MAXIMILIAN SANFORD BURKHARDT

root@maxb.fm :: [LinkedIn]

Education

- ◇ UC Berkeley College of Engineering: Bachelor of Science in Electrical Engineering & Computer Science (2013).

Areas of Expertise

- ◇ **Information Security Generalist**, with experience in diverse areas including application security, cloud infrastructure & network security, corporate security and zero-trust architectures, cryptography, radio frequency (RF) security, and malware analysis. Experience in securing both B2B and consumer-facing SaaS applications, at multiple stages of security program maturity.
- ◇ **System Designer and Architect**, with background both in high-scale, cloud-native, distributed systems (Airbnb, Figma) and traditional on-prem corporate networks (NCC Group, UC Berkeley).
- ◇ **Infrastructure Engineer & Incident Responder**, having built backend systems at both Airbnb and Figma, and held the sitewide pager for both of these companies at scale.

Work History

- ◇ **Security Manager, Figma** (2022–2023): Managed the Corporate Security team, focused on employee endpoint defense and internal permission systems.
  - ○ Managed a team of 4 individual contributors while also delivering technical impact (as a tech-lead manager).
  - ○ Grew team from 1 to 4 as the founding manager of the team.
- ◇ **Staff Security Engineer, Figma** (2020–2022): Early member of the security function at Figma; founded the infrastructure and corporate security programs. Notable projects included:
  - ○ Designed and implemented Figma's AWS multi-account transition, taking the infrastructure from a single AWS account to a segmented network of accounts for security and reliability benefits.
  - ○ Developed Figma's zero-trust strategy & technology for corporate access to internal resources, enabling a flexible remote workforce (see Inside Figma: securing internal web apps).
  - ○ Architect for the detection & response strategy in place at Figma, built on modern devops and serverless principles.
  - ○ Built Figma's *Endpoint Security Baseline*, an automated system of validations and auto-remediations that ensured that employee machines met security standards.
  - ○ Deployed Chromebooks to Figma employees as a high-security computing platform, after building custom software to integrate this platform into Figma's trusted device authentication system.
- ◇ **Staff Security Engineer, Airbnb** (2016–2020): Built the Security Engineering team and acted as technical lead for three security teams (Security Engineering, Data Security, and Production Security). Notable projects included:
  - ○ Designed, built, and championed *SecureStack*, a system to build mutually authenticated TLS tunnels in Airbnb's infrastructure by integrating with service discovery. This project introduced high-quality network segmentation to the Airbnb environment of 2,500 microservices.
  - ○ Core designer and leader of the *Permissions Working Group*, a cross-functional team redesigning authorization systems in a high-scale, highly distributed infrastructure. This eventually resulted in the Himeji project.
  - ○ Served for two years as a *Sysop*. Airbnb Sysops were highly experienced engineers that were on-call for any incident in the Airbnb platform, from DB instability to JavaScript issues.
- ◇ **Senior Security Engineer, NCC Group** (2014–2016) Performed penetration tests on products built by a wide variety of Silicon Valley companies. Testing performed covered most disciplines of information security, but had particular focus in:
  - ○ Authentication flaws in web applications, particularly ones using federated login such as Oauth2.0 or SAML.
  - ○ Network security & red teaming in organizations with a modern, web-focused stack.

- **Lead Information Security Engineer, UC Berkeley Student Affairs IT** (2012–2013)
  - Handled security operations and policy for approximately 10,000 people and 14,000 machines.
  - Led a team of five to complete a variety of security projects, including web app audits, firewall review, and IDS monitoring.
  - Was primary system administrator for team-owned workstations & servers (Linux & FreeBSD).
- **Information Security Consultant, UC Berkeley Student Affairs IT** (2011–2012): Mitigated malware outbreaks in the 12,000 machine residential network at UC Berkeley. Reverse-engineered samples recovered to build better mitigation strategies.
- **Webmaster & Graphic Design Consultant, Praxis Works** (2010–2014): Designed and built the Praxis website, as well as the graphics etched on to Praxis rings.

InfoSec Community Contributions
- Presented Sneaking In Network Security, about the SecureStack project, to the 35$^{\text{th}}$ Chaos Communication Congress (35C3).
- Presented Hunting the Modern Attacker, about AppSec incident response, to OWASP AppSec Day 2019.
- Guest lecturer for 6.858, the MIT undergraduate class on computer systems security (2019, 2020, 2022, 2023).
- Presented *Figma Stops Attackers with JOIN: Combining Data for Powerful Security Analytics*, about Figma's use of modern data tools for security purposes, to Snowflake Summit 2022.
- Spoke about zero-trust and access control philosophy on the Cloud Security Podcast and Access Control podcasts.
- Organized BERKE1337, Cal's Cybersecurity Competition Team. Led team to 1$^{\text{st}}$ place in Cal's second appearance at the Western Regional Collegiate Cyber Defense Competition, and 5$^{\text{th}}$ place in the team's first Nationals appearance. Served a role as primary expert in binary analysis & Windows defense.

Certifications
- PADI Advanced Open Water Diver. Also drysuit certified.
- General-class amateur radio operator. Callsign: KK6PEK.
- Wilderness First Aid certified by the National Outdoor Leadership School (NOLS).
- AIARE 1 certified (avalanche safety and risk management).