

Phillip White

me@phillipdwhite.com phillipdwhite.com
linkedin.com/in/phillipdwhite github.com/phillipwhite99

Summary

Security engineer with 7+ years across IT and security, from 50-person startups to 5,000+ user enterprises, specializing in detection engineering, cloud and identity security, and security automation. Grew from helpdesk and SaaS administration into security engineering, bringing hands-on knowledge of the identity, SaaS and cloud systems attackers target. Most recently, built AI agent pipelines that turn threat intel into automated hunts and triage vulnerability findings.

Skills

- Detection and Response: Panther (detections as code), Anvilogic (Splunk), Python and SQL detections, MITRE ATT&CK mapping, detection unit testing, alert tuning, threat hunting, incident response, threat modeling, tabletop exercises, on-call, incident.io
- Cloud and Infrastructure Security: AWS, GCP, Azure, Snowflake, Terraform/Atlantis, Cloudflare (DNS, WAF, rate limiting), Wiz, Lacework, Reco, Detectify, Intruder, CSPM, SSPM, Docker, Kubernetes
- Identity and Access: Okta, ConductorOne (just-in-time access), RBAC and least privilege, PAM, access reviews, Twingate (ZTNA), 1Password, Okta and GitHub hardening
- Data and Endpoint Protection: Netskope (CASB, SWG, DLP), Armorblox, Obsidian and Abnormal Security (email security), CrowdStrike EDR, Kandji (Iru), Jamf, ManageEngine, PDQ Deploy
- Security Data Engineering: Snowflake security data lake, S3, Fivetran, dbt, Sigma
- Governance and Compliance: SOC 2, ISO 27001, quarterly access reviews, audit evidence, AI usage policy and data controls, legal data discovery
- Automation and Scripting: Python, SQL, Bash, PowerShell, n8n, Okta Workflows, Zapier, GAM, REST APIs, MCP, OpenAI, Anthropic, AI coding and agent tools
- IT and SaaS Administration: Google Workspace, Microsoft 365, Atlassian (Jira, JSM, Confluence), GitHub, PagerDuty, Asana, BitGlass, Brivo, Eagle Eye, Outreach, Gong

Work Experience

Sigma Computing, San Francisco, CA

Security Engineer

Sep 2024 – Jul 2026

IT Engineer

Jan 2022 – Sep 2024

Detection and Response

- Built and maintained Panther SIEM using detections as code, writing 40+ custom Python and SQL detections, each mapped to MITRE ATT&CK, validated with unit tests against sample log data and tuned to cut false positives.
- Built an agentic threat intel pipeline in n8n that ingests RSS intel feeds, assesses each report's relevance to our environment, extracts IOCs and IOAs, and runs automated threat hunts through the Panther MCP server, posting results to Slack and paging on-call when findings warranted investigation.
- Onboarded 20+ critical and high-priority log sources, including AWS, GCP, Azure, Okta, 1Password and CrowdStrike.

- Designed a cost-conscious security data lake that filters logs before SIEM ingest, keeping multiple terabytes per month out of the SIEM while retaining raw logs in a team-owned Snowflake database for hunting and investigations.
- Led threat hunts and investigations, including scoping data exposure from a compromised third-party SaaS integration (partnering with compliance on customer notification), detecting unauthorized transfers of company data to personal infrastructure, and investigating offboarded employees for data exfiltration.
- Responded to a widespread npm supply chain attack as part of a company-wide incident response, supporting containment and remediation.
- Responded to multiple leaked-credential incidents, coordinating secret rotation and cleanup with engineering teams.
- Reverse engineered suspicious Chrome extensions based on CrowdStrike and other threat intelligence, and identified risky AI tool usage through browser extensions.
- Led threat modeling of critical systems, designed incident response processes and ran tabletop exercises covering account takeover, ransomware and insider threats, plus internal phishing awareness campaigns.
- Served as primary and secondary on a monthly security on-call rotation.

Cloud and Identity Security

- Led IAM across GCP, Azure, AWS and Snowflake, implementing RBAC and least privilege access.
- Cleaned up Snowflake admin access by creating auditable just-in-time roles with manager and stakeholder approval flows for non-standard privileged access; used ConductorOne to extend just-in-time access to other critical resources.
- Built a RAG agent that inventories cloud IAM resources and maps them to ConductorOne entitlements, letting engineers ask which roles or permissions they need for a given task.
- Managed infrastructure as code with Terraform/Atlantis, including Cloudflare DNS, WAF and rate limiting rules, and Azure, AWS and GCP IAM, firewall rules and other infrastructure.
- Hardened Okta and GitHub, and reviewed the policies and posture of critical apps to close data exfiltration and attack paths.
- Deployed Twingate ZTNA to secure access to clusters and Snowflake instances.
- Owned vulnerability and cloud security posture management in Wiz (and previously Lacework), using it to track and prioritize infrastructure, container and misconfiguration findings across AWS, GCP and Azure.
- Worked cross-functionally with engineering teams to drive remediation of prioritized findings, and resolved IAM and access findings directly or with my team.
- Built agent workflows to triage critical and high vulnerability findings, prioritizing by the infrastructure and libraries/packages involved.

Data Protection, Governance and Compliance

- Ran DLP and insider-risk monitoring with Netskope, and administered CrowdStrike and Kandji (Iru) endpoint security.
- Expanded SaaS data security coverage with Reco and Wiz to find sensitive data exposure and enforce access controls across cloud and SaaS apps.
- Led email security rollouts of Armorblox and Obsidian.
- Worked with compliance to develop LLM tool guidelines, approved settings, data controls and AI usage policy.

- Supported SOC 2 and ISO 27001 audits with evidence collection, quarterly access reviews and meetings with compliance vendors and certifiers; performed data collection and discovery for legal and executive leadership.
- Secured credentials and secrets in 1Password, establishing secure sharing and rotation policies.

IT Engineering and Automation

- Built a Python integration to automate Okta user lifecycle management from our HRIS (ADP Workforce Now) where no native connector existed.
- Architected data pipelines to populate our data lake with actionable information for analysis in the Sigma platform.
- Coordinated the entire IT build-out for new offices, including ISPs, networking contractors and vendors, conference rooms and all-hands spaces, and physical security planning.

IT Specialist, Wisk, Mountain View, CA

May 2021 – Jan 2022

- Okta admin, Google Workspace admin, CASB admin, EDR admin (malware troubleshooting and remediation), general SaaS admin as well as Jamf admin.
- Primary point of contact for user support.
- Okta SSO and SCIM integrations with SaaS apps (Lucidchart, Google Workspace, BitGlass, Microsoft, etc) as well as group and rule automation (Okta to on prem AD to O365/SharePoint)
- Wrote Python scripts to integrate with our VM vendor's API to create new VMs, reboot them as well as serve messages to users ("Your VM will reboot in 2 hours" etc)
- Contributed to legacy knowledge by creating KB articles for unique and common fixes.
- Administered all of our front end facing/SaaS apps.
- Used GAM for solutions not easily solvable via the Google Workspace GUI.
- Tried and deployed forensic software to gather legal hold images for pending litigations.

IT Support Engineer, April Health, San Carlos, CA

Oct 2020 – May 2021

- Sole helpdesk support for an org of 60+ team members.
- Initiated and successfully deployed the Local Admin Password Solution (LAPS) to fortify endpoint security across the organization.
- Achieved 100 percent approval from users who responded to ticket surveys.
- Scripted PowerShell Windows task to maintain WSUS compliance and email report to helpdesk, as well as LAPS compliance script.
- Authored 40+ public and internal KB articles documenting IT processes.
- Planned and set group policies, as well as managed users, devices and groups in AD.
- Managed O365 as well as Exchange and SharePoint Online.
- Maintained and upgraded vCenter, UCS and Nimble systems as well as monitored Veeam backups.
- Managed tablets and mobile devices with Hexnode MDM and managed Duo multifactor authentication for users.

ITCS Technician/Infrastructure Analyst, Adobe, San Jose, CA

Jun 2019 – Oct 2020

- Break/fix, asset management, troubleshooting/diagnostics
- Wrote script to remove all Adobe products from devices
- Discovered a solution for a severe antimalware/Catalina interaction that was causing systems to get stuck in a boot loop.
- Heavily contributed to a team that hit all SLA/CSAT goals by being the top ticket producer in HQ for a majority of months shortly after being hired
- Coordinated repairs with IBM/Apple/Lenovo as well as performed some in-house repairs.
- Managed devices centrally via AirWatch MDM.

Desktop Support Technician (Contract), Sutter Health, Bay Area, CA

Dec 2018 – Jun 2019

- Deployed Windows 10 devices with SCCM across multiple Sutter Health hospital sites in the Bay Area as part of an organization-wide OS refresh and upgrade.