KEYW Secure Operations Center

A Virtualized, Mission Focused Extension of Your Security Team

94% of companies are unaware they've had a breach

71% of attacks succeed in just minutes

400+ days from advanced intrusion to mitigation

— 2012 Verizon Data Breach Report

For sophisticated hackers, stealing credit card information from corporations is a low priority. Their target is an organization's most prized – and often least protected assets: intellectual property, business and legal strategies, merger-and-acquisition plans. These are the corporate "crown jewels" which can be exploited, sabotaged, or sold to the highest bidder. Cyber crime now operates as an organized business community with a range of operating models that allows attackers to rent, lease or buy highly sophisticated attack tools. Their approach is agile in nature and their attack strategies are highly dynamic.

KEYW has created the KEYW Secure Operations Center (KSOC), providing large enterprises with the ability to achieve equal agility in their cyber operations and security posture. The KSOC is a virtualized collection of mission-focused personnel, capabilities and technologies optimized to augment enterprise security teams and processes. Together, we solve the toughest security challenges.

Three New Services from KEYW Secure Operations Center

The KSOC goes beyond the boundaries of traditional SOC's by providing a fully-integrated cyber security ecosystem of experts, technologies, and analytics required to find, fix, and finish today's cyber attacks. The KSOC offers a variety of services, ranging from tools to help you do it yourself to complete outsourcing. Expert personnel in the KSOC are available to plan a proactive defense strategy, intercept threats as they emerge, or provide a systematic approach to identifying and eradicating malicious code or intrusions.

Three new services offered by the KSOC can help strengthen your organization's cyber preparedness:

KSOC Cyber Analytics Assessment

Actionable Approach to Security Intelligence

The best defense against cyber attacks is a proactive strategy designed to provide deep and actionable visibility across your landscape. Unlike services that are focused on assessing your baseline or compliance posture, the Cyber Analytics Assessment (CAA) looks at the state of your cyber defenses and your current ability to respond to an increasingly aggressive landscape of cyber attackers. The CAA looks across security and IT infrastructure – and recommends ways to improve your cyber awareness through better analytics, reports and dashboards.

This service allows organizations to gain efficiencies by reducing the personnel and number of they are involved in manual security analysis every year. In the case of an IT team with 15 employees, for example, it is likely that each employee spends 12 hours a week reviewing logs, correlating security data for reports, or executing ad-hoc queries. After a CAA, that team can identify an analytics strategy that reduces time spent on manual processes by $400,000 annually[1], with the added benefit of freeing those resources to be redeployed on higher value initiatives, while delivering a more consistent, actionable risk management program.

The assessment starts with an onsite review of all security policies, tools and IT/security infrastructure sources which currently feed your security monitoring infrastructure. It maps and analyzes both the policies and tools currently in use, examines the network environment, and analyzes current penetration and vulnerability testing practices. The output is a Cyber Analytics Gap Analysis and Recommendations report, as well as proposed set of custom Cyber Analytics Dashboards and Reports.

ASSESS

[1]Average salary $90,000 USD, working 251 days annually

KSOC Incident Response Service

Expert assistance when an attack is suspected

It is the rarest of organizations that are "out of reach" relative to today's cyber attacks and breaches. Even those with seemingly impenetrable security understand thousands of attempts are made against them every day, and they must be prepared with a plan when faced with a successful attack. In incident response, time is both money and reputation.

Should an enterprise experience or suspect a breach in their security, a quick and thorough response is critical. The team of experts at the KEYW Security Operations Center will help you respond to an attack immediately, beginning with a forensics process that will discover and diagnose the true impact of the compromise. Through a phased program of expert forensic analysis, mitigation and recovery, KSOC will apply advanced analytic tools to help you understand the event from every dimension, and will create a comprehensive picture of what happened. We also help contain and eradicate malicious attackers that may have intruded your organization.

KSOC Incident Response delivers the following services:

- Reconnaissance and analysis
- Containment
- Eradication and recovery

Hands-On Cyber Training

Offense, defense and programming courses that go way beyond theory

Cyber terrorists, organized criminals and political actors focus tremendous effort on finding the weak links in Enterprises of every size. When successful, these weak links provide access to valuable assets or back doors to even bigger targets, including Critical Infrastructure and Government networks. Your combat methods must be as sophisticated and relentless as their cyber attack methods or you will be the weakest link.

KEYW offers an in-depth Cyber Security curriculum based on real-world expertise defending the largest Agencies and Enterprises in the world. KEYW Cyber instructors assess, train and certify hundreds of responsible security experts each month in state-of-the-art classified and unclassified classrooms and customer facilities.

Specific courses include:

- Offensive methodology and analysis
- Adversarial offensive training
- Cyber leader course
- Tactical digital forensics
- Tool & capability development

To learn more, visit: http://training.keywcorp.com

The KEYW Secure Operations Center brings together the advanced tools of Sensage and the experienced personnel and services of KEYW to solve large enterprises' toughest problems across the spectrum of cyber awareness and defense:

- Services to proactively look for vulnerabilities and threats before they happen;
- Solutions to maintain optimal cyber awareness and defense as threats are attempted; and
- Action plans to eradicate or contain threats in the event defenses are breached.

SENSAGE
a KEYW company

Sensage, Inc.
1400 Bridge Pkwy.
Suite 202
Redwood City
CA 94065
www.sensage.com