

# Caleb S. Cupples

## PERSONAL DETAILS

---

Phone - US	+1 415 636-8698
Phone - AR	+54 9 11 5102-1154
EMail	caleb@cuppl.es

## CERTIFICATIONS/TECHNOLOGIES

---

Certifications	ITIL v3 Foundations, Microsoft Certified Professional
Tools	SentinelOne, Tenable Nessus, PowerShell, bash, SCCM, VMware vSphere, JIRA, RSA Archer, ELK Stack, ServiceNow, Aha.io, Vanta
Languages	English - Native, Español - C1, Português - B2
Keywords	Cybersecurity, Cyber Resilience, Incident Management, SOC2, ISO27001, NIST 800-53, Disaster Recovery, Policy, Cybersecurity Engineering, GRC, PCI-DSS, HITRUST

## WORK EXPERIENCE

---

### Senior Compliance Manager

05/24 - Present

#### *Observa, LLC*

- Provided comprehensive compliance management for a variety of startups across the fintech, health tech and technology verticals.
- Built and administered successful vendor risk evaluation and management strategies for multiple clients.
- Developed baseline template policies for compliance with HIPAA, SOC 2 and ISO requirements for clients in regulated spaces.
- Managed SOC 2, ISO 27001, HITRUST and PCI-DSS compliance audits for multiple clients.
- Administered Vanta, Secureframe and Drata for various clients to track compliance metrics and gather evidence for presentation to auditors.
- Ran tabletop exercises to ensure compliance with regulatory requirements and ensure best security practices.

### Senior Associate

06/24 - 12/24

#### *PwC Acceleration Center Buenos Aires*

- Led cybersecurity compliance projects from initiation through to final acceptance by the business.
- Built tooling to automate data importation from Aha into internal compliance tracking utilities.
- Acted as Scrum Master for compliance efforts regarding the development of the Next-Gen Cloud Evolution platform.
- Tracked business risks and helped develop mitigations for ongoing risks to cybersecurity goals.
- Administered ServiceNow, Archer and Aha! for tracking of compliance risks and mitigations.
- Worked with stakeholders in various jurisdictions, including Brazil, the EU, USA and South Africa for developing risk acceptance frameworks in accordance with regulatory requirements.

### Security Engineer - Corporate Security and Compliance

08/22 - 10/23

#### *Latacora*

- Led a squad of 4, assigning work and maintaining oversight over ticket queues.
- Assessed client risk registers for completeness and comprehensiveness.
- Mentored junior engineers and held weekly 1-1 meetings to review work and guide career advancement.
- Developed risk assessment methodologies for international hiring in over 50 countries
- Performed comprehensive audits of client Google Workspace and Github environments for best practices.
- Authored and evaluated security policies for over 40 clients, including disaster recovery, incident management and cyber resilience, supporting multiple certification efforts including SOC2 and ISO.
- Presented social engineering and security awareness training programs to a variety of startup clients, in multiple industries.
- Authored a library of security policy templates and tutorials for clients to jumpstart their security practice.
- Conducted audits against CIS controls for multiple clients and provided actionable recommendations to fortify their security posture.

**Professional Cybersecurity Analyst**

08/21 - 08/22

*Fortra (formerly Alert Logic)*

- Analyzed internal and external network traffic for threats to the security posture of 100+ clients.
- Administered dozens of WAF appliances as a service for a broad spectrum of customers across various industries.
- Managed client escalations, including presentation of in-depth incident analysis.
- Performed and presented analysis of customer environments and provided IDS (Intrusion Detection System) tuning recommendations for over 50 clients.
- Conducted training sessions for 10+ new analysts, acclimating them to the Security Operations Center.
- Created multiple training sessions on new and emerging threats within the customer landscape.
- Managed dozens of investigations of customer security incidents.

**Cybersecurity Analyst 2**

11/20 - 08/21

*Garmin International*

- Analyzed internal and external network traffic on over 20000 endpoints for threats.
- Leveraged EDR capabilities to actively review system logs and storylines for use in ongoing investigations.
- Led engagements with international stakeholders to ensure continued security compliance.
- Created SOC documentation within Confluence for written procedures and knowledge resources.
- Conducted ongoing training with non-US based analysts to ensure knowledge parity between US-based and international resources.

**Federal Information Systems Cybersecurity Engineer**

10/18 - 11/20

*Cerner Government Services*

- Evaluated the federal enclave for adherence to compliance frameworks, including NIST 800-series and HIPAA.
- Created and reviewed documentation for over 40 ATC (Authority to Connect) package submissions, and acted as the point of contact for government personnel throughout the ATC process.
- Led multiple audits, including client-observed incident management and disaster recovery drills, with government clients and Leidos Partnership for Defense Health stakeholders to ensure the successful continuation of the system ATO-C (Authority to Operate with Conditions).
- Analyzed Tenable Nessus scans to provide timely feedback to operations staff and project stakeholders on the security posture.
- Assessed system security artifacts for technical accuracy and compliance with DoD and VA regulations.

**Systems Administrator**

07/17 - 10/18

*Conduent, Inc., Advantage Resourcing and Randstad Sourceright*

- Managed over 700 virtual servers across multiple domains while embedded within a county IT department in the SF Bay Area.
- Created disaster recovery and crisis management procedures for the loss of both primary and secondary fiber connections.
- Created and developed metrics for process improvement during client's migration to a ServiceNow platform.
- Authored extensive Citrix maintenance and recovery documentation.
- Led Citrix SME training for the system administration team.
- Coordinated testing efforts with client developers to maintain continuity of operations after system upgrades.

**Senior Consultant, Cybersecurity Policy and Compliance Analyst**

6/14 - 6/17

*Booz Allen Hamilton*

- Spearheaded projects to maintain authority to operate on defense networks, including the highest score achieved by any Navy secure enclave to date.
- Audited client environments for compliance with DoD STIG, SECNAV and NIST 800-series requirements.
- Developed system documentation, including disaster recovery, cyber resilience, incident management and crisis management policies, in preparation for security audits, ensuring continued authorization to operate on defense networks.
- Created automated processes for software deployment and auditing within client environments.
- Developed automated software installation reporting scripts for compliance audits.
- Authored documentation on recovery from natural disasters for internal incident management playbooks.

## EDUCATION

---

**B.S. Psychology**

5/13

*The University of North Alabama*