Google SecOps

Das Gute sichern

Mit Cybersicherheit die Kontrolle behalten

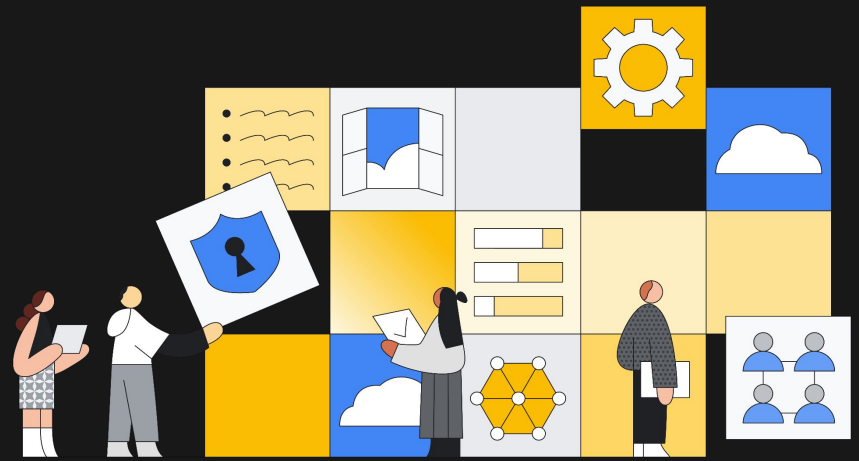
October 2024, @pverzi, PE, GCS

Google Cloud Security

Google

here
for
you

Pietro Verzi
Partner Engineering
Global Security Sales



Cyber risk has become many organizations **biggest risk**

Managing it effectively is **imperative** to succeed and thrive going forward

Old world

- Limited number of highly advanced attackers
- Nation-state level resources required
- Targeting governments and critical infrastructure
- Cyber-espionage focus

New World

- Numerous well-funded “commercial” threat actors
- Broad knowledge of advanced TTPs, exploits, tooling
- Targeting enterprises of all sizes and sectors
- Financial gain, business disruption focus

Increase in bot attacks

84%

of companies saw an increase in the number of bot attacks over the last year.

Successful attacks

71%

of those same companies saw an increase in successful attacks

Time spent resolving an attack

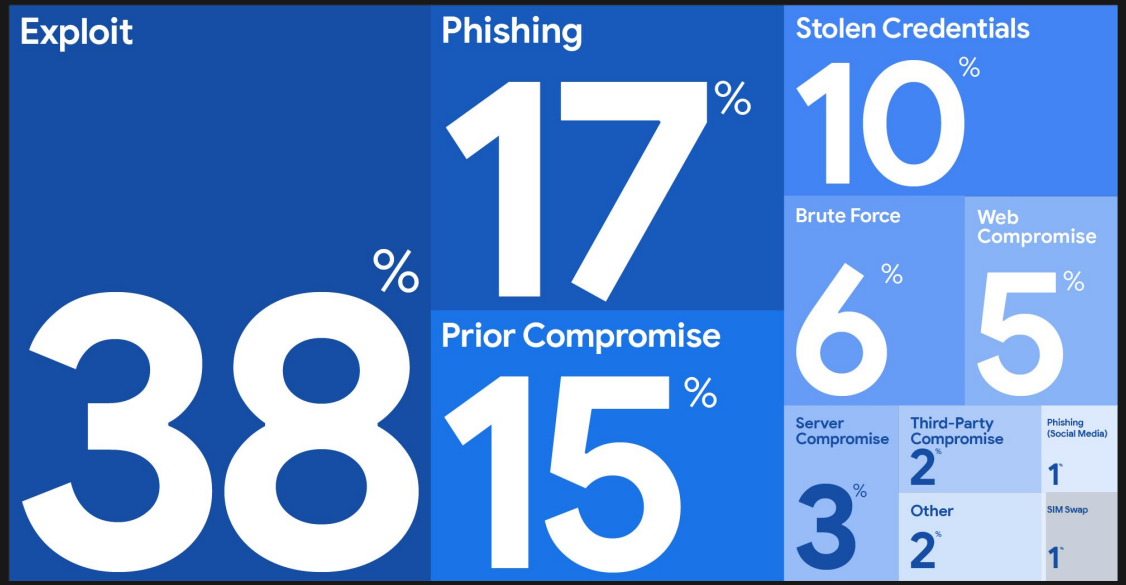
53 Days

of time spent on average fully resolving a bot attack

FORRESTER 2021

Initial infection vectors

Initial infection vector (when identified), 2023



Exploits are also the top vector by region

Americas: 41%

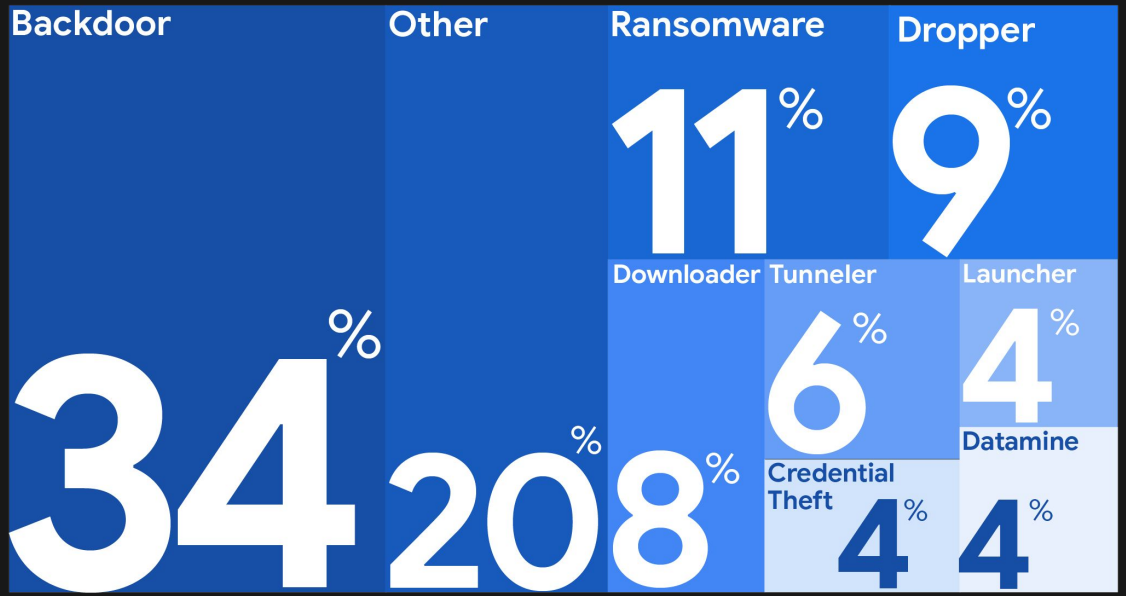
APAC: 39%

EMEA: 37%

Google

Malware categories and families

Observed Malware Families by Category, 2023



Most frequently seen malware families:

- BEACON (Backdoor)
- ALPHV (Ransomware)
- LEMERLOOT (Web Shell)
- SYSTEMBC (Tunneler)
- LOCKBIT (Ransomware)

Google keeps more people safe online than anyone else

5 billion
Google Safe Browsing users devices protected each day from malware and social engineering

2.5 billion
Active Gmail users protected against phishing, malware, and spam through embedded security monitoring

2.4 billion
Files and URLs analyzed by VirusTotal, the world's premier malware intelligence service

Petabytes
Of cloud telemetry analyzed each day by Chronicle and Security Command Center for threat detection and response

398m rps
DDoS attack, the largest ever recorded, was prevented by Google's network and Cloud Armor

Adopting Google's security approach

01

Trust Nothing

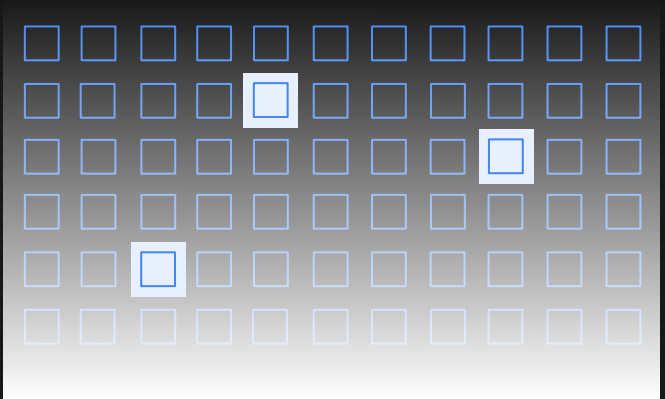
02

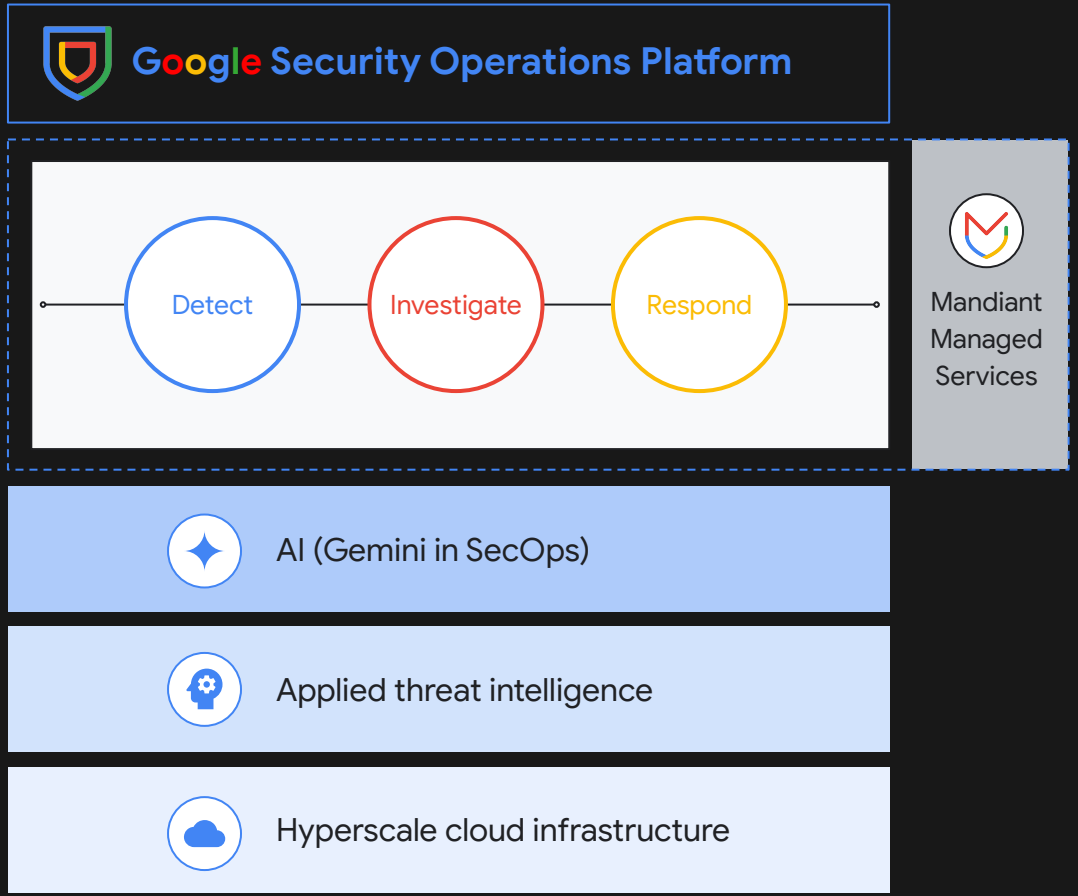
Detect Everything

03

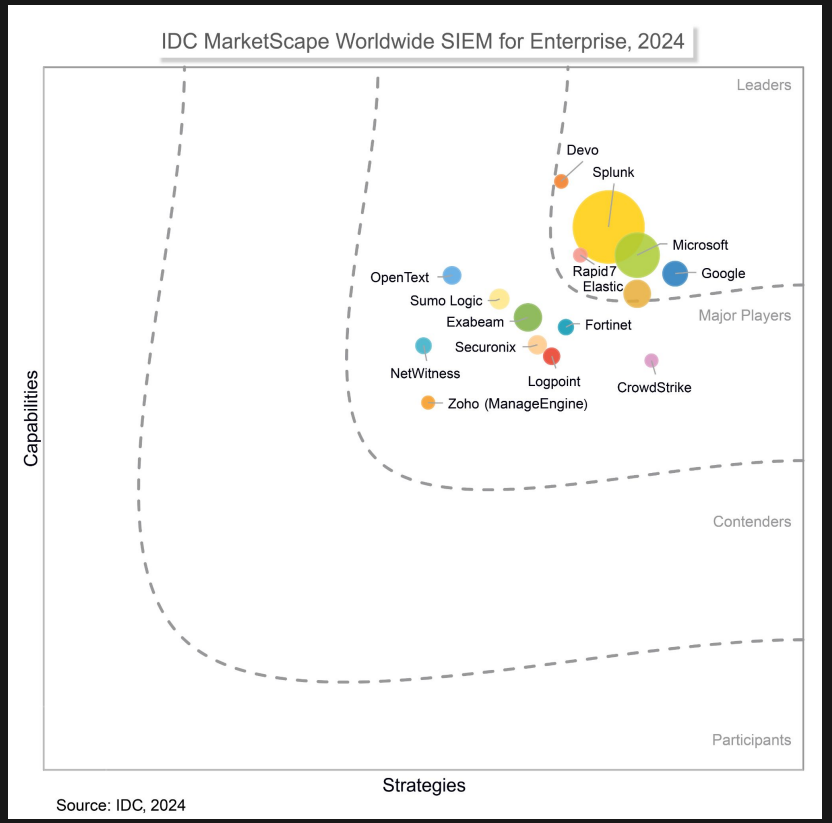
Know What Google Knows

A Unified AI and Intel-Driven Platform for Threat Detection, Investigation and Response





Google: a Leader in the Worldwide SIEM for Enterprise 2024 Vendor Assessment



Source: "IDC MarketScape Worldwide SIEM for Enterprise 2024 Vendor Assessment", By Michelle Abraham, September 2024, IDC #US51541324

IDC MarketScape vendor analysis model is designed to provide an overview of the competitive fitness of ICT suppliers in a given market. The research methodology utilizes a rigorous scoring methodology based on both qualitative and quantitative criteria that results in a single graphical illustration of each vendor's position within a given market. The Capabilities score measures vendor product, go-to-market and business execution in the short-term. The Strategy score measures alignment of vendor strategies with customer requirements in a 3-5-year timeframe. Vendor market share is represented by the size of the icons.

Google

Google Threat Intelligence

Combine frontline, curated, open source, and crowdsourced intelligence

Frontline expertise

Research, analysis, threat actors, TTPs, and reporting

Crowdsourced intelligence

Verdicts, OSINT, crowdsourced rules, community

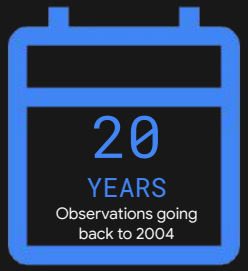
Threat insights

Security scanning devices, URLs, and files

AI-infused threat intelligence: risk profiling; digested threat intel; AI-assisted malware analysis

Unmatched visibility into threats

Far reaching **breadth** and detailed **depth**



50B+ files
Across thousands of file formats for all operating systems

1.5B+ Sandbox reports

2M Analyses per day

232 ISO COUNTRIES submitting files

3M+ MONTHLY USERS sourcing data

6B+ URLs
6M+ URL analyses per day

5B+ Domains

170B+ pDNS Resolutions

45/71

70+ Antivirus
90+ URL blocklists
20+ Sandboxes
30+ Crowdsourced {YARA, SIGMA, IDS} repos
100K+ Crowdsourced rules

1000+
Total employees supporting IR

300+
Incident response consultants

1100+
Investigations per year

400k
Incident investigation hours in 2023

4 Billion
Google Safe Browsing user devices protected each day from malware and social engineering

500+
Researchers & analysts

30+
Languages spoken

350+
Tracked threat groups

53+
Countries with incident response engagements

1.5 Billion
Active Gmail users protected against phishing, malware, and spam through embedded security monitoring

Google

Market leading threat intelligence

5B+
Devices protected

2B+
Gmail inboxes protected

200k
hours responding to attacks per year

1k+
Incidents responded to per year

+300
threat actors tracked at any time

+500
security researchers & intelligence analysts

43B
Files scanned per day

3.6 Billion
Files in the dataset

+30k
Intelligence reports

Google

Customer

Safer with **Google**

Thank you

Google