Solutions Overview
Data-driven Cybersecurity

Solutions

Advisory Services

ENTERPRISE ARCHITECTURE

- Cloud Strategy & Roadmaps
- Cloud Governance
- Cloud Architecture
- Technology Validation
- Technology Implementation
- Security architecture assessments
- Security operations center assessments
- Security tools assessment
- Penetration testing

DEVOPS + SECURITY AUTOMATION

- Cloud-native Architecture
- Security Automation
- Everything-as-Code Implementation
- DevOps Technology Implementation
- Security Testing & Validation

STRATEGIC STAFFING

- Virtual CISO
- Contract-to-hire
- Technology
- Operations

IDENTITY

- IAM & IGA Workshops
- IAM Domain Gaps
- IAM & IGA Program Advisory
- Strong Authentication Solution Implementation
- PAM Solution Implementation
- IAM-as-a-Service

CYBER RISK + COMPLIANCE

- Information Security Program Review
- Threat Management Program Review
- Security Policy Review & Development
- Business Continuity Management
- GAP & Risk Management Assessments

Technology Services

INTEGRATION

- Optimization services
- Tools assessments
- Tuning
- Optimization & integration partners
  - AWS
  - Microsoft Azure
  - Office 365
  - Google Cloud
  - Palo Alto Networks
  - Check Point
  - Fortinet
  - Netskope
  - VMware
  - Splunk
  - Zscaler
  - Protectwise
  - Cylance
  - Symantec Endpoint
  - SentinelOne
  - McAfee (CASB)
  - Saviynt
  - SecureAuth
  - OKTA

OPTIMIZATION

- Optimization services
- Tools assessments
- Tuning

VALIDATION

- Endpoint
- Firewall
- IDS/IPS

Technology Lab

- POC (Proof of Concept)
- Technology validation
- Reference architecture(s)
- Lab testing services
- Lab-as-a-service
- Performance & load testing
- Security testing & validation

Tech Partners

Value-added reseller for 150+ best-of-breed cybersecurity technology partners

855-404-TECH (8324)

connect@fishtech.group

CYDERES | 24/7 Security-as-a-Service

ENTERPRISE MANAGED DETECTION & RESPONSE

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 Chronicle Backstory

Unlimited data ingestion and full 1-year hot retention

Backstory forwarder 24x7 management and monitoring

Custom Backstory integrations/parsers

Thinkst Canary Deception Technology included

GSOC

Managed 24x7x365 SOC, detecting threats and escalating to your team for remediation

Named customer success manager (CSM)

Proactive threat hunting

Integrated managed Deception Platform (Honeypots – Thinkst Canaries)

Integrated managed Network Traffic Analysis (NTA)

Chronicle Backstory with unlimited data ingestion and one-year unlimited retention

CLOUD GOVERNANCE AS A SERVICE

Our cloud security & DevOps expertise extends your security program beyond your perimeter

- Proactively manage your cloud security risk
- Minimize your attack surface
- Improve your overall cloud security posture

BACKSTORY ESSENTIALS

Chronicle Backstory with unlimited data ingestion and one-year unlimited retention

- Fast start deployment for Chronicle Backstory
- Development of up to four custom parsers for Backstory
- 24x7 Backstory forwarder management and monitoring
- 8x5 Backstory product support

Best effort of security operations services including up to 5 hours per week in your environment in which we detect threats and escalate to your team for remediation

Named customer success manager (CSM)

Included $10k SIRT retainer for additional escalations / operations work as needed

SECURITY INCIDENT RESPONSE TEAM

Security Incident Response Team

Expertise on standby to help with every aspect of a security event

Breach response

Digital forensics

Expertise & guidance beyond just the event to communicate with regulators, law enforcement, your board and/or your clients

Reasonable rates

"Use it, don't lose it." Leverage your unused retainer dollars for vulnerability assessment, tabletop exercises, or any other Fishtech services or CYDERES subscriptions

RED TEAM AS A SERVICE

Red Team Engagements

External Penetration Testing

Internal Penetration Testing

Wireless Security Testing

Web App Penetration Testing

Social Engineering

Physical Security Review

HAYSTAX | Security Analytics Platform

INSIDER THREAT MITIGATION

Real-time threat analysis

Model-first user behavior analytics

An end-to-end SOC platform

PUBLIC SAFETY

Law enforcement / Fire safety

School safety / Event security

Emergency management

ENTERPRISE

Manage your cyber, physical, and insider risks from one platform

VENTURES

PERCH

Threat analytics

FORESITE

Managed security service provider