CONTINUOUS DETECTION. DECISIVE RESPONSE.

Proactive Security Operations Built for Federal-Grade Defense and Modern Threats

As a subsidiary of an Alaska Native Corporation, our purpose is unique. Koniag was incorporated under the 1971 Alaska Native Claims Settlement Act (ANCSA) to steward the land and assets of the Alutiiq people from the Kodiak Island region in perpetuity.

We invest in and operate our business through sustainable financial practices and resource management to be able to support this mission. Our approach to business, relationships, and community is anchored by one of our core values - Planning for the Long Term.

Our Mission

Anchored in federal-grade discipline and world-class talent, we safeguard organizations from evolving adversaries through 24/7 visibility, cutting-edge intelligence, decisive action, and forensic rigor.

We relentlessly monitor, hunt, and neutralize advanced threats — protecting our clients' most valuable assets so they can operate with confidence and resilience.

Core Services

MANAGED DETECTION AND RESPONSE

Proactive Defense. Continuous Visibility. Rapid Response.

Our Managed Detection and Response (MDR) service delivers **24/7 monitoring, threat hunting, technology configurations, and incident response** across your digital ecosystem — endpoints, networks, cloud environments, and identities.

We combine **human expertise, threat intelligence, and automation** to detect and contain attacks in real time, reducing the impact of ransomware, insider threats, and evolving threats to civilization

TECHNOLOGIES

- Microsoft
- Crowdstrike
- Palo Alto
- Google

OUTCOMES

Our MDR service transforms your security posture from reactive to resilient — enabling you to operate with confidence, knowing your environment is continuously monitored, intelligently defended, and immediately recoverable.

MANAGED ENDPOINT DETECTION AND RESPONSE (EDR)

Modern Endpoint Defense. Expertly Managed. Rapidly Responsive.

Our Managed Endpoint Detection and Response (MEDR) service delivers **continuous protection, policy management, and active response** across your endpoint security platforms. We take ownership of **platform management, policy optimization, health monitoring, and alert response**, ensuring every endpoint in your environment is configured, protected, and defended against modern threats.

TECHNOLOGIES

- Crowdstrike Falcon
- SentinelOne
- Microsoft Defender for Endpoint

OUTCOMES

With Managed Endpoint Detection and Response, you gain a fully managed EDR ecosystem that continuously adapts to new threats, eliminates noise, and ensures every endpoint — from workstations to servers — is both visible and defensible. Your organization operates confidently, knowing expert analysts are watching, managing, and responding around the clock.

THREAT HUNTING

Proactive Discovery. Human-Led Precision. Intelligence-Driven Defense.

Our Threat Hunting service delivers **proactive, intelligence-driven operations** that seek out hidden adversaries before they can cause harm.

Rather than waiting for alerts, our hunters continuously **search for indicators of compromise, behavioral anomalies, and stealthy attacker tactics** across endpoints, networks, identities, and cloud environments.

Every hunt is grounded in **current threat intelligence, MITRE ATT&CK** mapping, and **adversary tradecraft analysis** — ensuring that emerging TTPs are identified, validated, and contained before they evolve into incidents.

OUTCOMES

Our Threat Hunting service transforms raw data into actionable defense intelligence. By combining expert analysts, curated intelligence, and advanced analytics, we turn the unknown into the understood — ensuring adversaries have nowhere left to hide.

SIEM ENGINEERING

Precision Ingestion. Framework-Aligned Normalization. Reliable Detection at Scale.

Our SIEM Engineering service ensures your security analytics platform operates with **accuracy, efficiency, and resilience**.

We manage the full lifecycle of **data ingestion, normalization, tuning, and platform optimization** across technologies. Our engineers design, maintain, and optimize your SIEM infrastructure to deliver **high-fidelity, security-relevant telemetry** — enabling meaningful detections and actionable insights without unnecessary noise or data cost.

TECHNOLOGIES

- Microsoft
- Crowdstrike
- Palo Alto
- Google

OUTCOMES

With SIEM Engineering, your organization gains a high-performance, framework-aligned analytics foundation that fuels accurate detection, reduces operational overhead, and ensures your security operations team works with clean, meaningful, and actionable data — not noise.

DETECTION ENGINEERING

Purpose-Built Signatures. Precision Analytics. Continuous Evolution.

Our Detection Engineering service delivers **custom, high-fidelity detection logic** purpose-built to identify adversary behaviors, insider threats, fraud patterns, and anomalous activity across your security stack.

We design, test, and deploy **behavioral signatures and analytic rules** mapped to the **MITRE ATT&CK framework**, ensuring alignment with real-world threat tactics, techniques, and procedures (TTPs).

OUTCOMES

With Detection Engineering, your organization gains a living detection ecosystem — one that continuously adapts to adversary tradecraft, delivers actionable alerts, and strengthens your SOC's ability to respond with speed and confidence.

DFIR BREACH ASSESSMENT (PRE/POST)

Prepare. Respond. Recover. Strengthen.

Our DFIR and Breach Assessment service provides organizations with both **proactive readiness and rapid incident response** to contain, investigate, and recover from cyberattacks.

Whether responding to an active compromise or validating defensive posture before one occurs, our experts deliver **end-to-end breach lifecycle support** — from table top exercises, incident action plan development, forensic acquisition and root-cause analysis to remediation guidance and resilience hardening.

OUTCOMES

With DFIR & Breach Assessment, you gain an always-ready incident response capability — prepared before compromise, decisive during, and stronger after.
Our experts transform chaos into clarity, ensuring your organization can detect, contain, and recover from any incident with confidence.

VULNERABILITY MANAGEMENT

Identify. Prioritize. Remediate. Strengthen.

Our Vulnerability Management service delivers **continuous visibility and risk-based prioritization** across your infrastructure, endpoints, and cloud environments.

We identify exploitable weaknesses, measure their business impact, and guide timely remediation — ensuring your organization stays ahead of adversaries who exploit known and emerging vulnerabilities.

Through **automated scanning, threat intelligence correlation, and contextual risk scoring**, we transform raw findings into actionable insights that drive measurable risk reduction.

TECHNOLOGIES

- Tenable
- Rapid7

OUTCOMES

With Vulnerability Management, your organization gains a living, measurable defense program — one that turns vulnerability data into prioritized, actionable risk decisions and ensures your environment remains hardened against evolving threats.

Connect with Our Experts

Koniag Cyber unites world-class analysts, proven frameworks, and advanced technology to deliver continuous detection and decisive response.

We bridge human expertise with automation to provide 24/7 visibility, rapid containment, and enduring resilience.

info@koniagcyber.com
www.koniagcyber.com