CyberProof®
A UST Company

Better Security, Together.

Google SecOps

AGENTIC SOC · AGENTIC MXDR · AI-DRIVEN, HUMAN-LED SECURITY OPERATIONS

The Agentic SOC Vision

Get full value from your Google SecOps deployment

A fleet of autonomous SOC agents operating with human supervision to defend at machine scale and speed.

<1 min
Time to Detect

<1 min
Time to Investigate & Respond

Google Cloud Partner
Managed Service Provider

Powered by a hyperscale SecOps platform — Google Security Operations.
CyberProof is a Google Cloud Partner and Managed Service Provider.

© 2027 CyberProof. Agentic SOC and Agentic MXDR, co-delivered with Google SecOps.

cyberproof.com

THE OUTCOME

From 90 minutes to 10 minutes: a 9× faster response

Human-led, agent-executed. Your team sets the autonomy thresholds and owns the outcome; agents execute the lifecycle at machine scale and speed.

<30 sec	<5 min	30 min	10 min
Mean time to acknowledge	Mean time to detect	Mean time to respond today (from 90 min)	Mean time to respond, committed target

MEAN TIME TO RESPOND

70%
of investigations handled agentically

100%
of cases QA'd — not a sample

30+
CyberProof agents in production

Agents execute

- Analyze and operationalize all incoming threat intelligence
- Hunt for new threat actors and validate the posture of your environment
- Triage, enrich and investigate every alert; open cases on positive findings
- Create new detections, validate detection health, optimize ingestion
- Produce the QA record on 100% of cases

People lead

- Set the detection roadmap and the autonomy threshold per action class
- Approve consequential action — isolation, disablement, blocking
- Lead major incidents and own the escalation path
- Answer to you, by name, for the result — nothing irreversible happens without a named human

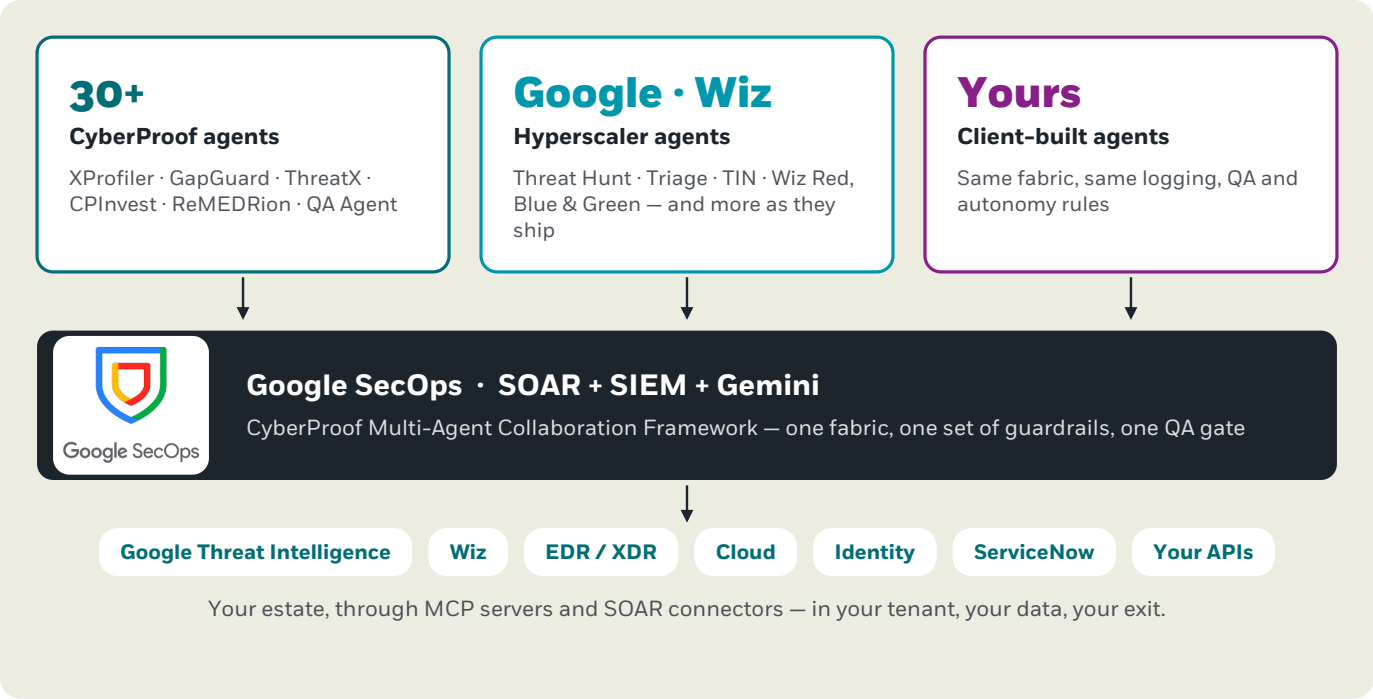
THE OPERATING PRINCIPLE

Human led, agent executed. Agents drive the security lifecycle to positive outcomes; people set the autonomy thresholds, approve consequential actions and own the result.

HOW IT WORKS

One Agentic SOC fabric on Google SecOps – your agents, ours, Google's and Wiz's

SOAR-orchestrated, A2A and MCP native. Every agent runs under the same logging, QA and autonomy rules, whoever built it — and escalates to a named human on defined thresholds.



SIX OF THE AGENTS ALREADY IN PRODUCTION

X	G	T	C	R	Q
XProfiler	**GapGuard**	**ThreatX**	**CPInvest**	**ReMEDRion**	**QA Agent**
Threat profiler	MITRE mapping	Threat hunting	Agentic investigation	EDR health	SOC case QA

Human on threshold

Autonomy is granted per action class, not per agent. Every agent action is logged, attributable and reversible; escalation to a named person is a rule, not a hope.

SECURED BY DESIGN — OWASP AGENTIC TOP 10

8 of 10 risk classes avoided by design

2 of 10 risk classes reduced by controls

- **No natural-language input to the agents**
- **Strong RBAC, limited spawning, limited execution**
- **Frontier models in hyperscaler environments**

Why Google SecOps, why CyberProof – and how you buy it

The modern Agentic SOC runs on Google SecOps. We deploy it, migrate you onto it and operate it with you; the solution is transacted through the Google Cloud Marketplace.

WHY GOOGLE FOR DEFENSE

Google Cloud

Google SecOps

Cloud-native SIEM and SOAR at petabyte scale on a flat-rate cost model — log what matters, not what you can afford.

Google Threat Intelligence

Mandiant frontline intelligence and VirusTotal telemetry drive our detection roadmap and your threat profile.

Gemini and agents in SecOps

Native summarisation, natural-language search, Threat Hunt and Triage agents where the analyst already works.

Google Cloud Marketplace

A transactable offer that draws down committed Google Cloud spend — procurement within minutes.

Proof

CyberProof delivered the first Google SecOps deployment of cloud-native SIEM + SOAR for an Enterprise+ client.

What we bring

Migration off legacy SIEM with a modelled cost case, ported detection content, and 24x7 co-managed Agentic SOC operations from day one.

Your tenant, your data

We operate inside your Google tenant. You own the data, the detections and the exit.

HOW YOU BUY IT

Co-sold with Google → **Transacted** on Google Cloud Marketplace → **Delivered & operated** by CyberProof

One contract, one accountable Agentic SOC operator, and procurement within minutes.

Petabyte
scale, cloud-native SIEM + SOAR

Flat-rate
cost model — log what matters

Minutes
to procure via Marketplace

24x7
co-managed operations from day one

AGENTIC SOC · THE DECISION

Ready to run your Agentic SOC?

A method, not a migration weekend. Five stages, each producing an artifact you own — and nothing degrades while it changes.

01 Assess	02 Decide	03 Build	04 Cut over	05 Run agentic
ARTIFACT	ARTIFACT	ARTIFACT	ARTIFACT	ARTIFACT
Current-state & readiness assessment	**Target architecture & decision record**	**Content pack & agent autonomy matrix**	**Cutover runbook & parity evidence**	**Operating manual & commitment baseline**

WHAT YOU ALWAYS KEEP

- Your tenant, your data, your exit
- Detection content, runbooks and hunt hypotheses — portable and exportable
- The autonomy threshold for every action class
- Any function, back in-house, whenever you decide

THE NEXT STEP

co-sold with Google · on Marketplace

Start with a current-state & readiness assessment

Detection content, data sources, tooling, licences, run-rate and threat profile — measured, not surveyed. You leave stage 01 with the evidence to decide greenfield or migrate, and a decision record you own either way.

Contact Us

10 min
Mean time to respond — committed target

70%
Of investigations handled agentically

100%
Of cases QA'd, not a sample

CyberProof® A UST Company | Better Security, Together.

Google SecOps

Google Cloud Partner
Managed Service Provider

© 2027 CyberProof. All rights reserved.

cyberproof.com