Kraft Kennedy

Managed Security Services

Why Kraft Kennedy?

- Client security incidents are tracked in our proprietary Security Information Event Management (SIEM) tool managed by industry leading security analysts.
- Fast incident remediation and proactive communication in real time.
- A uniquely deep knowledge of IT, with over 30 years of experience.
- Our 24x7x365 security operations center is designed to give you the security capabilities of the largest companies without the high cost.

Kraft Kennedy's security operations center (SOC) monitors, detects, and combats cybersecurity incidents using innovative technology and proven processes. Our team of security analysts and engineers defend networks, servers, endpoints, databases, applications, and websites.

Endpoint Tracking and Modeling

A continuous, unobstructed understanding of every endpoint with rapid identification of compromise.

Vulnerability Management

Scans, configuration and compliance checks, malware detection, web application scanning, and more.

Security Log Management

Automated log search and real-time analysis to scan for threats and conduct quick remediation.

Managed Firewall

Detect possible hacker attacks, protect personal information, and eliminate unwanted sources of network traffic. Firewalls are regularly patched to eliminate security vulnerabilities.

Intrusion Protection

Network protection with superior visibility, embedded security intelligence, automated analysis, and industry-leading threat effectiveness.

Anti-Virus and Anti-Malware

Detection of and defense against viruses, spyware, adware, unauthorized users and devices, Rootkits, ransomware, and other threats for PCs and Macs.

Email Targeted Threat Protection

Protection from malicious URLs, email attachments, internal email threats, social engineering, and impersonation attacks.

Web Filtering Management

The SOC uses DNS to stop threats over all ports and protocols — even direct-to-IP connections—without an impact on performance.

Policy Change Management and Threat Detection

Detect network changes, anomalous end-user behaviors, misconfiguration threats, unauthorized logins, changes to administrative rights, and unauthorized use of wireless connections.

Security Awareness Program

A formal process to employees about security hygiene, corporate policies and procedures for working with their information technology department.