Enterprise Incident Response Retainer

Enterprise Protection Services Summary

Kivu incident response customers can allocate unused breach response hours to proactive security services in order to improve their security posture. We provide a full range of Enterprise Protection Services (EPS), helping you proactively identify and address security risks affecting critical business functions and data.

No matter the size or risk posture of your organization, our EPS offering helps you minimize the risk of cyber security breaches by equipping your organization with the insight and tools to protect its operations.

PENETRATION TESTING

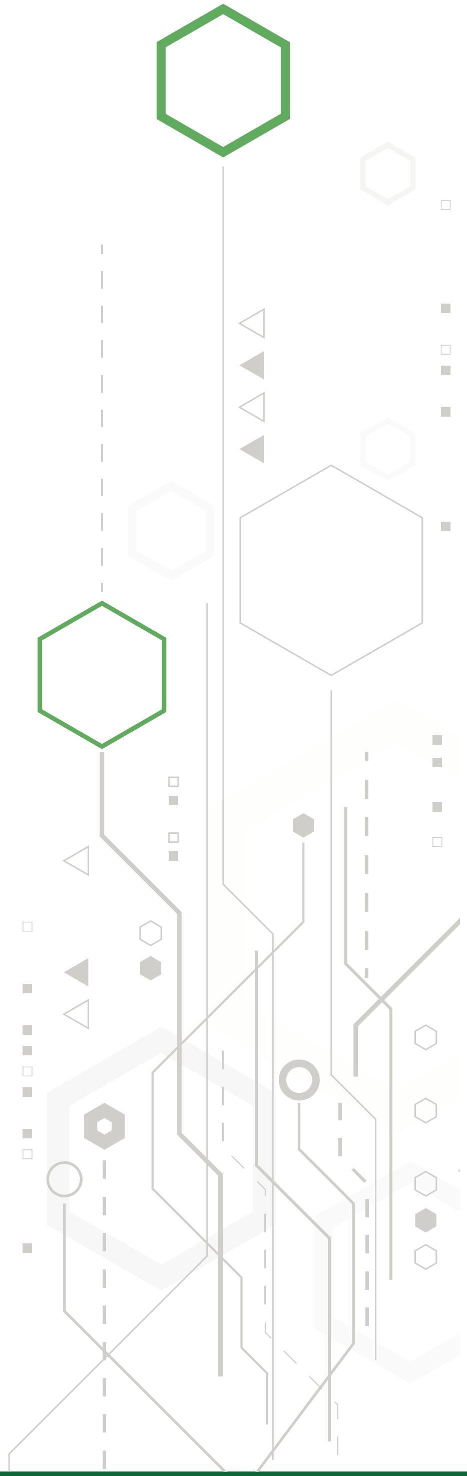
A simulated cyber-attack on your network using multiple attack vectors, including social engineering, to ascertain the security of your digital operating systems.

BUSINESS ANALYSIS & STRATEGY

Thorough assessments of various aspects of your organization's security policies, with focus on how they can be optimized to support business objectives.

PROGRAM ASSESSMENT & COMPLIANCE

In-depth reviews of the security configurations for your public cloud infrastructure, including data security compliance checks.



PENETRATION TESTING

Internal/External Penetration Testing

Emulates a real-world attack on your network. The objective of this assessment is to breach your organization's security measures and gain access to digital information and assets.

Tactics usually include:

- Open source reconnaissance against your organization
- Full port scan covering all TCP ports and the top known vulnerable UDP ports
- Full vulnerability scan of the targets
- Manual and automated exploit attempts
- Password attacks
- Social engineering (e.g. phishing) attacks

Web Application Testing

An in-depth test of both the unauthenticated and authenticated areas within your website. Kivu will test all aspects of the Open Web Application Security Project (OWASP) top critical security flaws and a variety of other potential vulnerabilities based on security best practice.

Areas tested include:

- Sensitive data exposure
- Website mapping
- Directory enumeration
- Injection flaws on all input fields
- Directory traversal
- Malicious file uploading
- Remote code execution
- Password attacks and testing for vulnerabilities in authentication code
- Session attacks: hijacking, spoofing, man-in-the-middle and fixation
- Broken authentication

Social Engineering & Phishing Test

Includes popular tactics for email spoofing and phishing campaigns, as well as phone-based testing. We track employee responses to ascertain the level of awareness among staff and identify areas for training and improvement.

Vulnerability Scanning & Management

An automated process conducted by Kivu staff that identifies security gaps on a network, run on a regular basis. The scans detect and classify system weaknesses in computers, networks and other communications devices. You will receive a comprehensive risk report to enable you to address vulnerabilities.

Tabletop Exercises & Simulations

Utilize penetration testers and defender consultants. The former attempt to circumvent security controls and gain unauthorized access to your systems. The latter team will then work with internal stakeholders of your choosing to determine their ability to either detect, deflect and/or deter the attack.

Physical Security Testing

An assessment of the physical security of your organization's premise. Kivu will attempt to gain access to your facility by identifying weaknesses in your security practices and/or using social engineering techniques. Once Kivu has gained access to your facility, we will attempt to gather sensitive information and gain access to sensitive areas as well as your network.

BUSINESS ANALYSIS & STRATEGY

Mergers & Acquisitions Analysis

A formal risk assessment that evaluates the overall security posture of a company including the threats to the organization, the network vulnerabilities and the security controls in place to protect the network in order to help drive strategic decisions at leadership level.

Internet of Things (IoT) Assessments

Evaluates the resilience of your organization's IoT devices and infrastructure against common attacks using the OWASP IoT Framework Assessment methodology. Assessments can target edge and gateway devices, cloud infrastructure and mobile applications.

Policy/Procedure Review and Creation

Designed to review existing, and assist in the creation of comprehensive, security policies.

Common policies include:

- Incident Response
- Ransomware Response Plan
- Access Control Policy
- Acceptable Use
- Disaster Recovery Plan
- Password Policy

Virtual CISO Service

Makes senior specialists available to your organization for security expertise and guidance. Kivu's subject matter experts have decades of experience in building and managing information security programs that work with your business objectives and result in measurable improvements to your organization's security posture.

PROGRAM ASSESSMENT & COMPLIANCE

Cloud Configuration Benchmark Assessment

An essential review that provides assurance over your organization’s security configurations for your public cloud infrastructure. Kivu will review password policies and procedures, advise on multifactor authentication, and ensure that your notifications, logging, rules, admin controls and alerts are properly set up. Special attention is paid to permissions, to ensure secure and controlled access to your environment.

Ransomware Risk Assessment

Builds on Kivu’s learnings from over 700 ransomware cases. We analyze your environment’s configuration and policies, evaluating exposed ports, traffic logging, remote access, patching, endpoint monitoring, as well as access and permission rules. Kivu will also review the tools that can prevent or mitigate attacks, such as back-ups, segregation, data governance, incident response plans and password policies.

Experts in Their Fields

Kivu’s EPS team consists of seasoned cyber security professionals with backgrounds in federal government and private organizations of all sizes. Our consultants bring extensive depth of experience and knowledge that ranges from general IT expertise to building and managing security programs for Fortune 100 companies.

SEAMLESS SECURITY COVERAGE WITH KIVU’S MANAGED SECURITY SERVICES

Kivu also offers Managed Security Services which seamlessly integrate with our EPS offering, providing 24x7x365 endpoint monitoring and response as well as other continuous security services for extra peace of mind.

Speak to your Kivu contact or email **managedservices@kivuconsulting.com** for more information.

About Kivu

Kivu is a global technology and cyber security services firm that offers a full suite of pre- and post-breach services, specializing in the forensic response to data breaches and proactive IT security compliance. Headquartered in the U.S. with offices worldwide, Kivu is a pre-approved cyber forensics partner for leading North American and EMEA insurance carriers.

KIVUCONSULTING.COM

CONTACT US

Get in touch with our team to learn more about our range of enterprise protection and pre-breach services and how they can be tailored to your needs. Speak to your Kivu contact or email us **info@kivuconsulting.com.**