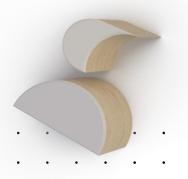
## **Cyber Services**

Moving to the cloud requires an integrated approach to security and privacy that covers the core platform, applications, enterprise, and operations. Coupled with Google Cloud's security solutions, Deloitte leverages decades of experience to provide end-to-end cloud security solutions to assist with large scale digital transformation journeys, Security Operation Center (SOC) modernization efforts, and implementation of Zero Trust security models to help organizations protect their data, users, and applications.





**Services** 

### Deloitte's Google Cloud Cyber Capabilities

### Google Cloud

### Secure Cloud Foundations & Transformations

- Secure cloud strategy and readiness
- Secure cloud migration and transformation
- Secure cloud development
- Secure cloud operate

### Chronicle

## SOC Modernization & Security Analytics

- SOC strategy and roadmap
- SOC design and implementation
- SOC automation
- ♣ SOC operate

### BeyondCorp Enterprise

### Secure Access & Zero Trust

- Zero Trust strategy and roadmap
- BCE jumpstart and MVP deployment
- BCE design and implement
- BCE operate

### Deloitte Solutions & Offerings



- Cloud Security Policy Orchestration (CSPO)
- Cyber Cloud Managed Services (CCMS)
- Cyber predictive analytics
- Attack surface management

Predictive Analytics for Cyber in Enterprises (PACE™)



Managed Extended
Detection and
Response (MXDR)
by Deloitte



Deloitte's Zero Trust Access

. . . . . .

### Market trends

Attack surface expansion

Security tools consolidation

Digital supply chain risk

Engineering trust with cloud-native controls

# Common business challenges

## Cyber as a catalyst to empower your organization

### **C-SUITE**



Regulatory adherence and compliance



Business agility, customer experience, and trust



Software Development Life Cycle (SDLC), DevSecOps, tools, and governance



Secure digital transformation, secure solutions, and better user experience

### VPS/DIRECTORS/MANAGER



Transformation and operating advancement



Technology shift, modernization, and cost



(3)

Adoption of new technologies and next-gen cyber products



Next-gen cyber transformation of people, process, technology, and automation

### **ANALYST/ENGINEER**



Shortage of skilled resources



Lack of industry and business case knowledge and exposure



(5)

Upskilling and technology adoption, Infrastructure as Code (IaC), Policy as Code and automation for cybersecurity



Cyber standard operating procedures, playbooks, templates

Use of artificial intelligence, machine learning, user and entity behavior analytics, and advanced toolsets

### Why Deloitte & Google Cloud



Four-time Global Services Partner of the Year (2017, 2018, 2019, 2020)

Industry Partner of the Year (2021)

Inaugural Public Sector Partner of the Year (2020)



1,700+

**GOOGLE CLOUD CERTIFIED PROFESSIONALS** including architects, security engineers, and developers



PREMIER PARTNER STATUS
SECURITY SPECIALIZATION
GOOGLE CLOUD

### **Spotlight:** Deloitte engagements



#### CLIENT:

MAJOR BANK

### Background:

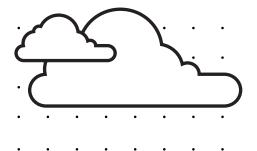
Deloitte is assisting a major bank in building a secure and resilient Google Cloud environment for migrations over a multi-year period.

### **Solution:**

Secure Cloud Foundations and compliance automation developed to accelerate application migration and deployment into Google Cloud.

### Impact/Outcome:

Secure and resilient network structure that enables minimal latency and maximum security. Securely migrating over 700 applications to Google Cloud enabling the bank to exit the data center.





#### CLIENT:

MAJOR HEALTHCARE ORGANIZATION

### Background:

Client was looking to migrate their existing security threat management platform to something more scalable and cloud native capable of monitoring their on-prem and multi-cloud environments. Their requirements also included centralized security log management, advanced security analytics and a flat fee structure to avoid increased storage or processing costs as their environment grew.

#### Solution:

Deloitte implemented PACE and developed custom sets of analytics and persona-based visualizations for the SOC team to enable threat detection and hunt at scale, and bespoke analytics for the insider threat team.

### Outcome:

Improved detection capabilities using predictive analytics to proactively detect threats. Cost reduction and efficiency improvements realized with Chronicle's ingestion capabilities and extensible rulesets.



#### CLIENT:

**GLOBAL INVESTMENT BANK** 

### **Background:**

Client was looking to mature their cloud security as they build foundational capabilities for development of new products and market offerings in the cloud at scale.

#### Solution

Deloitte developed and automated security guidelines for use of Google Cloud services.

Assisted with cloud security design reviews and developed threat models in conjunction with client tech risk personnel.

Developed Open Policy Agent (OPA) policies to help enforce Policy-as-Code (PaC) for Google Cloud's Kubernetes Config Connector (KCC) based IaC deployments across the clients Google Cloud environment and implement into development process with Continuous Integration, Continuous Delivery (CI/CD) pipelines.

### Outcome:

Ability to shift left in cloud development with automated preventative guardrails confirming Google Cloud resource configuration even before deployment.

### Start the conversation



### Arun Perinkolam Principal Deloitte & Touche LLP aperinkolam@deloitte.com



**Soumendra Rath**Managing Director
Deloitte & Touche LLP
sorath@deloitte.com



Chris Trollo
Senior Manager
Deloitte Services LP
ctrollo@deloitte.com



Ryan Lee Alliance Manager Deloitte Services LP ryanlee8@deloitte.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 & Touche LLP 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.