CYDERES EMDR
Enterprise Managed Detection & Response

CYDERES

fishtech group

FEATURES:

Managed 24x7x365 Security Operations Center (Tiers 1-4)

Threat detection and triage for all technologies

Security incident response

Proactive threat hunting

Build playbooks (phishing, malware, lateral movement)

Named technical account manager (TAM)

Endpoint Detection & Response management

Sole EMDR 100% Powered by Google Chronicle with full Cloud Native Analytics Platform Features

Unlimited data ingestion and full 1-year hot retention

Chronicle forwarder 24x7 management and monitoring

Custom Chronicle integrations / parsers

Thinkst Canary Deception Technology Included

Stop chasing alerts. It’s time to shift from reactive monitoring to proactive hunting.

As breaches escalate in size and scope, protection alone is failing. Of course, prevention is still important, but detection and response are top priorities for secure organizations today. Securing big data typically means big costs while using antiquated SIEM technologies that come with very little security analytics. How does an organization gain security maturity with legacy “alert-factory” technology, an industry-wide skill shortage, and limited resources?

CYDERES Enterprise Managed Detection & Response yields the results organizations need—fast, consistent, and highly automated outcomes using custom playbooks. This comprehensive, human-led and machine-driven Security-as-a-Service operation supplies the people, process, and technology they need to manage cybersecurity risks, detect threats, and respond to incidents in real time.

Backed by the revolutionary power of Chronicle, CYDERES EMDR enables organizations to focus on business objectives and delivering stakeholder value instead of worrying about the next inevitable security event. Chronicle is a global security telemetry platform for investigation and threat hunting within an enterprise network. It makes security analytics instant, easy, and cost-effective.

Chronicle is built on core Google infrastructure, and brings unmatched speed and scalability to analyzing massive amounts of security telemetry. As a cloud service, it requires zero customer hardware, maintenance, tuning, or ongoing management.

Key Differentiators to the CYDERES/Chronicle EMDR Solution:

- **Get started faster.** We have the expertise to help including custom parsers, forwarders, and support adding value to your environment in less than 24 hours.
- **Disruptive economics.** Fixed, predictable pricing enables you to focus resources on your business. 10x the performance at 1/10 the cost.
- **Full visibility and response.** Centralize your security operations and response with our 24/7 Chronicle experts.

Focus on enabling your business. Let us handle your threats.

Managed Tanium Comply

TANIUM CYDERES

SOLUTION:

Managed Discover and Core

- Real-time Visibility
- Comprehensive Control
- Rapid Response
- Centralized Logging

Identify vulnerability and compliance exposures within minutes across widely distributed infrastructures.

Tanium Comply conducts vulnerability and compliance assessments against operating systems, applications, and security configurations and policies. It provides the data necessary to help eliminate security exposures, improve overall IT hygiene and simplify preparation for audits.

Leverage our expertise in centralizing your compliance operations with managed modules for patch and vulnerability management.

Patch and Deploy

Quickly and confidently distribute, manage, and report on operating system and application patches across endpoints to reduce risk. Easily update installations and out-of-date software.

Support for Industry-Specific, Security Best Practices or Custom Checks

Tanium Comply supports the Security Content Automation Protocol (SCAP) and can employ any Open Vulnerability and Assessment Language (OVAL)-based content, including custom checks. The Tanium content library updates daily with the most current vulnerability and compliance data.

Alignment with Regulatory and Corporate Requirements

Organizations can use Tanium Comply to help fulfill configuration hardening and vulnerability scanning portions of industry regulatory requirements, including PCI, HIPAA and SOX. The freedom to conduct ad hoc scans also improves adherence to corporate mandates for proactive security assessments.

FISHTECH GROUP

855-404-TECH (8324)
connect@fishtech.group

Email to get started today. ***connect@fishtech.group***

Managed Tanium Threat Response

TANIUM CYDERES

SOLUTION:

Client licenses Tanium Threat Response for detection and response:

Seamless Tanium Stream Integrations into Google Chronicle

CYDERES provides professional services for the lift and shift to the Tanium platform

CYDERES provides Managed 24/7/365 threat-monitoring service

Custom Playbook creation

Defined Response Actions in SOC Operations

UNMETERED Incident Response and Advanced DFIR

CYDERES will also perform:

- Case Tracking
- Document Activity Investigation
- Incident Management Services
- Parameters for escalations will defined and maintained

FISHTECH GROUP

855-404-TECH (8324)
connect@fishtech.group

Leverage CYDERES experts 24/7 to manage detection, investigation and escalation of security alerts within Tanium Threat Response (or other Endpoint Detection and Response products).

CYDERES will monitor alerts generated by Tanium, investigate suspicious activity in order to distinguish between false and true positives, jointly develop playbooks with the client for investigation and response to endpoint events, execute against playbooks for actions like quarantining devices, whitelist and blacklist executables, and make recommendations for additional action or escalation.

CYDERES will work across the Tanium Core, Discover, Threat Response and Enforce console and Chronicle to conduct investigations that expand beyond the scope of endpoint agents. CYDERES will perform case tracking, document activity investigation, and incident management services as well as build workflows that ensure a consistent process is followed when responding to security incidents.

CYDERES Security Operations includes proactive threat hunting: CYDERES resources proactively investigate within the client's Tanium console (e.g. Tanium Core, Discover, Threat Response and Enforce Console) for opportunities for improvement in endpoint architecture, configuration or operations, as well as "hunting" for threats that have not yet tripped detective controls. This includes custom queries within the client's Tanium and Chronicle consoles.

CYDERES takes full ownership and performance of detection and response/ remediation activities using the Tanium Threat Response solution along with carrying out the associated incident response and forensics tasks, after approval is received from Client.

Email to get started today. ***connect@fishtech.group***