



# SECURE YOUR CLOUD ADOPTION WITH SECURITY COMMAND CENTER ENTERPRISE (SCCE)

Enable and operationalize Google Cloud's native CNAPP<sup>1</sup> across your multi-cloud environment

Deloitte helps enable multi-cloud enterprises to rapidly adopt and operationalize SCCE with on-going managed services. Leverage Deloitte Cyber experience to jumpstart SCCE's CNAPP technologies, integrate with Mandiant Attack Surface Management (ASM), and operationalize the Google SecOps suite.

1 Cloud Native Application Protection Platform.



## Reality of the cyber world today



Cyber attacks are increasing in sophistication and persistence, targeting organizations across various industries



Multi-cloud environments are at risk of misconfigurations that permit misuse



Cloud misconfigurations put sensitive data and enterprise systems at risk of exposure



Cyber professionals are scarce and in high demand

**<4**

Average number of attack path steps to reach a 'crown jewel' within a public cloud environment<sup>2</sup>

**45%**

US professionals concerned over growing number of hackers/cybercriminals<sup>3</sup>

**\$1.8  
BILLION**

In fines and legal penalties levied against 11 financial institutions for non-compliance with regulations in Sept 2022<sup>4</sup>

2 Orca, 2022 State of Public Cloud Security report, 2022.

3 CompTIA, State of Cybersecurity, 2024.

4 Deloitte, "US Regulatory Deloitte Capital Markets Regulatory Outlook," January 2023.

5 Information Technology Service Management

## We deliver outcomes that help your business



Cost-effective enablement and operationalization of CNAPP across a multi-cloud environment



Assessment of cloud environments by Deloitte Cyber Security Professionals



Alignment of SCCE detection and prevention policies to an organization's security and compliance requirements



Integration with existing enterprise ITSM<sup>5</sup> solutions and security operations playbooks



24x7x365 monitor of multi-cloud environments

## Google's approach

↑  
OPERATIONAL CONVERGENCE  
↓



### Cloud security

Proactively manage cloud exposures, posture, data, and identity



### Security operations

Identify ownership and streamline responses to high-risk cloud events



## Deloitte's capabilities



### Attack Surface and Management (ASM)

Bolster private cloud security, providing near real-time visibility into vulnerabilities, asset tracking, and rogue system detection.



### Security Health Analytics (SHA)

Automated security checks that identify misconfigurations and compliance violations across multi-cloud resources.



### Integrated Security Operations

Development and configuration of Google SecOps playbook to enable automated SOC responses for SCCE findings.



### Cyber Threat Intelligence

Leverage predictive cyber threat intelligence informed by adversary tactics, techniques and procedures, as well as tailored analysis and malware analysis.

## Deloitte's offerings



### Jumpstart in less than a month

Configure and enable SCCE foundational capabilities, including ASM and SHA. Prioritized remediation and action of SCCE findings, threats, and vulnerabilities from Deloitte cloud security analysts.



### Implementation in less than three months<sup>6</sup>

Fully adopt and implement SCCE for your enterprise. Leverage Deloitte's cloud security experience and solutions to help address security and compliance requirements. Respond to and remediate threats using custom detection rules and a tailored Google SecOps playbook.



### Managed Service on a recurring basis

Provide ongoing management and operationalization of SCCE for your enterprise, offering 24/7/365 threat and vulnerability monitoring, coupled with Deloitte's advisory support, governance, and guidance for vulnerability management.

**FLEXIBLE DELIVERY APPROACHES FOR WHEN YOU NEED HELP WITH  
STRATEGY, EXECUTION, OR OPERATION**

<sup>6</sup> Timeline based on business days and depends on the complexity of the organization's environment (in less than three months)

Google Cloud SCCE **DELIVERS a**



**MODERN CNAPP** ✓



**DELOITTE**



**DELIVERS resilient security outcomes**

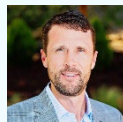
## START THE CONVERSATION



**Mark Nicholson**  
Principal  
Deloitte & Touche LLP  
[manicholson@deloitte.com](mailto:manicholson@deloitte.com)



**Chris Trollo**  
Senior Manager  
Deloitte Services LP  
[ctrollo@deloitte.com](mailto:ctrollo@deloitte.com)



**Jason Tarlton**  
Deloitte Security  
Alliance Manager  
Google LLC  
[jtarlton@google.com](mailto:jtarlton@google.com)



**Ryan Lee**  
Deloitte Security  
Alliance Manager  
Google LLC  
[rryanlee@google.com](mailto:rryanlee@google.com)

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

All product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this document.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see <http://www.deloitte.com/us/about/for-a-detailed-description> of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2025 Deloitte Development LLC. All rights reserved.