

LUCAS GUNDRY

CORPORATE / ENTERPRISE SECURITY ENGINEER | Identity | Endpoint | Security Operations | Automation

lucas@lucasgundry.com | linkedin.com/in/lgundry/ | California

SUMMARY

Hands-on Security Engineer with 10+ years across corporate security, security operations, and IT infrastructure. Experienced owning identity, endpoint, SaaS, network, vulnerability, and detection controls; building onboarding and access workflows; leading incident response; and supporting SOC 2, ISO 27001, HIPAA, CIS, NIST, and FedRAMP environments. Current work includes SentinelOne, Datadog SIEM, Okta, Google Workspace, fraud and phishing investigations, and Claude Code. Comfortable operating as a broad security owner and partnering with IT, Engineering, HR, Legal, auditors, and leadership.

TECHNICAL

Identity & SaaS: Okta, Entra ID / Azure AD, OneLogin, SSO, MFA, RBAC, access reviews, JML, Google Workspace, Microsoft 365 | Endpoint & Network: CrowdStrike Falcon, SentinelOne, Red Canary, Jamf, Intune, Defender, Carbon Black, Cloudflare, Meraki, VPN, ZTNA/CASB | Security Operations & Risk: Datadog SIEM, Elastic SIEM, Splunk, QRadar, XSOAR, DLP, vulnerability management, incident response, threat hunting, vendor risk, SOC 2 / ISO 27001 / NIST / CIS / HIPAA / FedRAMP | Automation & AI: Claude Code, MCP integrations, Torq, Bash, APIs, Docker, Git/GitHub, Terraform (lab)

EXPERIENCE

Security Engineer (Contract) | Altruist | 08/2026 - Present | San Francisco, CA

- Investigate endpoint, identity, phishing, and fraud-related security activity across SentinelOne, Datadog SIEM, Okta, Google Workspace, and Sardine.
- Tune Datadog detections and investigation workflows by refining filters, suppressing known-benign patterns, and adding context where coverage or triage is weak.
- Use Okta Admin and Google Admin to review account, sign-in, access, and user activity during investigations and response.
- Use Claude Code for investigation enrichment, SIEM analysis, and repeatable security workflows while keeping consequential actions under human review.

Senior Security Engineer (Contract) | Vera Therapeutics | 10/2025 - 04/2026 | Brisbane, CA (Remote)

- Owned security engineering work across endpoints, infrastructure, cloud services, and operational controls, from hardening and troubleshooting through remediation.
- Led a vulnerability management platform from proof of value through selection and implementation, then worked with system owners to establish a practical remediation process.
- Led evaluation and design of ZTNA and CASB capabilities, balancing access requirements, network behavior, user impact, and security risk.
- Investigated activity through Red Canary and SentinelOne; maintained technical standards, runbooks, risk assessments, and controls supporting ISO 27001, NIST, HIPAA, and SOC 2.

Cyber Engineer / Analyst | Armis | 08/2022 - 03/2025 | San Francisco, CA (Remote)

- Helped build and run the security operations program across endpoint, identity, cloud, SIEM, DLP, vulnerability management, and incident response.
- Administered CrowdStrike Falcon for endpoint security and response, including investigations, containment, prevention policy, and operational troubleshooting with IT.
- Reworked SIEM detections and correlation logic, reducing alert volume by roughly 30% while preserving useful coverage and improving responder context.
- Implemented DLP controls that reduced exposed storage files by 50%, working through findings, exceptions, and remediation with data owners.
- Served as Incident Commander and sole responder for the FedRAMP GovCloud environment, coordinating containment, recovery, after-action reporting, and control improvements.

Corporate Security Engineer | Demandbase | 08/2021 - 08/2022 | San Francisco, CA

- Administered corporate identity, endpoint, and security systems across Okta, Entra ID/Azure AD, Conditional Access, Intune, Microsoft Defender, SentinelOne, Red Canary, Cloudflare, Jamf, and AWS.
- Restructured Okta around joiner-mover-leaver workflows, SSO/MFA, group-based access, role changes, onboarding/offboarding, and recurring access reviews.
- Managed endpoint policy through Jamf and Intune and investigated endpoint events through SentinelOne and Red Canary, including policy conflicts and user-impacting issues.
- Administered Microsoft 365 security and compliance controls across endpoint, email, identity, and data protection, including Defender and Purview.
- Partnered with IT, HR, Engineering, Legal, and leadership on access reviews, third-party risk, audit evidence, remediation decisions, and SOC 2 / ISO / CIS control work.

24/7 SOC / Threat Analyst | PG&E | 08/2020 - 08/2021 | Concord, CA

- Investigated alerts in a regulated 24/7 SOC using QRadar, endpoint telemetry, network data, and threat hunting; used XSOAR to document and coordinate response.
- Triageed Endgame endpoint alerts and supported firewall, network segmentation, and containment work during active investigations.

Security Operations & IT Manager | Peerspace | 11/2018 - 03/2020 | San Francisco, CA

- Built the company's IT and security function as the first internal owner, covering Okta identity, employee onboarding/offboarding, endpoints, SaaS, networks, email security, and incident response.
- Implemented Okta SSO/groups, managed Jamf/MDM and Carbon Black endpoint security, Google Workspace, Meraki networking/firewalls, SaaS access, 1Password, and DMARC/DKIM/SPF.

- Worked directly with leadership, HR, Engineering, Legal, and Finance on access, vendor decisions, risk, budgets, and security priorities; automated routine checks with Bash.

Senior IT Engineer | Indeed | 10/2016 - 11/2018 | San Mateo, CA

- Administered macOS, Windows, and Linux environments with Google Workspace, Jamf, OneLogin, Active Directory/LDAP, Duo, GlobalProtect VPN, NAC, firewalls, asset inventory, and office infrastructure.
- Managed SSO and SaaS access, employee provisioning, office/network infrastructure, and troubleshooting across a large enterprise environment.

IT Support Specialist | Varsity Technologies | 08/2015 - 10/2016 | San Francisco, CA

- Supported 25+ nonprofit client environments across Windows Server, macOS, Linux, VMware, Cisco/Meraki networking, IAM, and HIPAA-regulated systems.

PROJECTS

AI Security Homelab | Personal Project | 2026 - Present

- Maintain an Ubuntu/Docker security homelab using Claude Code, Okta, Terraform, Git/GitHub, and MCP-style integrations to practice corporate-security and detection workflows.
- Build fictional identity, endpoint, and SIEM scenarios to practice investigation, access changes, false-positive tuning, and human-in-the-loop controls without granting an LLM unrestricted administrative authority.

EDUCATION & CERTIFICATIONS

CSU East Bay - Economics | GCIH | CompTIA A+ | CompTIA Network+ | CompTIA Secure Infrastructure Specialist (CSIS) | CompTIA Security+