Autocops NetGraph

AutoCops NETGRAPH
Continuous Exposure Management

CONTINUOUS EXPOSURE MANAGEMENT

Unify. Correlate. Mobilize — a graph-native, open Security Operations Platform.

THE NEED — WHY A NEW APPROACH

- **Unaffordable economics**
  Mid-market teams cannot carry legacy SIEM ingestion pricing and tiered licensing.
- **Ten disconnected tools**
  SIEM, SOAR, TIP, EDR, NDR, CSPM, CNAPP, DSPM, VM, BAS — stitched together with dashboards.
- **No single source of truth**
  Logs, identities, assets, CVEs, code & cloud posture sit in separate index domains.
- **Blast radius unanswerable**
  "What is exposed across code, cloud, identity, data & network — right now, and historically?"

THE NETGRAPH PLATFORM APPROACH

- **One security knowledge graph**
  Every event, alert, asset, identity, CVE & finding is a typed node — detection is traversal.
- **Converged, not stitched**
  26 modules — SIEM through CNAPP, VM and Agentic AI — share one identity-asset-data graph.
- **Open data, zero lock-in**
  Parquet, Iceberg, OCSF & OTel throughout — detach NetGraph, keep querying your data.
- **Self-sufficient & sovereign**
  Runs fully air-gapped; no paid SaaS for any Tier-1 detection; DPDP / CERT-In built in.

ONE GRAPH

Detect, hunt, respond & assess exposure as graph traversal.

≤ 15% COST

Of legacy SIEM ingestion economics at matched retention.

AIR-GAP READY

Full function with zero dependency on any external SaaS.

AGENTIC SOC

Five LLM agents — grounded, cited and human-gated.

PROVEN AT GA 100k EPS / shard <60s source-to-searchable <2s hot-tier query 200+ BAS-tested detections

Twenty-Six Modules. One Graph. One Console.

DATA PLANE

- **Ingestion**
  100k EPS/shard · OCSF 1.3+ · agent & agentless
- **Processing**
  Flink / Spark enrichment · UEBA features
- **Storage**
  Hot ClickHouse · warm Iceberg · knowledge graph

DETECT & RESPOND

- **Detection Engineering**
  Sigma-as-Code · Git CI · BAS-gated
- **Correlation + Context**
  Three engines · sub-100ms context service
- **Alerting**
  Graph-proximity grouping · risk weighting
- **SOAR / Workflows**
  Temporal · 100+ integrations · 30+ playbooks
- **Remediation**
  Identity / endpoint / cloud · blast-radius preview
- **NDR & CDR**
  Zeek / Suricata · beacon detection · cloud-TTP

HUNT & VALIDATE

- **Threat Hunting**
  50+ hunts · hunt-to-detection compiler
- **BAS / ATT&CK Emulation**
  Atomic Red Team + Caldera · CI gating
- **Retrospective Analysis**
  Auto-replay over 90+ days of history
- **Threat Intelligence**
  STIX / TAXII · free mirrorable feeds
- **UEBA & Analytics**
  Risk 0-100 · graph embeddings · explainable

EXPOSURE & POSTURE

- **Vulnerability Management**
  VulnRisk score · reachability proof
- **CNAPP**
  IaC + image scan · runtime Falco · SBOM graph
- **CSPM**
  AWS / Azure / GCP · CIS packs · drift-to-IaC
- **DSPM**
  Aadhaar / PAN classifiers · data-flow graph
- **CTEM**
  Attack-surface inventory · exposure paths
- **SAST / DAST**
  Semgrep / Gitleaks + ZAP / Nuclei · SARIF
- **Phishing Simulation**
  Eight Indian languages · user-risk graph

Plus **Compliance · Reporting · Forensics & Case Management · Graph RAG · Agentic AI (five SOC agents)** — every module tenant-native at GA.

WHAT NO INCUMBENT SHIPS NATIVELY

Graph is the substrate
Detections, hunts, posture & SOAR are graph operations.

Detection-as-Code + BAS
Every detection ships an emulation test; CI fails on regression.

Retrospective by default
New or changed detections auto-replay against history.

Reachability-aware VM
Prioritised by real blast radius — not CVSS in isolation.

Open data guarantee
Detach NetGraph at any time; your data stays queryable.

Air-gap-ready, India-first
No phone-home; DPDP / CERT-In / RBI / SEBI built in.

Unified Fabric at Work — Continuous Exposure Management

01 Account Takeover → Lateral Movement, Contained

Okta sign-in from a new country minutes after MFA — impossible-travel fires in under 60 seconds. The Context Service decorates it; a new-IP RDP flow and a privilege-escalation chain on the same identity fuse into one incident by graph proximity. L1 and L2 agents investigate; the analyst approves SOAR containment with a blast-radius preview.

≤ 60s	≤ 15m	Correlation	NDR
MTTD	TIER-1 MTTR	UEBA	SOAR	SOC Agents

02 From 4,000 CVEs to the Twelve That Matter

A new critical dependency CVE floods thousands of findings. The graph computes a VulnRisk score per asset — CVSS, EPSS, KEV, reachability, exposure and criticality — and presents the reachability proof. A graph min-cut builds the smallest fix-set that closes the most exposure paths; tickets route to owners and a re-scan verifies the fix.

≥ 90%	≤ 15%	Vuln Mgmt	CNAPP
CRIT+HIGH IN SLA	FP, TOP DECILE	SAST	CSPM	SOAR

03 DPDP & CERT-In — Breach Response on the Clock

A user downloads 5 GB from an S3 bucket DSPM has classified as holding 12M Aadhaar records. DSPM × SIEM fusion auto-escalates a critical data-breach incident; graph traversal returns the regulatory blast radius. The CERT-In six-hour clock starts, templates auto-fill, DPDP notices are drafted, and an evidence package compiles in under ten minutes.

6 hrs	< 10m	DSPM	SIEM

04 The Agentic SOC — Grounded, Cited, Human-Gated

Alert backlog outpaces headcount. The L1 Triage Agent enriches and classifies; the L2 Investigation Agent pivots the graph and proposes containment. Graph RAG keeps it honest — hybrid retrieval, PII redacted pre-LLM, hallucinated citations rejected. The RCA Agent drafts new detections as pull requests. Every write tool is OPA-policy-gated.

− 60%	− 50%	SOC Agents	Graph RAG

Stop stitching dashboards. Start traversing NetGraph — Continuous Exposure Management