OccamSec

With a focus on operational resilience, OccamSec fills a critical gap in business infrastructure with information security solutions so you can thrive with confidence.

Security isn't a technical matter, it's a business matter.

Business disruption, data breach responses, remediation plans—organizations often deal with the impact of complex and advanced threats from third parties that commonly go undetected. Currently, more than 60% of ransomware attacks target small and medium-sized enterprises, i.e., your vendors, that present a more vulnerable and expedient access point to your business.

Reported attacks on SMEs increased by 41% in 2019.

RADIUS

Radius is our vendor risk management solution that removes the blinders so you can ensure the privacy and security of your data.

Safer

Integrated threat intelligence provides a holistic view to inform vendor risk level.

Smarter

Collaboration, compliance, and industry standards ensure efficiency.

Stronger

In-depth solution helps to prevent, adapt, and recover from operational disruptions.

Who We Are

We are information security experts with extensive experience in security operations and program implementation. What does that mean? Well, we've been in your shoes and know firsthand the critical issues you face and how they impact the business. This also means we offer real solutions to help you protect what matters most.

We've breached some of the largest organizations in the world, penetrating every possible point to cause maximum damage. Think of us as the good guys, pretending to be the bad guys, working to strengthen your organization's risk posture against the increasing vulnerabilities of third-party access to your data.

Think Like a Hacker. Protect Like a Boss.

What We Do

No endless cycles of increasing costs, useless features, and long-term headaches. We've grown by actually offering value to our clients.

Penetration Testing

Determine potential impact of an attack on critical assets and operations. Provide a detailed analysis, remediation plan, and testing post threat.

Red Teaming

Simulated advanced attacks across social, technical, and physical areas assess the effectiveness of your security program from detection to response.

Purple Teaming

Response assessment using simulated but realistic attacks designed to test current security controls, identify gaps, and develop fixes.

Incident Response

A time-sensitive technical campaign that poses operational challenges to an organization supported by an unparalleled understanding of business impact.

Wargaming

Training for all levels of your organization using simulated attacks based on real-life experiences to enhance management and response capabilities.

Risk and Compliance

Prepare for and meet various industry compliance standards including PCI, CSA, ISO, NIST, and others.

Countermeasures

Used within your environment to increase detection, reduce the likelihood of a successful attack, and enable faster corrective action.

Threat-Hunting

Actively pursue threats and signs of compromise within your environment using technology and an attacker's perspective.

Security Consulting

With years of operational experience, consulting ranges from program development to architecture design and review to intelligence fusion and analysis.