Cyderes Cloud Native Analytics Platform

Traditional SIEM/UEBA solutions, whether deployed on-premises or self managed in the cloud, are plagued by challenges around TCO, data management overhead, analyst productivity, and effectiveness of analytics. Cyderes CNAP is a cloud native cybersecurity platform specifically designed to overcome those long standing hurdles in meeting SOC goals and operational metrics. CNAP provides comprehensive threat detection, investigation and workflow along with rich reporting for compliance use cases. CNAP is powered by and built entirely on GCP and Chronicle, Google's security analytics offering.

Architecture

Architecturally, Cyderes CNAP is built on a GCP infrastructure foundation layer for unmatched performance, scale, availability as well as trust and compliance. Additionally, CNAP fully leverages Chronicle's unified security data model, high performance search/ingest APIs, and advanced rules engine (YARA-L). The combination of GCP and Chronicle effectively represent a purpose built security data lake that CNAP content and workflows leverage. All security

telemetry is retained in an instantly accessible (sub-second search latency) state for 12 months by default. For a comprehensive overview of Chronicle's capabilities, see the Chronicle White Paper.

A deep and robust integration between Cyderes and GCP Chronicle foundation tiers ensures transparent expansion and support for future enhancements in Chronicle's data model, APIs, search engine, and rules engine. The technology integration is also supported by a close engineering partnership.

CNAP builds on its GCP and Chronicle foundational architecture with a rich library of pre-built data source connectors and SOC ready content including correlation rules, operational and compliance dashboards, and pre-defined triage workflows. CNAP also provides enhanced management and tracking of Chronicle's data ingestion and forwarding software to increase overall availability, reliability and tracking.

Key Use Cases

- Investigation & Hunting: with sub-second latency, visual anomaly detection
- Advanced Threat Detection: Sigma support and 500+ rules mapped to ATT@CK
- Operational Workflow: case management integration, best practice playbooks
- Compliance Reporting: OOTB coverage of requirements for major industries and mandates
- Optional Add-ons: managed services, managed orchestration, custom content and playbooks

Key Customer Benefits

- Up to 500% TCO advantage over other SIEM solutions
- Automated advanced threat detection
- Improved return on security investment (RoSI)
- Higher analyst productivity metrics (caseload, TTD/TTI/TTR)
- Easy expansion to managed services, orchestration, custom use case development

Delivery Model and Pricing

CNAP is delivered as a true SaaS offering to eliminate the overhead of management, tuning, and upgrades that often consumes half the operational effort in traditional SIEM deployments. With a fixed, predictable pricing model that is decoupled from data volume and usage, Cyderes CNAP incentivizes organizations to collect and analyze ALL their security telemetry. Based on an organization's preference, Cyderes offers alternate models to consume CNAP as a managed service. Base managed services can be tiered up to include orchestration automation as well as custom parser, content and playbook development.