Google Cloud

Google Cloud Security

Uwe Jockel
it-sa Oktober 2022

Chronicle SIEM & SOAR - Security Operations

01

Trust

Nothing

02

Detect

Everything

03

Know What

Google Knows

The perfect cybersecurity storm

Increasing Threat Actor Activity

Nation state actors pivoting to eCrime and targeting mainstream enterprises

600+ threat actors emerged in last 12 months

Skills Shortage

500,000+ unfilled cybersecurity positions in the US alone

Rising Complexity

Expanding environments and attack surfaces (Cloud, IoT, containers)

Exponential data volumes to collect and analyze

Cybersecurity
Action Team

Chronicle
Google Cloud

Google keeps more people safe 🔒 online than anyone else

4 billion

Devices running Chrome are protected each day against malware and social engineering attacks

2.5 billion

Active Gmail users protected against phishing, malware, and spam

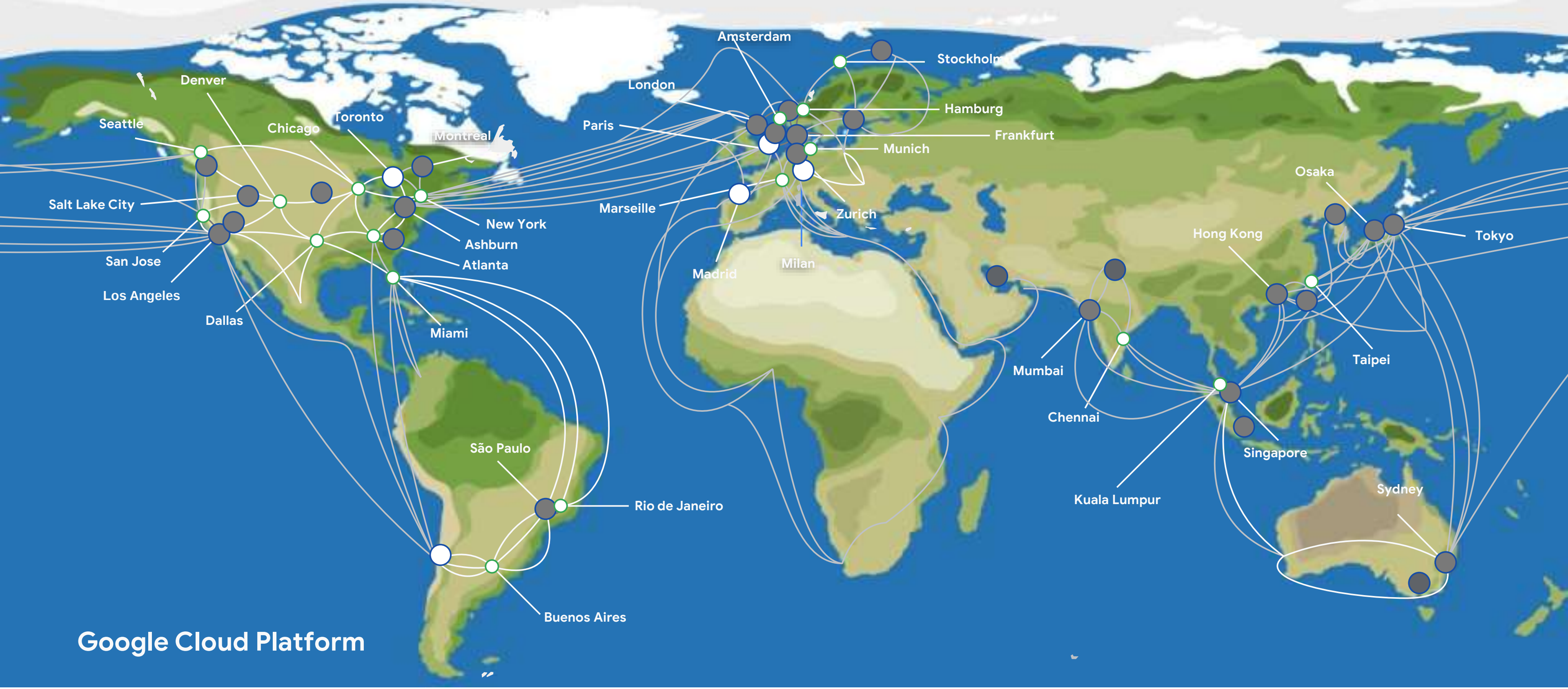
50 Billion

Cloud events analyzed by Security Command Center every day to detect runtime threats in the cloud

2.4 billion

Files and URLs analyzed by VirusTotal ,the world's premier cyber threat observatory

Google’s global infrastructure



Google Cloud Platform

34 regions, 103 zones, 147 network edge locations, 200+ countries

○ Dedicated Interconnect — Network ● Current region with 3 zones ○ Future region with 3 zones

Cybersecurity Action Team

Chronicle Google Cloud

What if enterprises were built on the same platform, and could use the same tools and practices that protect Google?

Cybersecurity Action Team

Chronicle
Google Cloud

Reimagine security operations

Bringing the Power of Google To Security Operations Chronicle SIEM Chronicle SOAR

Cybersecurity Action Team

Chronicle
Google Cloud

Security Operations is Ripe for Transformation

"We **can't store and analyze** all data, resulting in blindspots"

"It's **cost prohibitive** to ingest all the data we need"

"It takes **too long** to investigate alerts"

"We **struggle to build effective detection** and have too many false positives/negatives"

"Our processes are **too manual**, we are too slow to respond to and remediate threats"

"We don't have enough **skilled engineers** to make everything work"

Security Operations by Google

01
All your Data

Store, normalize and analyze everything - at cloud hyperscale

02
At a Disruptive Cost

Ingest and retain everything you need at a predictable cost

03
At your Fingertips

Faster time to “aha” with sub-second search and context-rich investigation

04
With Google Intelligence

Leverage Google’s Threat detection and intelligence to democratize SecOps

05
Automated Response

Automate and orchestrate processes to speed up response and free up valuable analyst resources

06
And Google Best Practices

Transform SecOps with expert guidance and best practices

Google security products supporting a safe cloud journey

Our extensive range of security products represents a rich heritage of Google security that your business can benefit from.

Chronicle SIEM

Delivers security analytics, collection, and analysis

VirusTotal

Analyzes suspicious files, domains, IPs, and URLs to detect malware

BeyondCorp Enterprise

Secures internet and application access from anywhere

Cloud Intrusion Detection System

Detects network-based threats with industry-leading security

Chrome Browser

The most used and secure browser for the modern-day challenge of the security landscape

Chronicle SOAR

Modern, fast, and effective response by combining playbook automation, case management

reCAPTCHA

Protects third-party websites and collects human-labeled data for machine learning

Security Command Center

Manages security vulnerabilities and threats from one platform

MANDIANT

Incident and exposure management and threat intelligence capabilities

Chrome OS

Linux-based operating system derived from open-source Chromium OS

NIST Cybersecurity Framework (NIST CSF)

Identify

Cloud Asset Inventory

Security Command Center

VirusTotal

Protect

chrome

BeyondCorp Enterprise

Google Workspace +

Security Command Center

reCAPTCHA

Cloud Armor

Detect

Chronicle

Security Command Center

Cloud IDS

Cloud DLP

Respond

MANDIANT

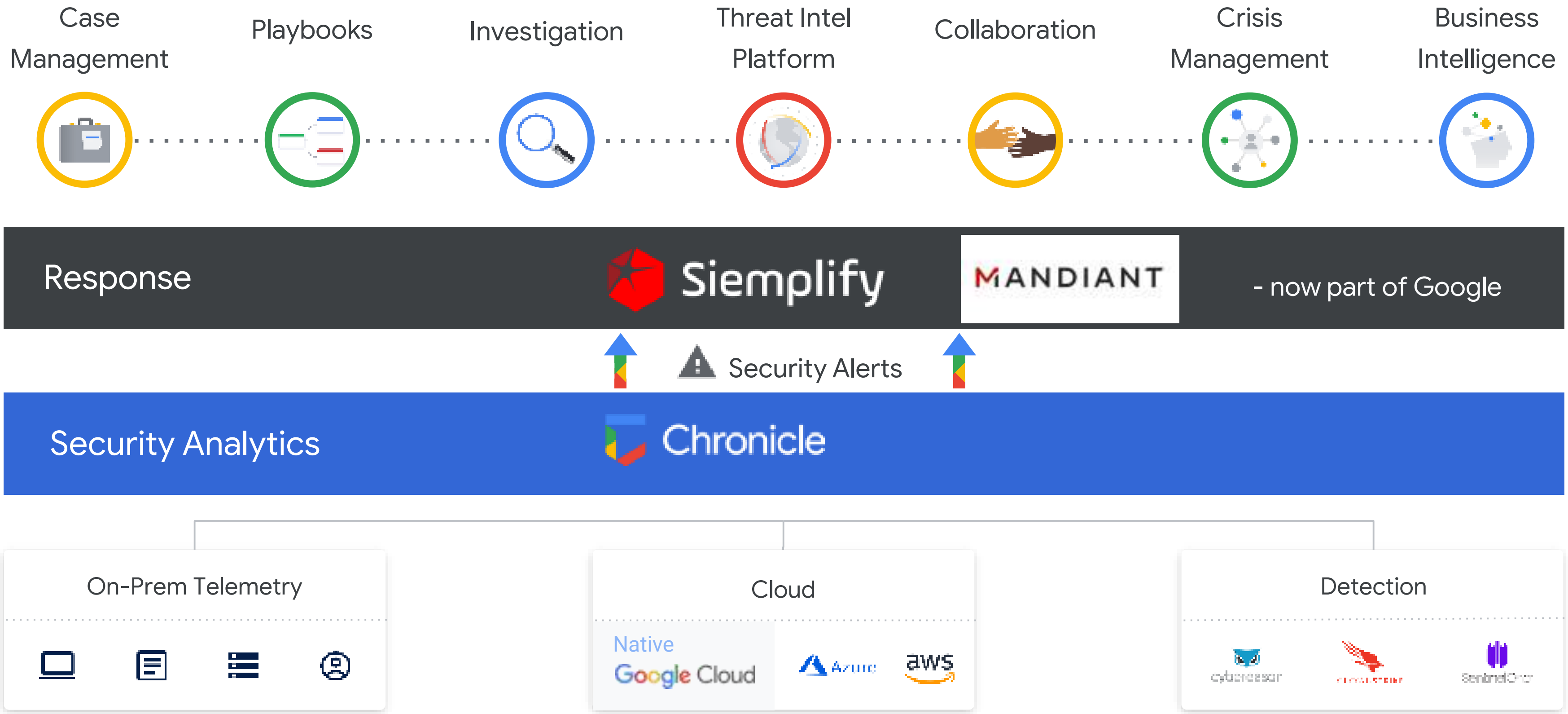
Siemplify

Recover

MANDIANT

Actifio Go

Detect Everything - Security Operations by Google



Case Management

Playbooks

Investigation

Threat Intel Platform

Collaboration

Crisis Management

Business Intelligence

Response — Siemplify — MANDIANT - now part of Google

Security Alerts

Security Analytics — Chronicle

On-Prem Telemetry

Cloud

Native Google Cloud

Azure

aws

Detection

cybereason

CROWDSTRIKE

SentinelOne

Cloud-native security analytics

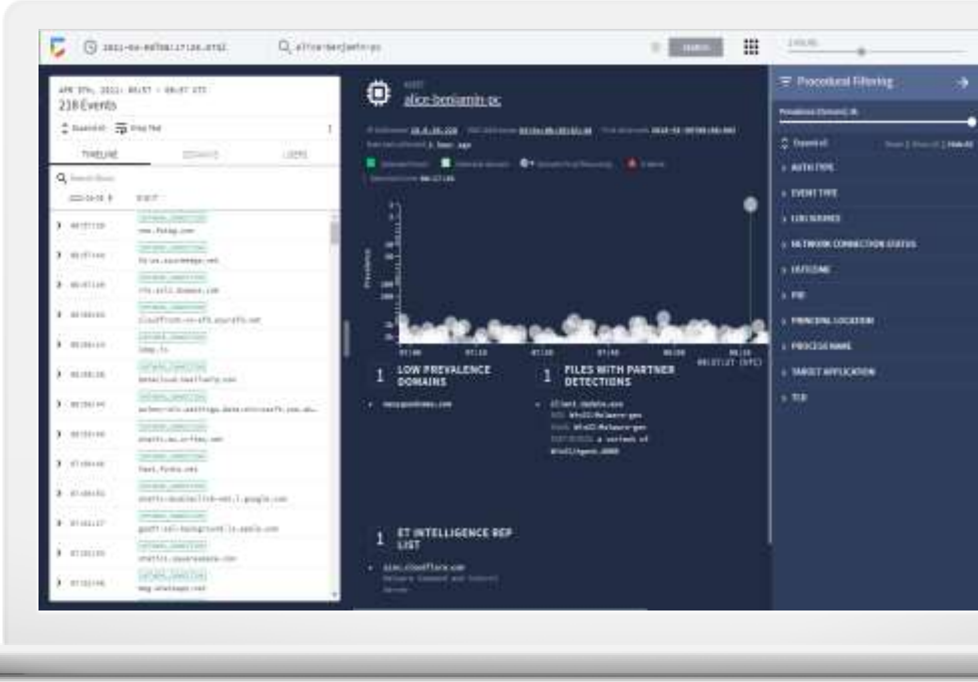
Ingest and analyze **data at cloud-scale** with 12 months hot retention

“Google Search” your data with **sub-second queries** and rich context

Use Google expertise codified as **curated detections** for advanced threats and build custom detections with **intuitive detection authoring** using YARA-L

Get faster insights with **context rich investigation views** that automatically stitch together relevant entities and pinpoint anomalies

Chronicle SIEM Deep Dive



Cybersecurity Action Team

Chronicle
Google Cloud

Automated response

Manage, prioritize and assign work with unique **threat-centric case management** purpose built for security operations

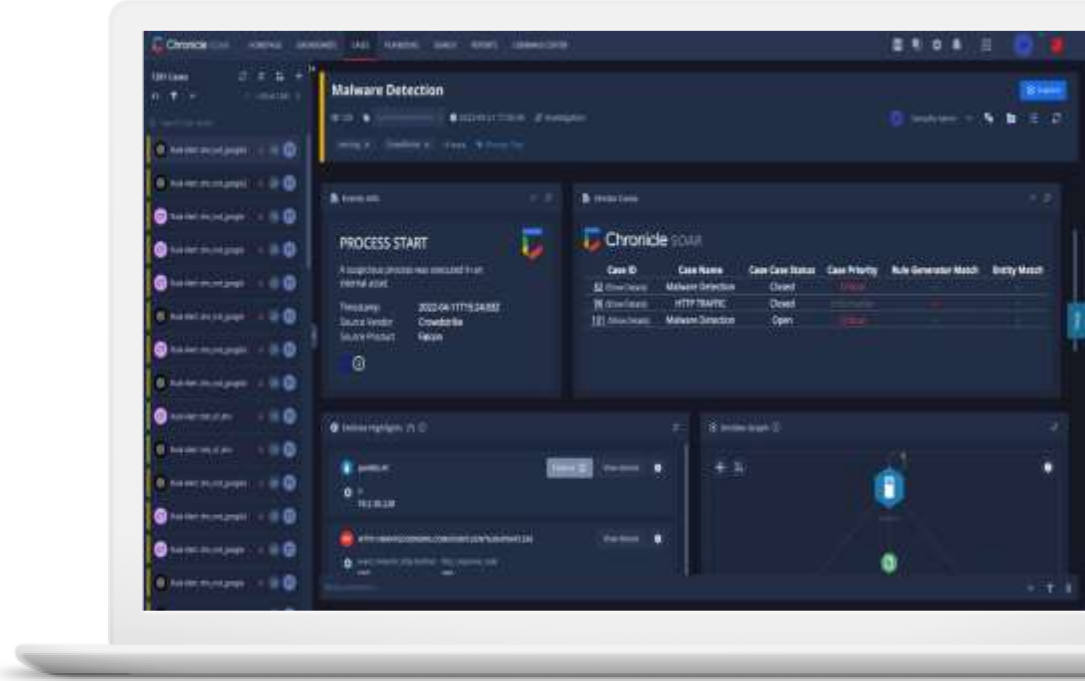
Drive consistency in your response and automate repetitive tasks with a **full- featured intuitive playbook builder** and 300+ integrations

Make good, fast decisions with a **context-rich investigation workbench**

Easily **collaborate on every case** with fellow analysts, service providers and other stakeholders

Track and measure key SOC metrics

Chronicle SOAR Deep Dive



Malware Detection

PROCESS START

Timestamp 2022-04-11T15:24:03Z
Source Vendor Crowdstrike
Source Product Falcon

Chronicle SOAR

Case ID	Case Name	Case Case Status	Case Priority	Rule Generator Match	Entity Match
[illegible]	Malware Detection	Closed	[illegible]		
[illegible]	HTTP TRAFFIC	Closed	[illegible]		
101	Malware Detection	Open	[illegible]		

Cybersecurity Action Team

Chronicle Google Cloud

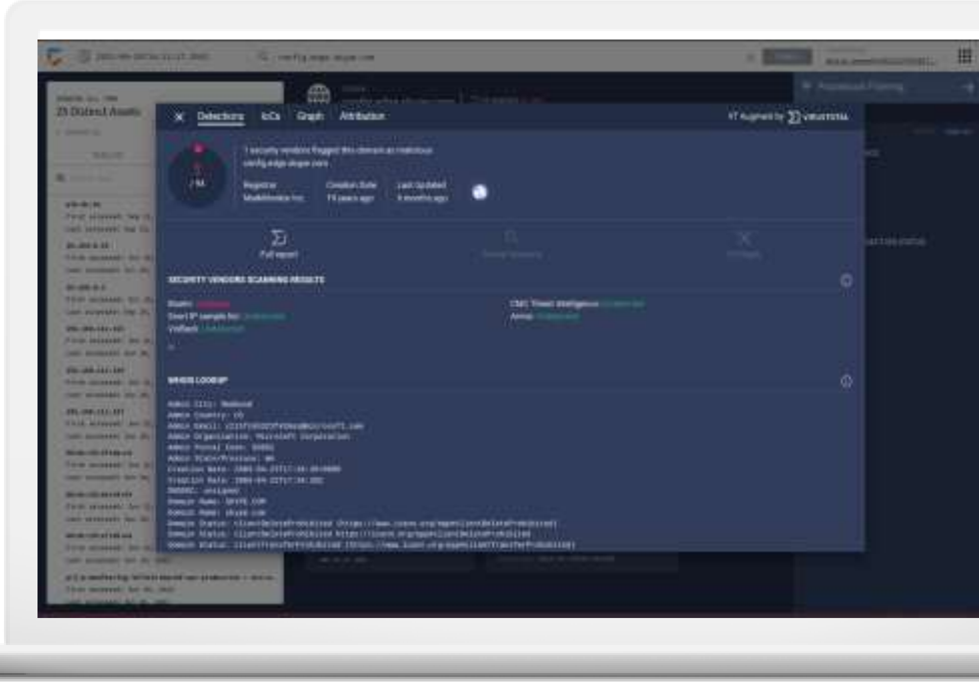
Powered by Google’s -Scale Threat Intelligence

Drive better detections with high-quality actionable, **native curated detections**, built, and maintained by Google Cloud Threat Intelligence researchers

Surface insights with native **VirusTotal Integration** with knowledge from the world’s richest, crowdsourced, near real-time malware corpus

Integrate your own threat intelligence feeds on our **API-driven open threat-intelligence platform**

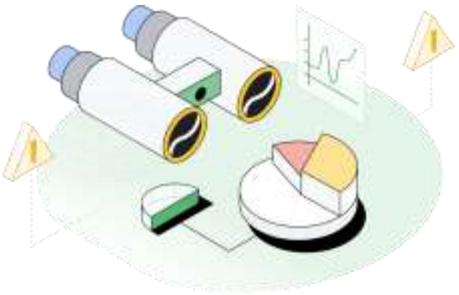
UPCOMING Leverage Mandiant’s world-class threat intelligence from the front-lines



Cybersecurity Action Team

Chronicle
Google Cloud

Multiple Ways to Start your Journey



Augmentation

Eliminate existing scalability challenges, data blindspots, or lack of orchestrated response by adding a modern cloud-native security operations suite to your existing stack

Cloud TDIR

Improve threat detection, investigation and response (TDIR) to threats in your Google Cloud environment with a cloud-native and cloud-aware suite

Transformation

Embark on a journey to Autonomic Security Operations. Modernize your SOC across people, process and technology with Google's products and expert help

Cybersecurity Action Team

Chronicle Google Cloud

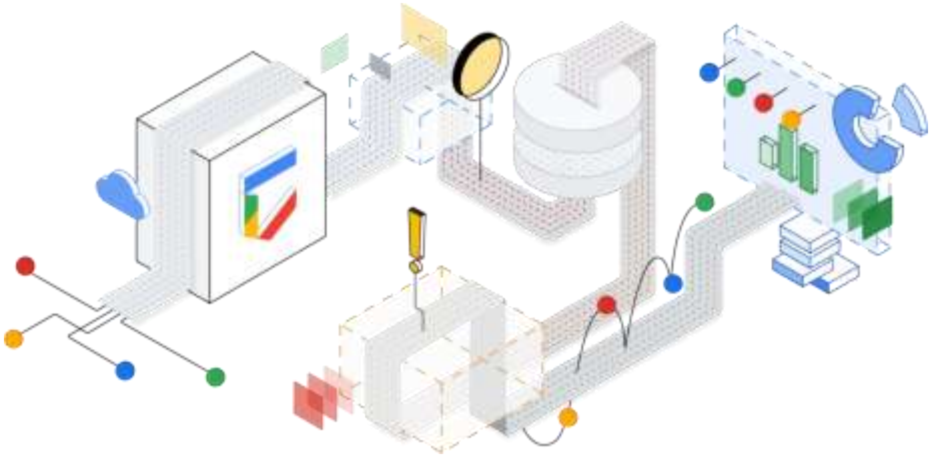
Recommended Resources

- GCAT website: gcat.google.com
- Threat Reports
  - Threat Horizons, Issue #1
  - Threat Horizons, Issue #2
  - Threat Horizons, Issue #3
- Key OCISO WP
  - CISO's Guide to Security Transformation
  - Risk Governance of Digital Transformation in the Cloud
  - Autonomic Security Operations: 10X Transformation of the Security Operations Center
- Cloud CISO Perspectives (CISO Blog)
  - May 2022
  - June 2022
- Cloud Security Podcast by Google

DANKE !

kontaktieren - besuchen Sie uns

uwejockel@google.com



Cybersecurity Action Team

Chronicle

Google Cloud