public Safety First Aid (California)	2/9/2025
Fire Control 3	3/9/2025
S-190 Weather and Wildland Fire Behavior	3/31/2025
L-180 Wildland Firefighting Tactics	3/31/2025
CERT Instructor	1/30/2023
CERT Basic	2/8/2023
Rope Rescue Technician	8/31/2018
NFPA 1500 Respiratory Protection Refresher	5/8/2017
Haz-Mat FRO Refresher for CATF3	7/23/2014
Rope Rescue Awareness Refresher	9/1/2011
Structural Collapse Technician (FEMA, Combined SCT)	1/11/2011
Rescue Systems 2	12/1/2010
ICS 400	9/1/2010
Trench Rescue	10/28/2009
ICS 100	12/16/2007
IS800 National Response Plan	10/16/2007
NIMS IS-700	10/15/2007
Weapons of Mass Destruction Response	10/12/2007
Collapsed Structure Rescue (NASA)	5/12/2007
Swiftwater Rescue Technician 1	2/13/2005
ICS 300	1/26/2005
Confined Space Operations	7/1/2004
IS10, IS11 (Animals in Disasters)	12/7/2003
Swiftwater Rescue Technician Advanced	10/19/2003
Rescue Systems 1	9/6/2003
Hazardous Materials Operations	7/23/2003
ICS 200	2/4/2003
Emergency Medical Technician (California)	~ 6/2000
Managing Search Operations	5/1/1999
Firefighter 1	1/6/1998
Emergency Medical Technician (Maryland)	2/8/1997

Publications / Speaking

Representing Google

- “Hacking Google” ep 002, “Detection and Response”
- Co-Author: “Building Secure & Reliable Systems” (Chapter 15: Investigating Systems)
- Author: “Building Secure & Reliable Systems” Chapter 17: Crisis Management
- Burnout: My Invisible Adversary (video) (Black Hat EU 2023 Community Talk)
- Security Weekly - Incident command (video)
- “Excuse me while I kiss this guy” - What you said isn’t what they heard
    - Talk to FIRST Incident Response forum about incident communications and how to do it better.
- “Behind the Speculative Curtain (video) ” - Black Hat Panel on Spectre & Meltdown.
    - Live panel w/ Red Hat, Microsoft, Google, CERT-CC
    - Audience size ~1,100
- “CPU Security” for Google Cloud Podcast (audio) (M. Linton, P. Turner)
    - 30 minute technical breakdown of CPU Side channels
- “You are the Weakest Link - and that’s OK”
    - Talk about the technical and sociological realities of why phishing works so well, and what can be done about it.
- SANS DFIR Summit Lightning talk: “Network Disasters - when the bits hit the fan (video)”
    - Talk delivered entirely in the form of a Dr. Seuss book (to win a bet).
- “The Remediation Ballet” - Incident Response at Scale
    - SANS Threat Hunting & IR Summit 2016
    - FIRST Information Security Summit 2018
- Exploitation in Meatspace - Physical Penetration Testing Tips
    - SANS Pen-Test Hackfest 2015
- “Go ahead, run your own mailserver - what, are you chicken?”
    - SANS Pen-Test Hackfest 2016
- SANS DFIR Summit War-Games
    - 2018, 2019 war-game exercises
- https://www.youtube.com/watch?v=hhUQcUZ4GJ8 (Forensic Lunch w/ David Cowen)

Representing NASA

- NASA Nebula - NASA’s secure by default private cloud
    - SANS Cyber Security Innovation Summit (2013)
- NASA and IPOST: Security automation and gamification
    - SANS Cyber Security Innovation Summit (2012)
- Oct 2010 - California CIO Information Security Forum (video)
    - Representing NASA for Cloud Security (in 2010, cloud was a pretty new thing)

Selected Blog Posts

- https://medium.com/@matt_97344

- Operational Professionalizing vs Proceduralizing
- On Burnout in Cybersecurity
- You can’t Incident Command an Email Thread
- Proving Negatives
- On Fire Drills and Phishing Tests (blog)
- “Beats & Bytes: Striking the right Chord in Digital Forensics” Ryan Pittman, Cindy Murphy, Matt Linton