Google Cloud

New Hampshire
Government Finance
Officer's Association
NHGFOA.org

Trends in Cybersecurity and Proacative measures

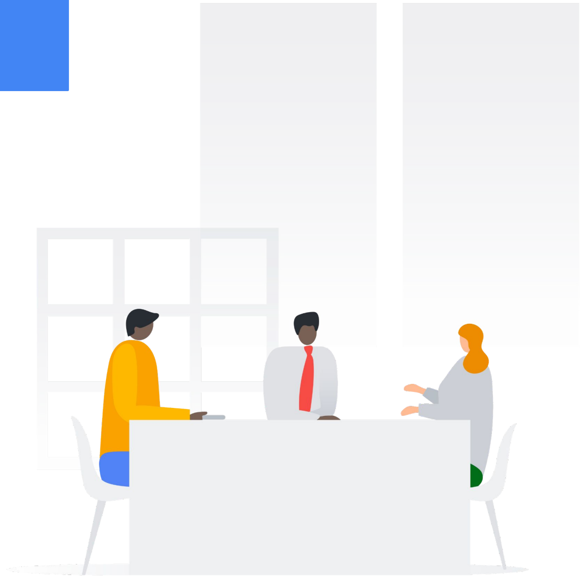
May 4th, 2023

Amar Parikh - amarpar@google.com
Nick Haas - nickhaas@google.com

Google Public Sector

Google for Government

Agenda



1. Insights from our latest report on cyber security and the threat landscape
2. Challenges in the security realm for Government organizations
3. How to holistically secure your org and tackle the threat landscape
4. Q&A and Next Steps

M-Trends 2023 Report

- Annual report – 14th edition
- Today’s most relevant cybersecurity metrics and deep insights
- Mandiant IR investigations/engagements and threat intelligence analysis from January 1, 2022 - December 31, 2022
- Hot topics in this edition:
    - ■ Dwell time and notification sources
    - ■ Infection vectors and malware developments
    - ■ The invasion of Ukraine
    - ■ North Korean financial operations
    - ■ New and unique attacker techniques

Download a copy: https://www.mandiant.com/resources/blog/m-trends-2023

MANDIANT
NOW PART OF Google Cloud

M-TRENDS 2023
MANDIANT SPECIAL REPORT

Key Investigation Statistics

16 Days	Global median dwell time
18%	Investigations that involved ransomware
48%	Threat groups motivated by financial gain
43%	Intrusions that involved obfuscated files/info
63%	External incident notification
9 Days	Global median dwell time for ransomware only
913	Newly tracked threat groups
73%	MITRE ATT&CK techniques used by attackers

When Are Attackers Found

Dwell Time

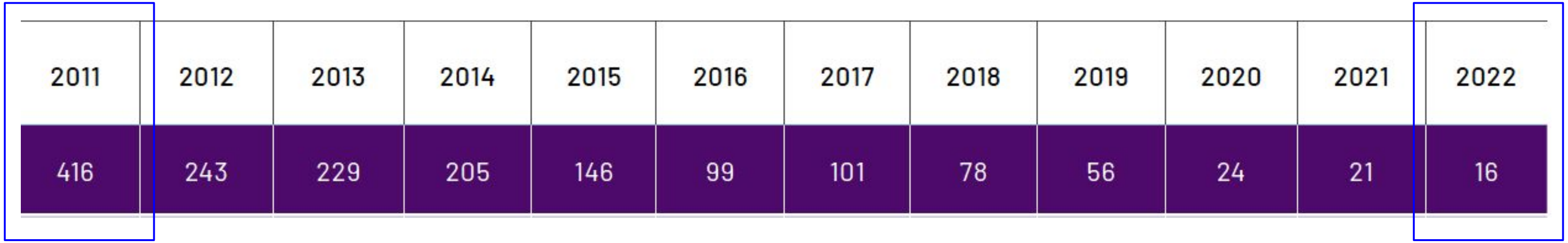
M-Trends 2023

Global Median Dwell Time

Change in Median Dwell Time

21 → **16**

Days in 2021 Days in 2022



2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
416	243	229	205	146	99	101	78	56	24	21	16

M-Trends 2023

Ransomware Dwell Times

Change in Global Investigations Involving Ransomware

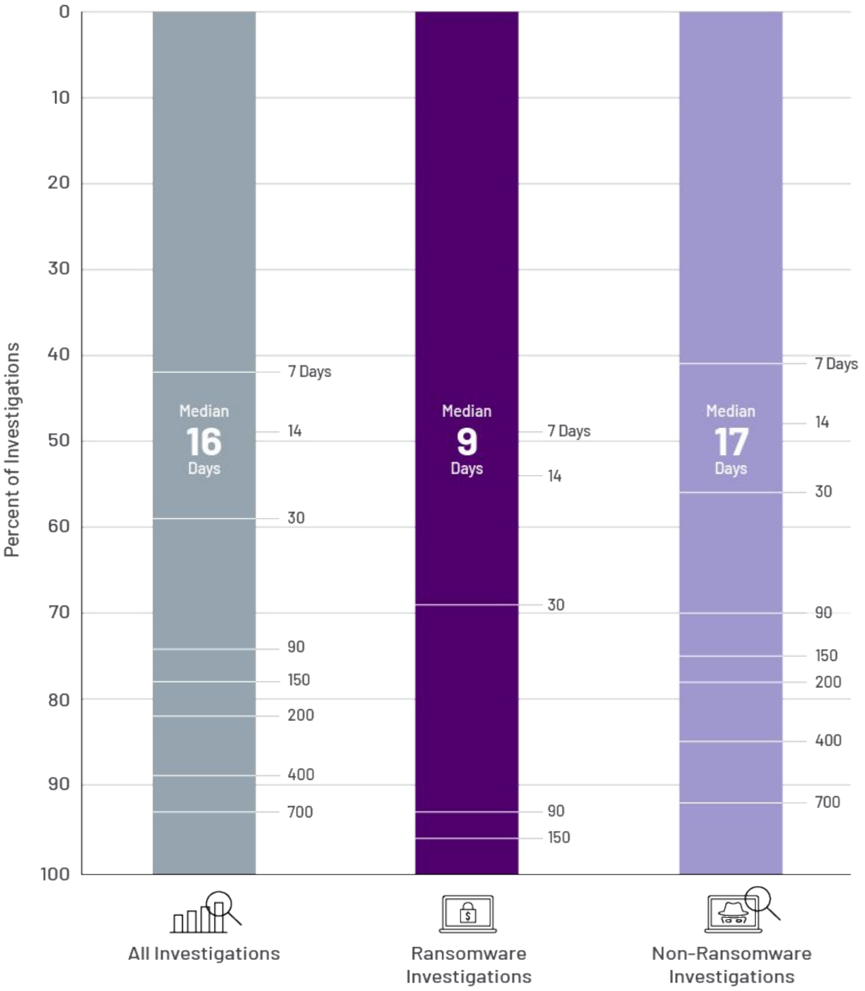
23% in 2021 → **18%** in 2022

Change in Global Median Dwell Time – Ransomware

5 Days in 2021 → **9** Days in 2022

Change in Global Median Dwell Time—Non-Ransomware

36 Days in 2021 → **17** Days in 2022

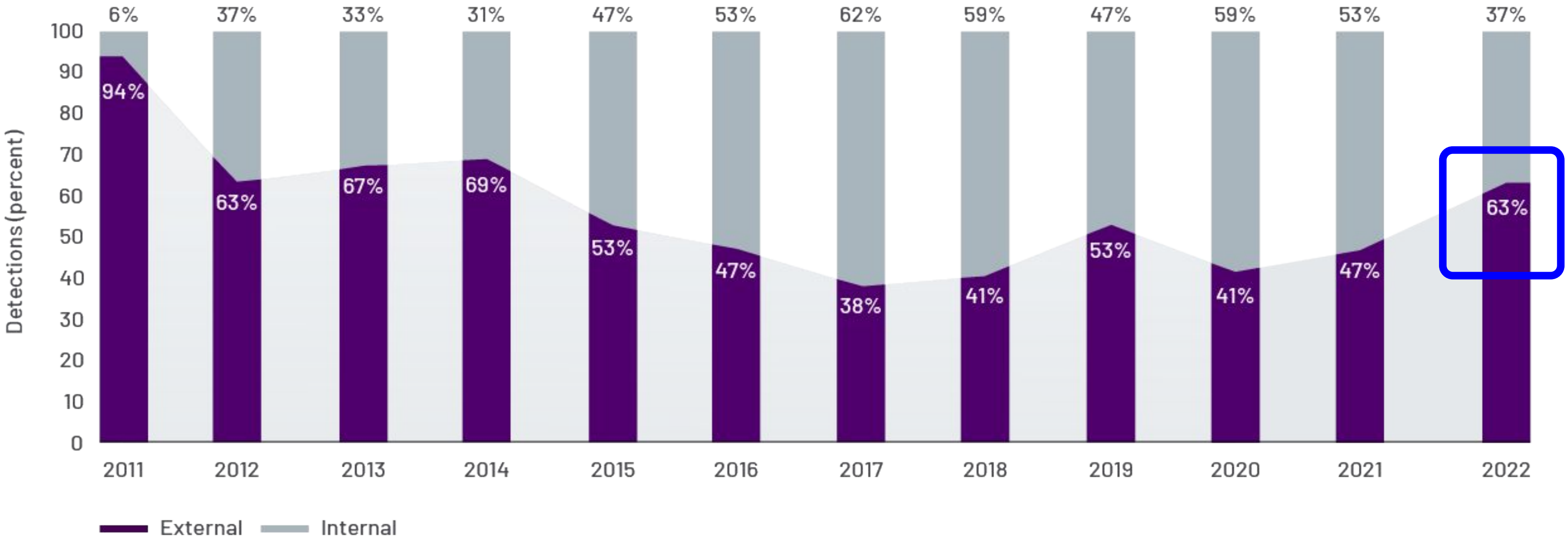


How We Find Them

Detection By Source

M-Trends 2023

Global Detection By Source



Google for Government

What They Target

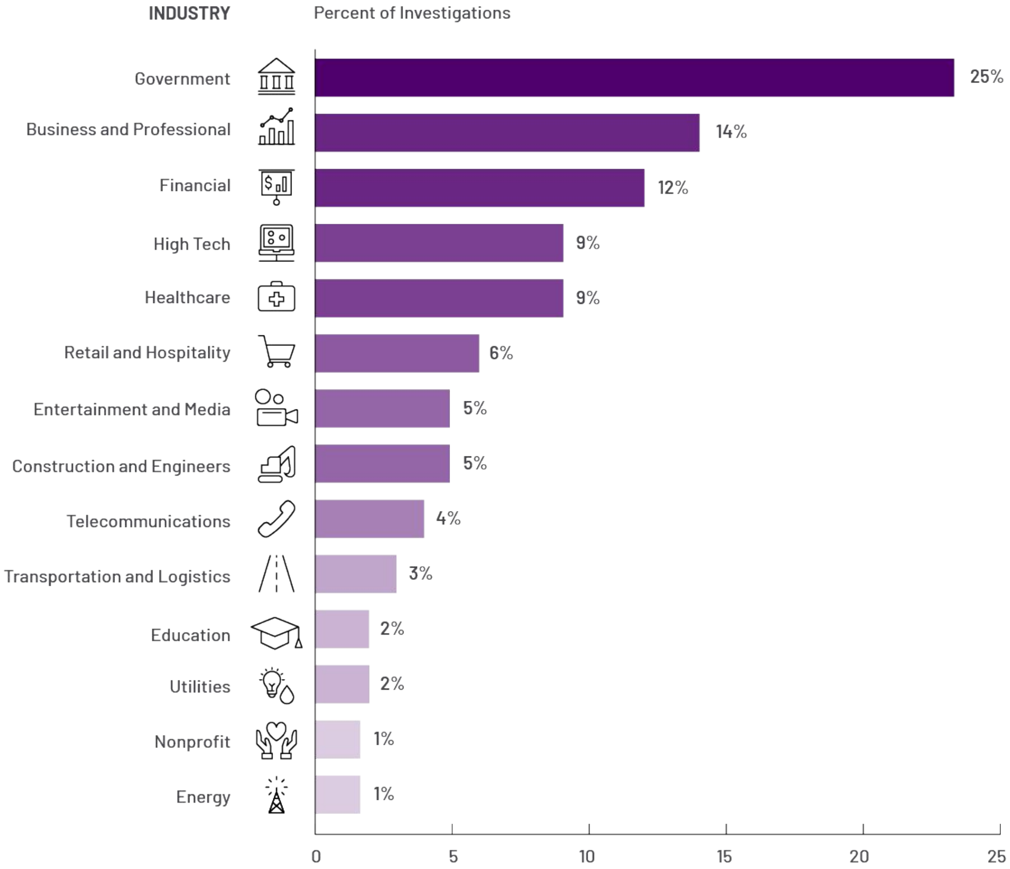
Top Industries and Adversary Mission Objectives

Top Industries Targeted

- Response efforts for government-related organizations captured a quarter of all investigations

- This primarily reflects Mandiant's work in support of Ukraine

- The next four most targeted industries are consistent with Mandiant's observations over the last two reporting periods

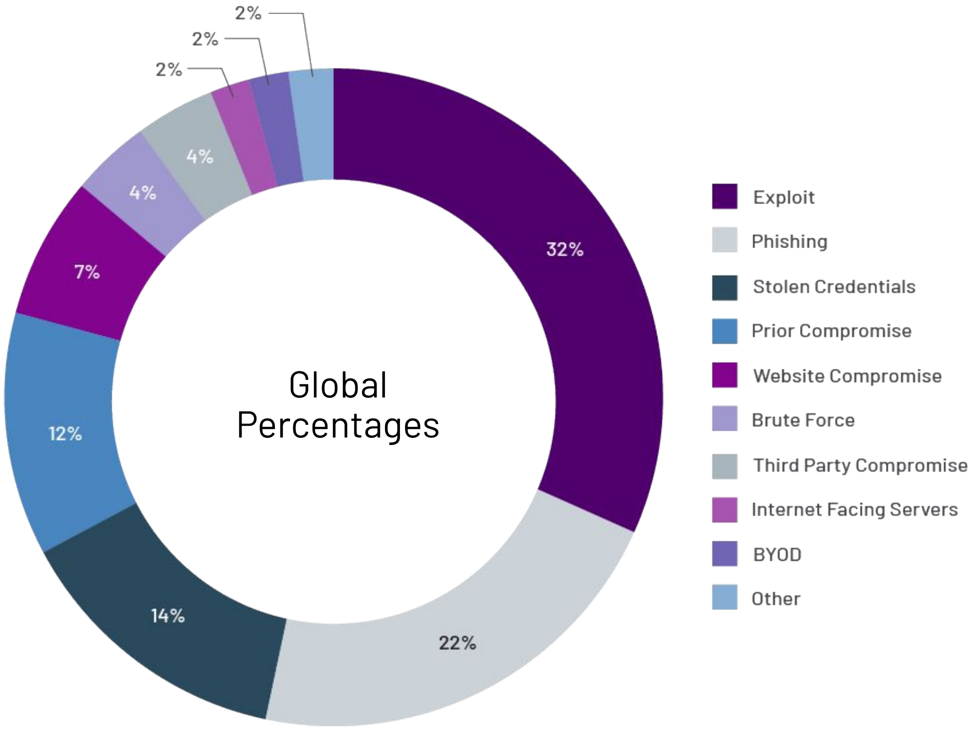


How They Do It

Infection Vectors, Threat Groups and Attacker Techniques

M-Trends 2023

Initial Infection Vector (when identified)



Most Prevalent Vector by Region

Americas: Exploits at 38%

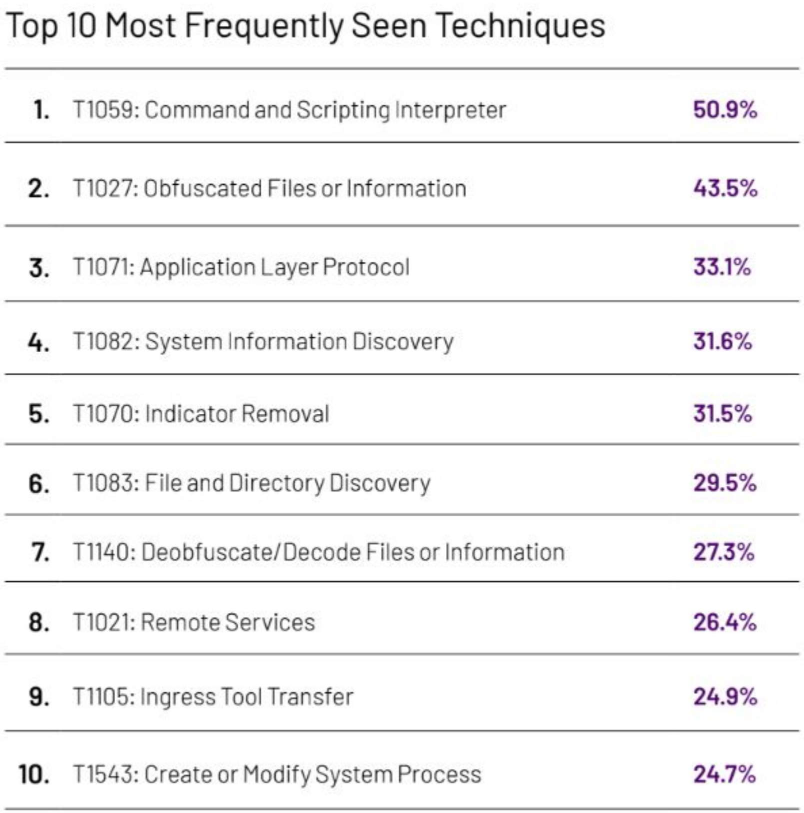
APAC: Prior Compromise at 33%

EMEA: Phishing at 40%

Most Frequently Used Adversary Techniques

43.5%

OF INTRUSIONS INVOLVED OBFUSCATED FILES OR INFORMATION (T1027) – FALLING TO THE SECOND SPOT IN 2022 COMPARED TO THE TOP SPOT IN 2021

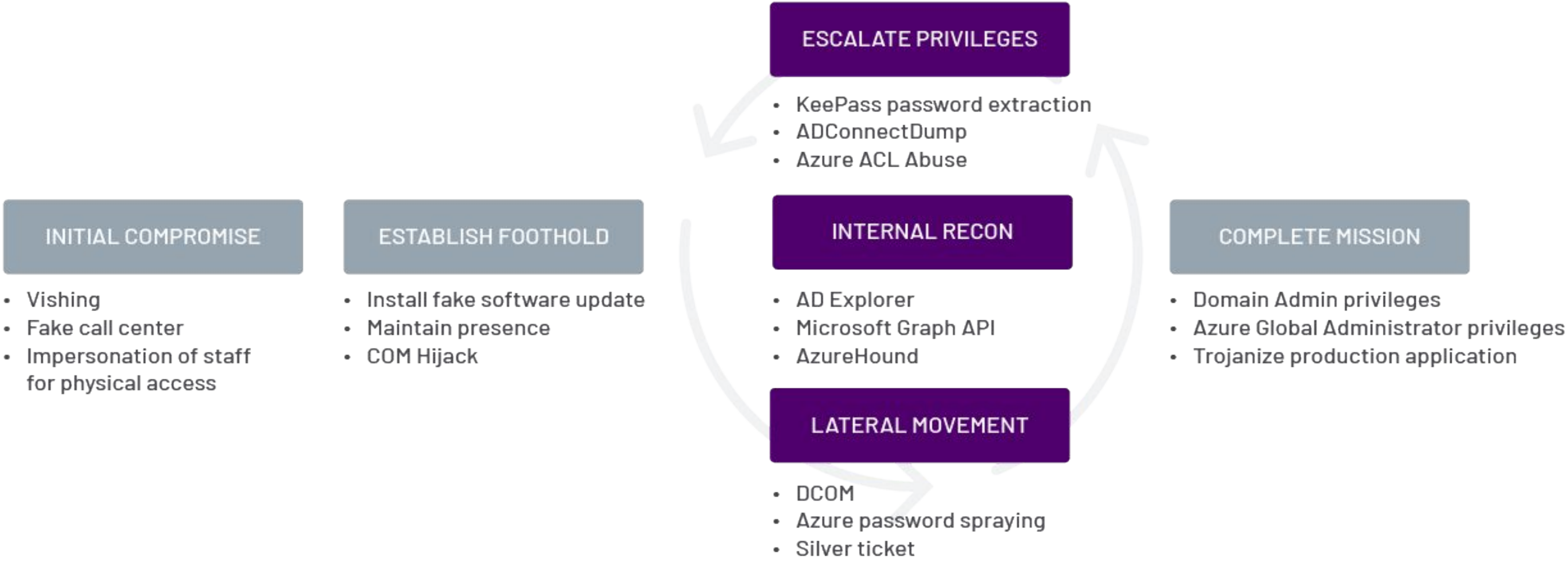


Top 10 Most Frequently Seen Techniques

1.	T1059: Command and Scripting Interpreter	50.9%
2.	T1027: Obfuscated Files or Information	43.5%
3.	T1071: Application Layer Protocol	33.1%
4.	T1082: System Information Discovery	31.6%
5.	T1070: Indicator Removal	31.5%
6.	T1083: File and Directory Discovery	29.5%
7.	T1140: Deobfuscate/Decode Files or Information	27.3%
8.	T1021: Remote Services	26.4%
9.	T1105: Ingress Tool Transfer	24.9%
10.	T1543: Create or Modify System Process	24.7%

nent

Red Team Findings: Cloud-focused Operations



INITIAL COMPROMISE

- Vishing
- Fake call center
- Impersonation of staff for physical access

ESTABLISH FOOTHOLD

- Install fake software update
- Maintain presence
- COM Hijack

ESCALATE PRIVILEGES

- KeePass password extraction
- ADConnectDump
- Azure ACL Abuse

INTERNAL RECON

- AD Explorer
- Microsoft Graph API
- AzureHound

LATERAL MOVEMENT

- DCOM
- Azure password spraying
- Silver ticket

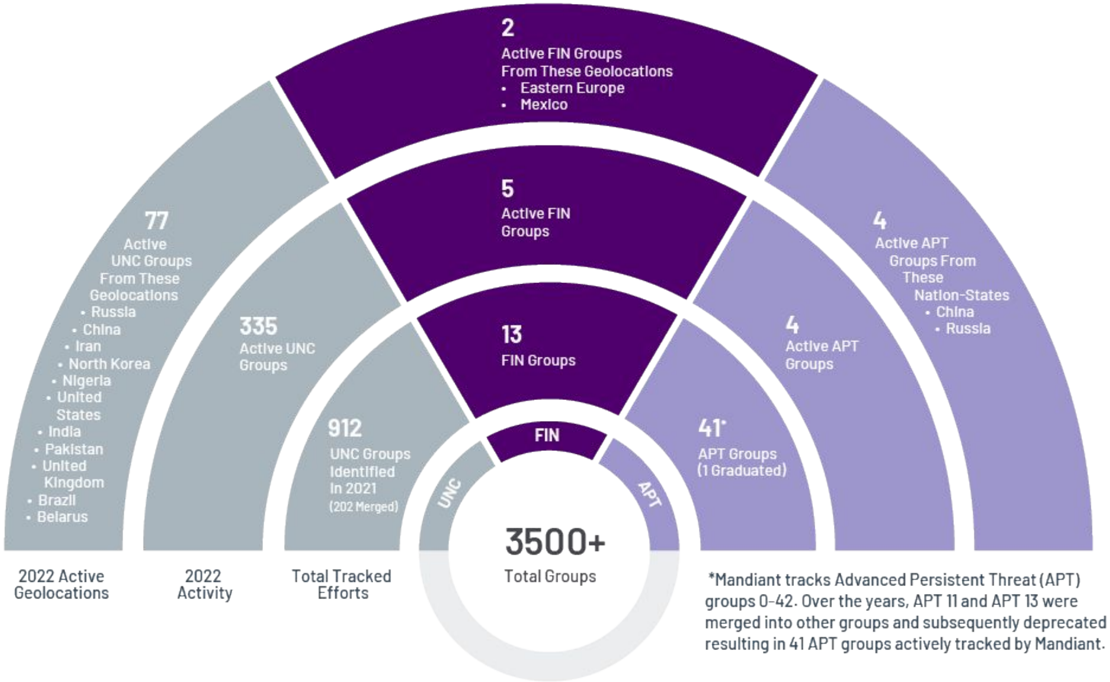
COMPLETE MISSION

- Domain Admin privileges
- Azure Global Administrator privileges
- Trojanize production application

Who They Are

Threat Groups and Malware Families

Today’s Threat Groups



2
Active FIN Groups From These Geolocations
- Eastern Europe
- Mexico

5
Active FIN Groups

13
FIN Groups

FIN

77
Active UNC Groups From These Geolocations
- Russia
- China
- Iran
- North Korea
- Nigeria
- United States
- India
- Pakistan
- United Kingdom
- Brazil
- Belarus

335
Active UNC Groups

912
UNC Groups Identified In 2021
(202 Merged)

UNC

4
Active APT Groups From These Nation-States
- China
- Russia

4
Active APT Groups

41*
APT Groups
(1 Graduated)

APT

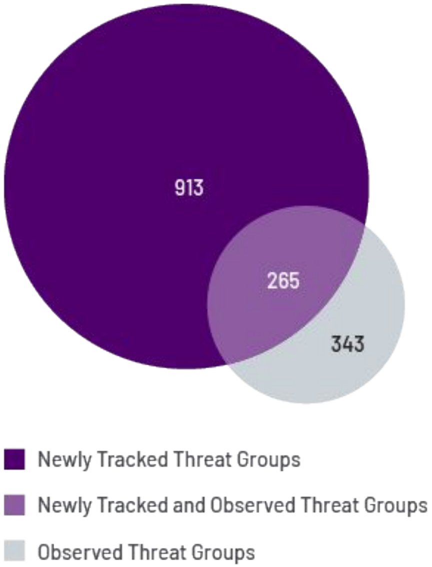
3500+
Total Groups

2022 Active Geolocations

2022 Activity

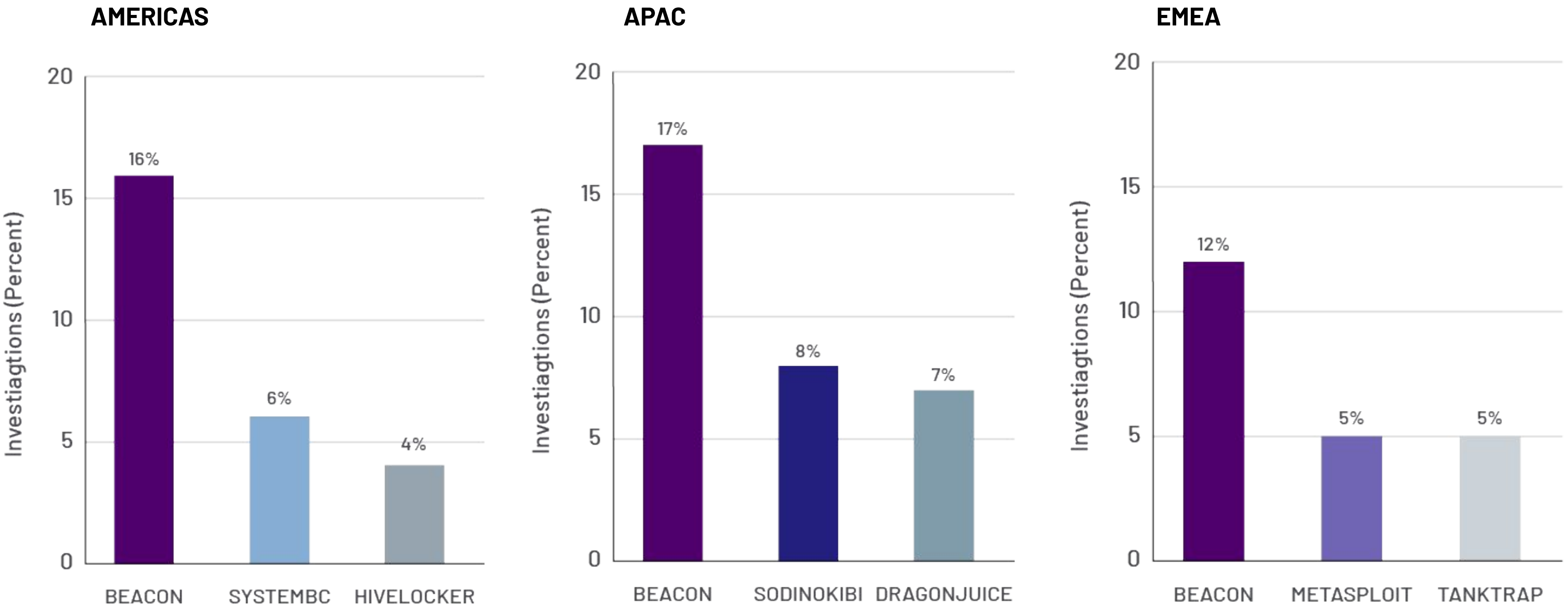
Total Tracked Efforts

*Mandiant tracks Advanced Persistent Threat (APT) groups 0-42. Over the years, APT 11 and APT 13 were merged into other groups and subsequently deprecated resulting in 41 APT groups actively tracked by Mandiant.



- ■ Newly Tracked Threat Groups
- ■ Newly Tracked and Observed Threat Groups
- ■ Observed Threat Groups

Most Frequently Seen Malware Families



'We're Doing It Wrong': The Navy's Plan for Better Cybersecurity

CIO Aaron Weis' take on a continuous ATO process includes moving to a currency mindset.

Kate Macri

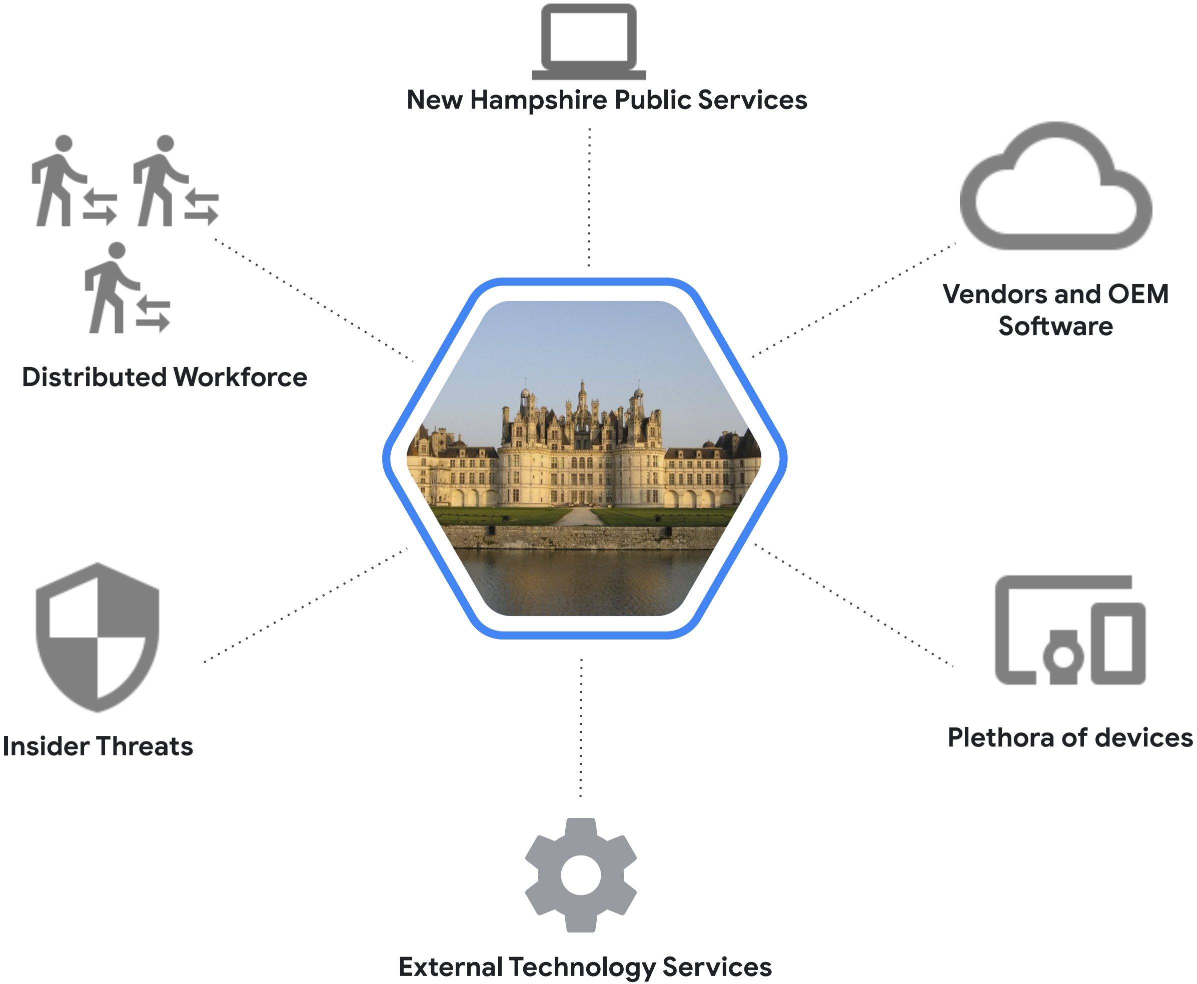
Wed, 02/15/2023 - 16:04

Photo Credit: Petty Officer 2nd Class Reymundo Villegas/DVIDS

"The way we approach the problem of cybersecurity is wrong," Weis said during a session at AFCEA West. "We're doing it wrong. We approach cybersecurity as a compliance problem, with endless checklists, RMF (risk management framework), eMASS (enterprise mission assurance support service), tools, checkers checking the checkers, years and billions of dollars. But I can tell you we have 15 years of track record that says it's not working. We continue to get our lunch money stolen and get locked out of our own lockers. What is the definition of insanity? Doing the same thing over and over again and expecting a different result."

Source: https://governmentciomedia.com/were-doing-it-wrong-navys-plan-better-cybersecurity

https://commons.wikimedia.org/wiki/File:Chambord_Castle_Northwest_facade.jpg



New Hampshire Public Services

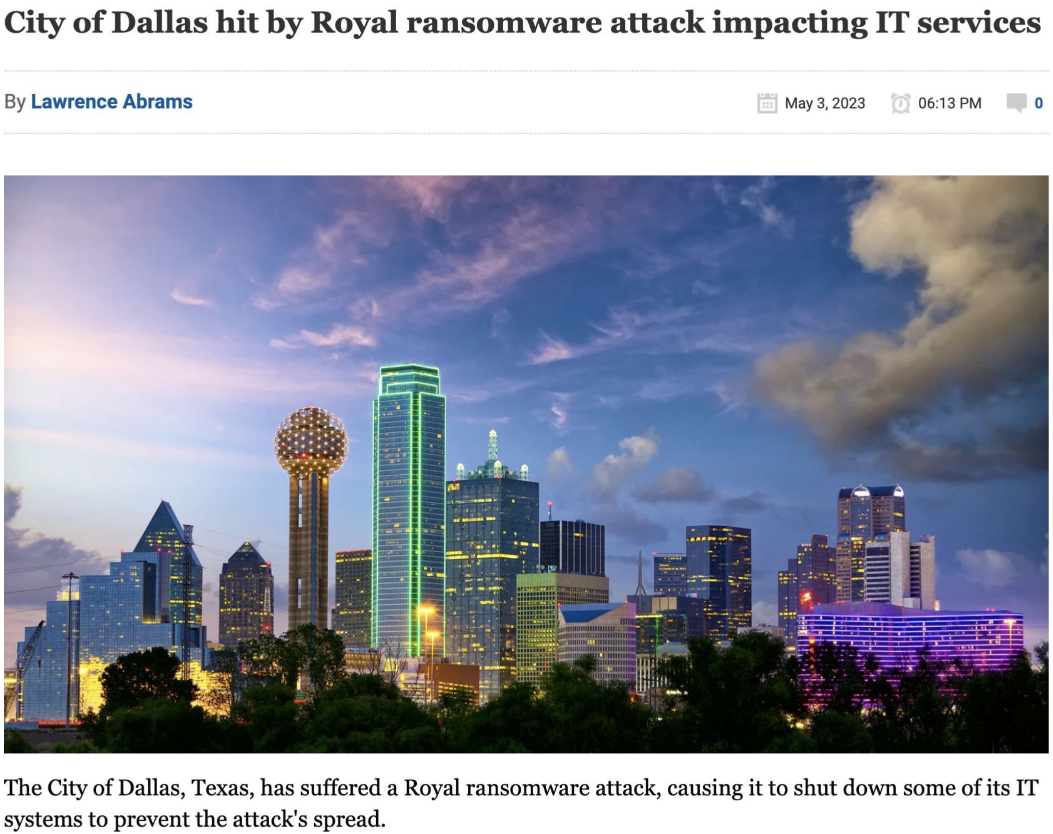
Vendors and OEM Software

Plethora of devices

External Technology Services

Insider Threats

Distributed Workforce

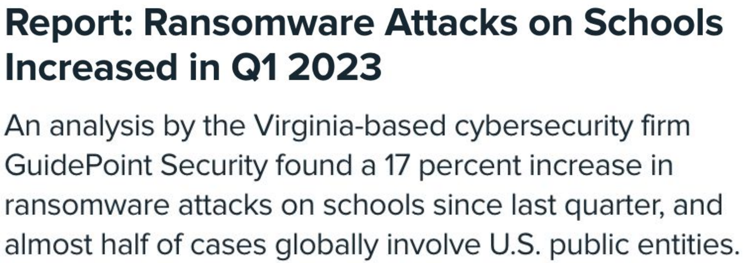


City of Dallas hit by Royal ransomware attack impacting IT services

By Lawrence Abrams

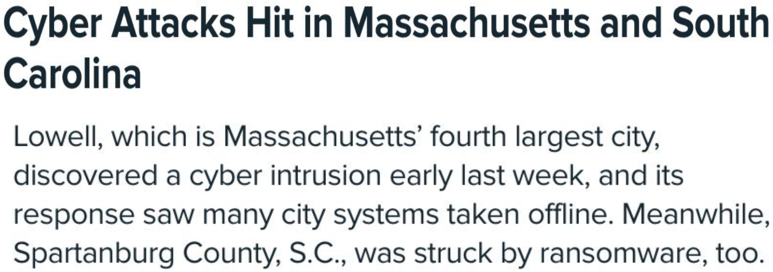
May 3, 2023 06:13 PM 0

The City of Dallas, Texas, has suffered a Royal ransomware attack, causing it to shut down some of its IT systems to prevent the attack's spread.



Report: Ransomware Attacks on Schools Increased in Q1 2023

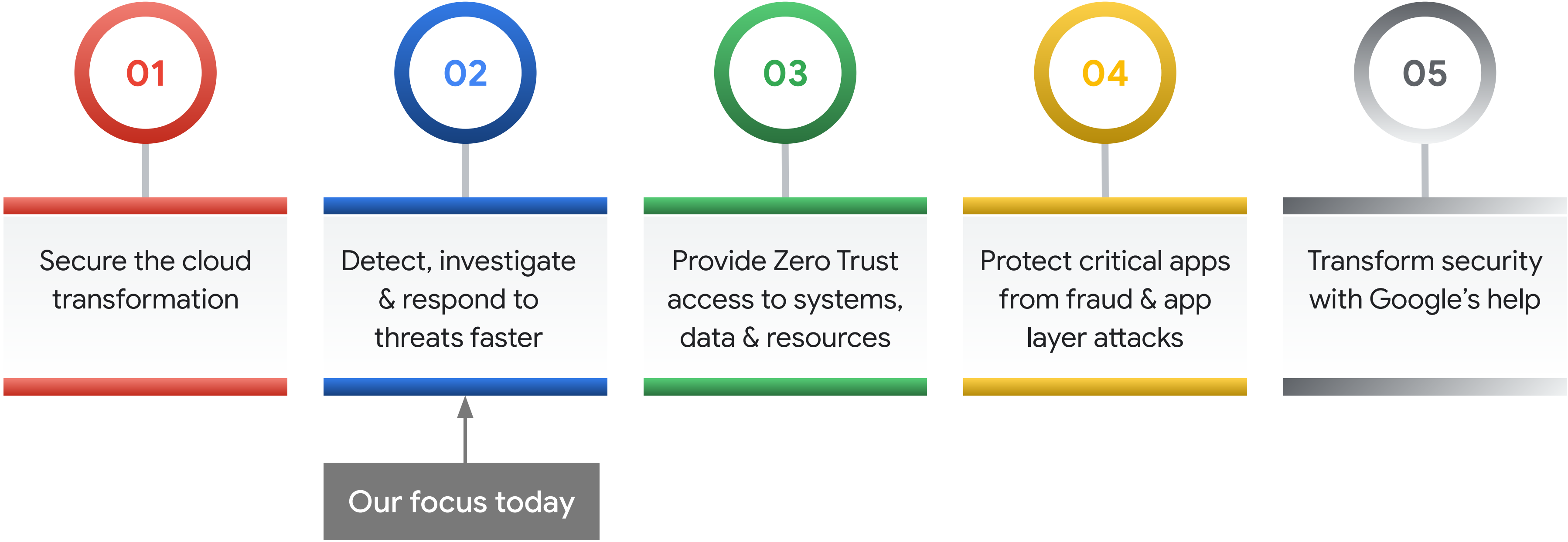
An analysis by the Virginia-based cybersecurity firm GuidePoint Security found a 17 percent increase in ransomware attacks on schools since last quarter, and almost half of cases globally involve U.S. public entities.



Cyber Attacks Hit in Massachusetts and South Carolina

Lowell, which is Massachusetts' fourth largest city, discovered a cyber intrusion early last week, and its response saw many city systems taken offline. Meanwhile, Spartanburg County, S.C., was struck by ransomware, too.

I’ve been hacked.



01 Secure the cloud transformation

02 Detect, investigate & respond to threats faster

03 Provide Zero Trust access to systems, data & resources

04 Protect critical apps from fraud & app layer attacks

05 Transform security with Google's help

Our focus today

Common SecOps Challenges

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

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

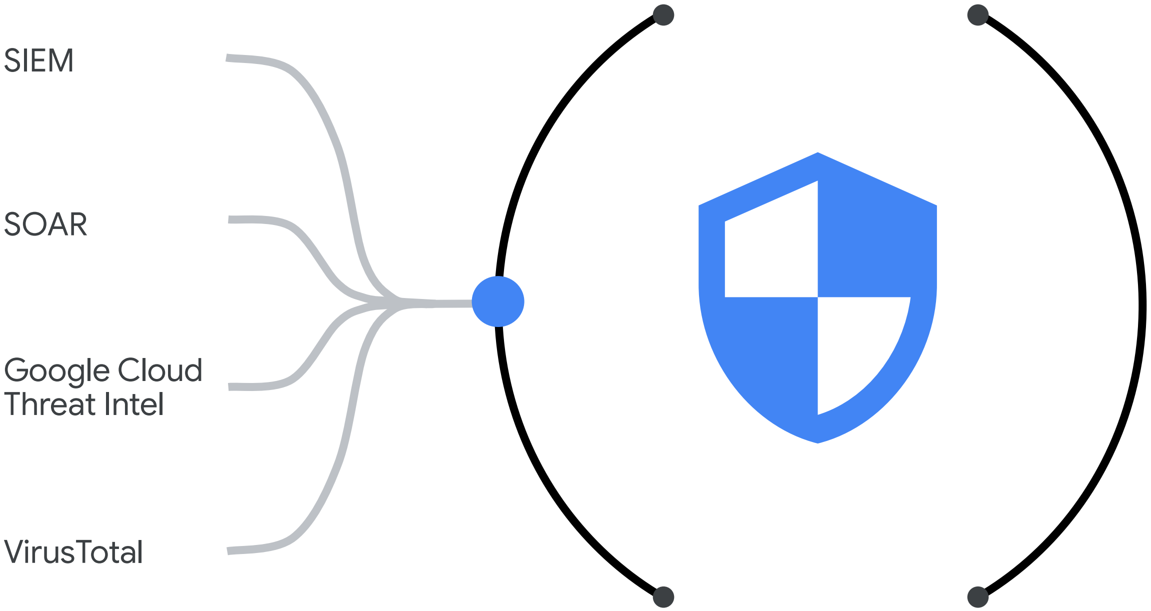
"It takes **too long** to investigate alerts"

"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"

Google Cloud Security Operations



SIEM

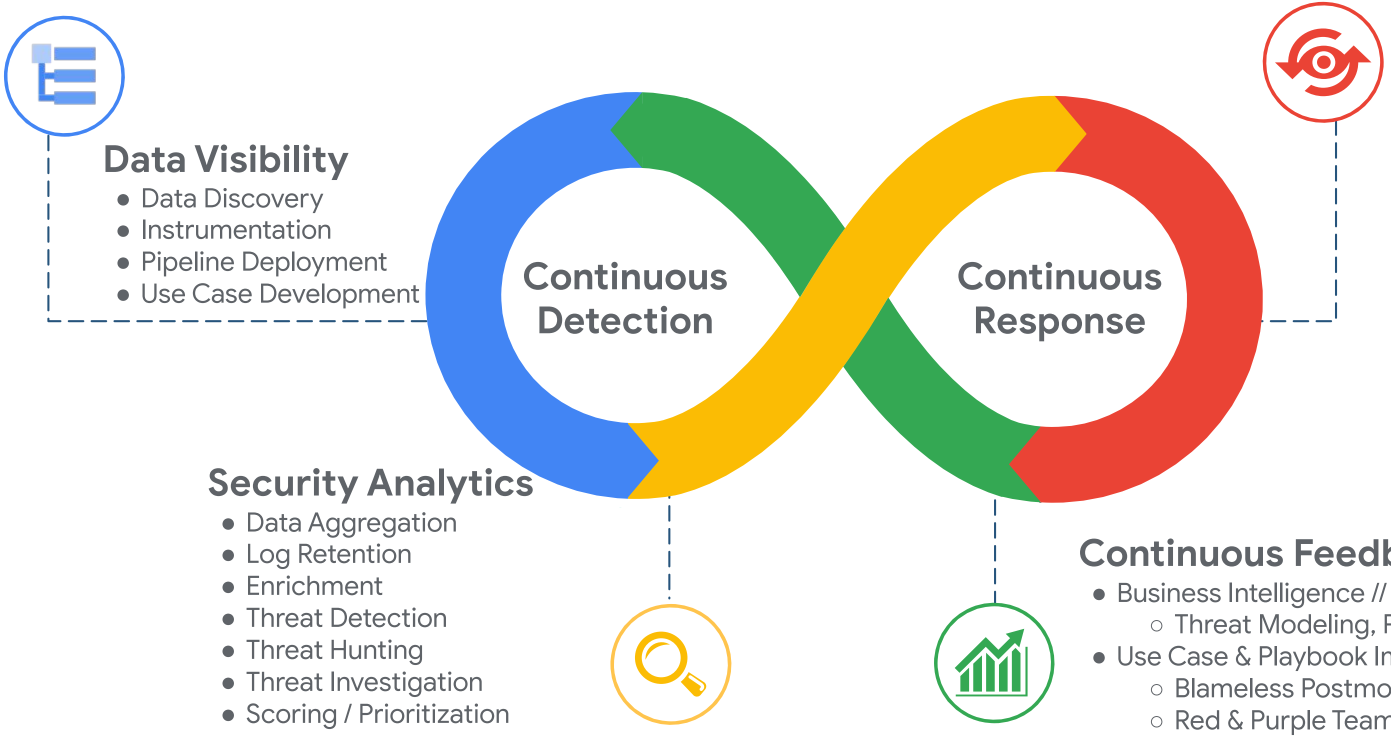
SOAR

Google Cloud Threat Intel

VirusTotal

From Assembly Line to Deployment Pipelines

Continuous Detection, Continuous Response (CD/CR) Framework



Data Visibility

- Data Discovery
- Instrumentation
- Pipeline Deployment
- Use Case Development

Security Analytics

- Data Aggregation
- Log Retention
- Enrichment
- Threat Detection
- Threat Hunting
- Threat Investigation
- Scoring / Prioritization

Response Orchestration

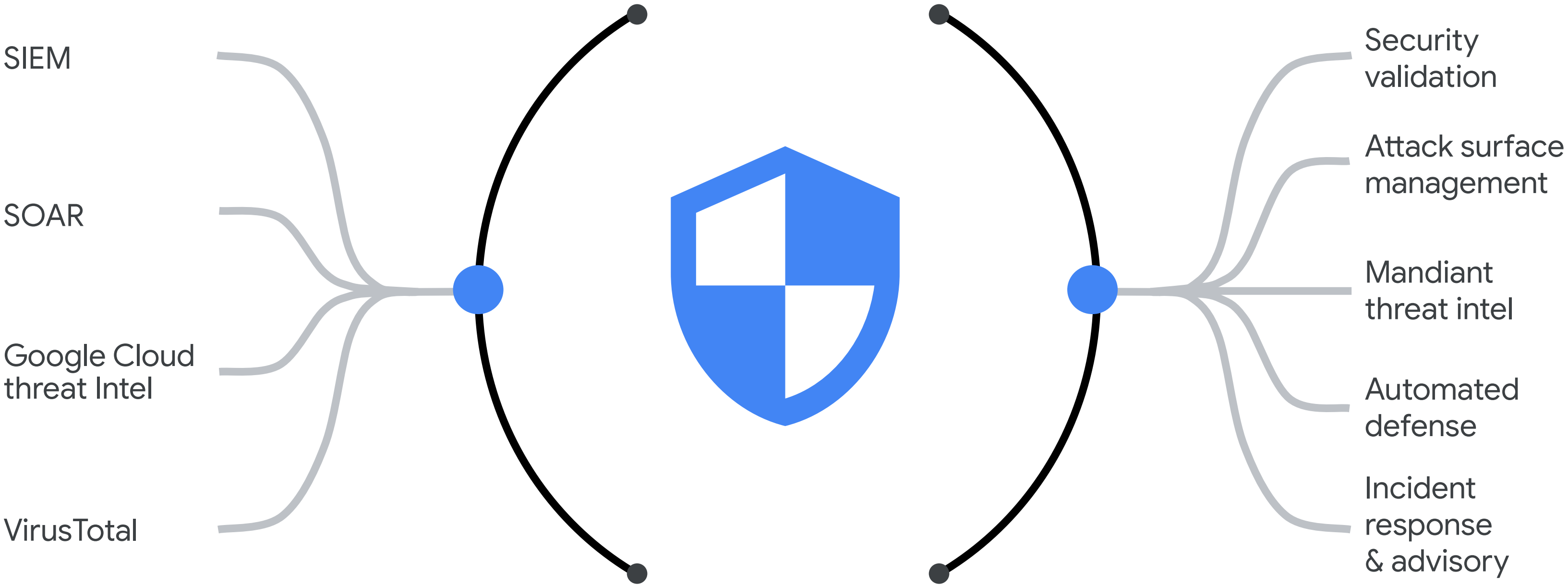
- Alert Triage
- Case Management
- Playbook Development
- Dashboards and Reports
- Response Automation
- Forensics Capture
- Incident Management
- Incident Response

Continuous Feedback

- Business Intelligence // Shifting Left
  - Threat Modeling, Preventive Controls, Architecture
- Use Case & Playbook Improvements
  - Blameless Postmortems, Metrics, OKRs
  - Red & Purple Team Exercises
  - Threat Research & Intelligence

Google Cloud MANDIANT

Bringing the power of Google and Mandiant to modernize security operations



SIEM

SOAR

Google Cloud threat Intel

VirusTotal

Security validation

Attack surface management

Mandiant threat intel

Automated defense

Incident response & advisory

Bringing the power of Google and Mandiant to modernize security operations

Cloud-scale data

Store, normalize and analyze your data - at a disruptive cost

At your fingertips

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

With frontline intelligence

Google & Mandiant’s threat detection and intelligence

Automated response

Speed up response and free up valuable analyst resources

Contextual awareness

Understand your organization from an attacker's perspective

Unparalleled expertise

Mitigate threats and reduce risk before, during and after an incident

Why Mandiant is a global leader in cybersecurity?

EXPERTISE

200K+	hours responding to attacks per year
1K+	engagements per year
1K+	Years of investigative experience

INTELLIGENCE

3K+	threat actors tracked at any time
800+	security researchers and intelligence analysts
26	countries covering 30+ languages

TECHNOLOGY

7.6B	Analyst hours saved per year through expert automation

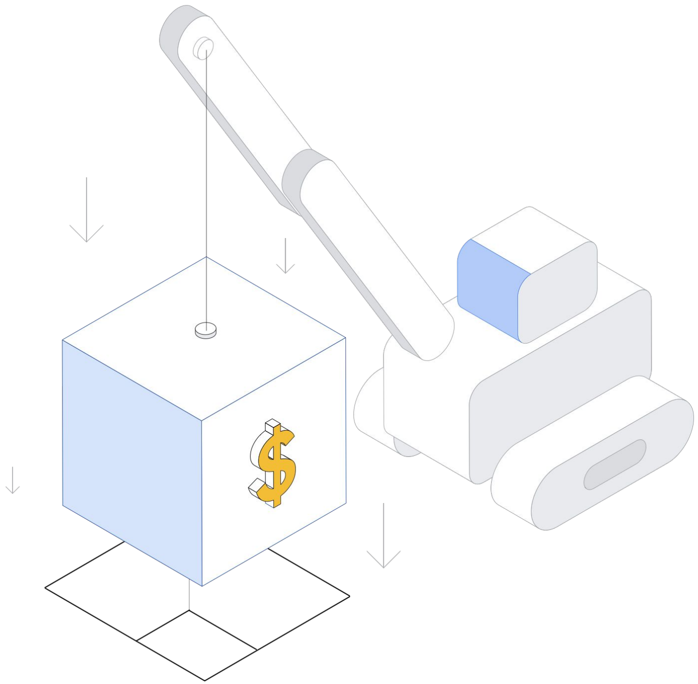
Cloud-scale Data - At a Disruptive Cost

Leverage **Google's cloud-native scalable infrastructure** to store & analyze your data to detect attacks at every level of sophistication

12 months of hot retention to enable longer IoC correlation & uncover persistent threats

Extensible unified data model provides a holistic view across all assets; raw & enriched data retained

Disruptive economics eliminate trade offs between cost & security blindspots



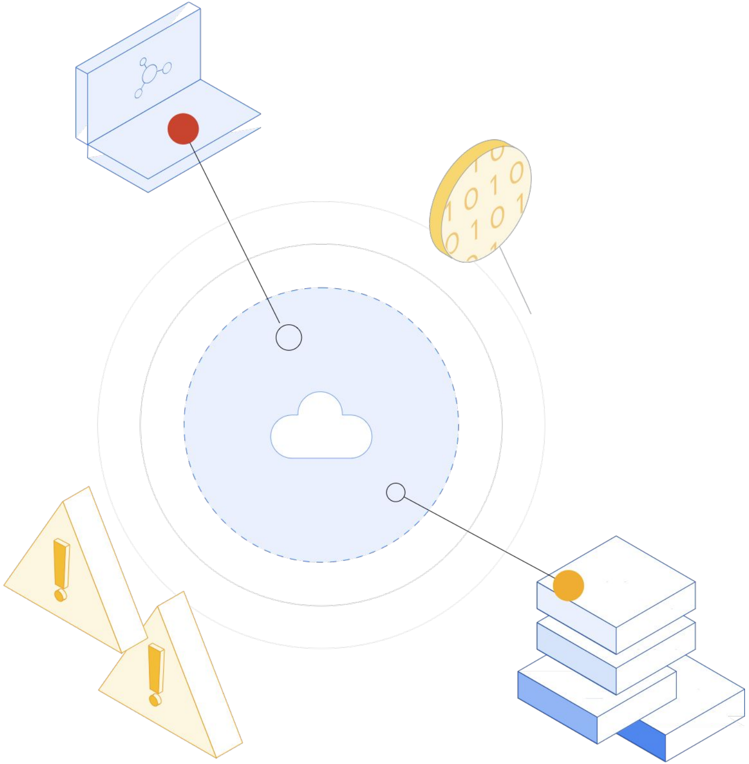
At Your Fingertips

Sub-second search results across petabytes of information

Related alerts are automatically grouped into **threat-centric cases** enabling a single analyst to efficiently investigate & respond to a threat

Powerful contextual visualizations help quickly zero in on what matters most

Mandiant Automated Defense to augment the SOC as a virtual analyst with events investigated at machine speed - all in the context of frontline intel



With Frontline Google Cloud + Mandiant Intelligence

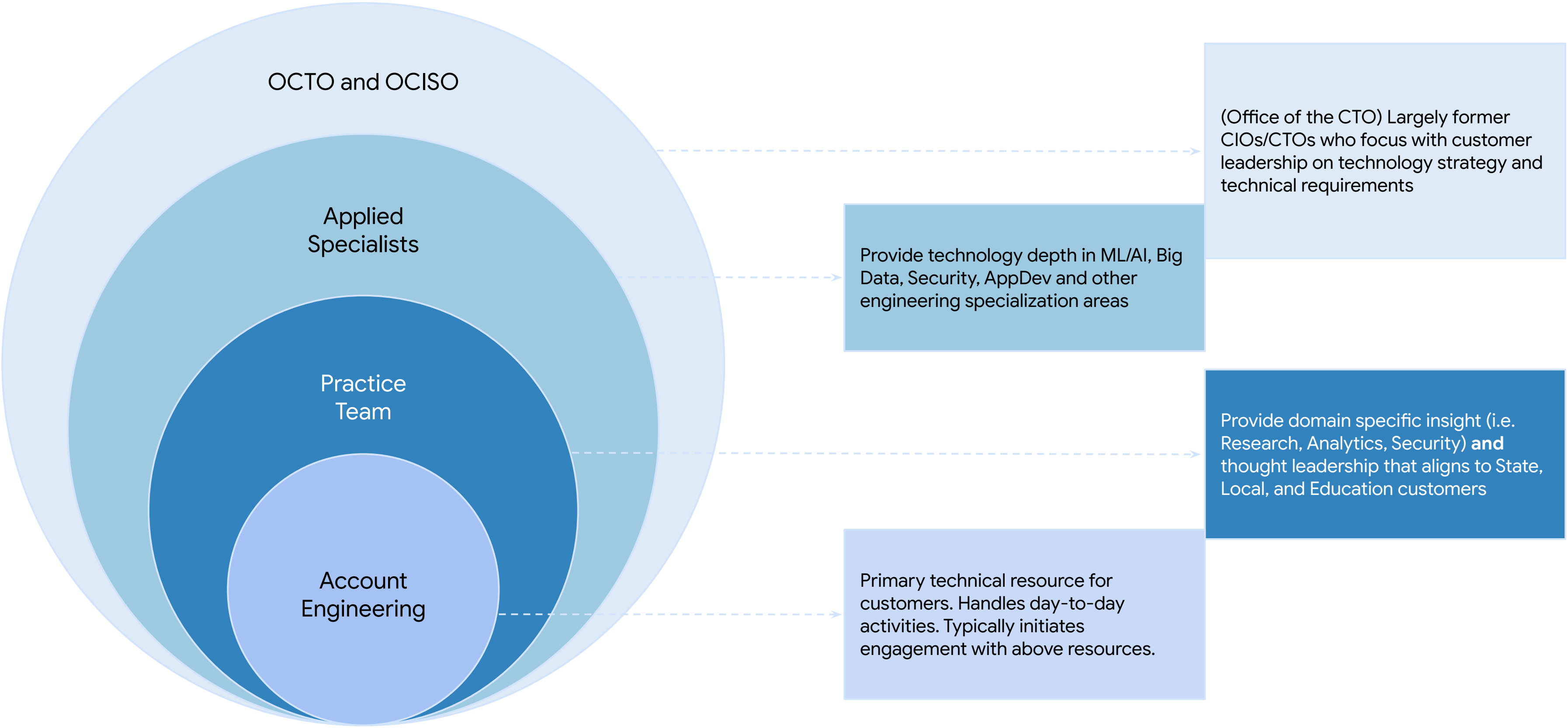
Access to **Mandiant Threat Intelligence, VirusTotal & Google Cloud Threat Intelligence**

Curated threat intelligence from providers such as Anomali, Crowdstrike as well as custom feeds

Curated detections leveraging Google's threat intel & best practices

Simplified detection authoring powered by YARA-L

The Engineering Ecosystem



OCTO and OCISO

(Office of the CTO) Largely former CIOs/CTOs who focus with customer leadership on technology strategy and technical requirements

Applied Specialists

Provide technology depth in ML/AI, Big Data, Security, AppDev and other engineering specialization areas

Practice Team

Provide domain specific insight (i.e. Research, Analytics, Security) **and** thought leadership that aligns to State, Local, and Education customers

Account Engineering

Primary technical resource for customers. Handles day-to-day activities. Typically initiates engagement with above resources.

Unique, up-to-date and actionable intel

Help before, during and after incidents

Transform your cybersecurity with frontline intelligence, expertise and AI-powered cloud innovation

Supercharging security with generative AI - across our entire portfolio

Google Public Sector

Accelerate innovation to meet your mission

Amar Parikh - amarpar@google.com

Nick Haas - nickhaas@google.com

Google for Government