Cyber Fraud Security
Combating Deceptive Cyber Practices

As business process automation grows, cybercrime expands alongside it, so organizations must remain wary of cyber fraud. The COVID-19 pandemic has also led fraudsters to exploit the increased usage of virtual environments.

In an ever-evolving threat landscape, enterprise networks continue to grow more complex as they cloud capabilities, mobile devices, IoT/OT and more. Enterprise fraud security programs must broaden their threat visibility to keep pace and ensure that their people, processes and technology are capable of detecting, protecting and responding to security threats.

Optiv’s Cyber Fraud Strategy is designed to help you face these challenges and support the reduction of fraud risk. Through a comprehensive evaluation of your organization’s capability to identify threats and vulnerabilities, we simultaneously support the confidentiality, availability and integrity of your critical business operations and data.

Our Solution
The Optiv Cyber Fraud Strategy is based on Optiv’s Cyber Fraud Kill Chain and uses a multi-layer strategy. First, we look at the adversary’s tactics, techniques, and procedures (TTPs), then we determine how to protect, detect and respond to these threats through enhanced governance, procedures and technology.

Optiv’s Cyber Fraud Kill Chain

**Reconnaissance**
Gather information on users, credentials and target environment for future operations.

**Circumvent Controls**
Bypass security tooling to access targeted accounts and victim networks.

**Access**
Adversary will gain access to the environment and laterally move to access targeted applications.

**Execution**
Perform exfiltration or extortion activities, establish persistence, gain additional access for broader operations.

Cyber crime is predicted to grow 15% year over year, reaching $10.5 Trillion annually by 2025. That’s $11.4M per minute.

Source: Cybersecurityventures.com | Hackerpocalypse Cybercrime Report 2016
The Optiv Advantage

Our experts will assist your team by developing a comprehensive plan that enables enterprise-wide security risk reduction aligned with industry-leading practices.

Cyber Fraud Kill Chain Process Overview

The Optiv Cyber Fraud Framework includes a phased approach that enables Optiv’s subject matter experts to conduct a comprehensive analysis of your organization’s cyber fraud strategy. The framework aligns the severity and the probability of a cyber fraud attack against your organization to develop a customized, in-depth, overall strategy to improve your organization’s security posture.

Our approach includes:

- Identifying the adversary, environment and the specific TTPs used
- Establishing governance documentation aligned with managerial oversight to protect, detect and respond to cyber fraud events and incidents
- Creating processes in compliance with applied governance to implement guidance and regulation for daily operations
- Integrating tools and technology to detect and defeat adversaries within the environment
- Continuous improvement to adapt to the changing threat landscape and evolving TTPs, ensuring proactive risk reduction against cyber fraud attacks

Secure your security™

Optiv is a security solutions integrator – a “one-stop” trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, cyber operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are leading a completely new approach to cybersecurity that enables clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.

©2021 Optiv Security Inc. All Rights Reserved. Optiv is a registered trademark of Optiv Inc.