End-to-End Detection and Response

Enhance Operational Effectiveness: Optiv + CrowdStrike

Providing effective detection and response requires extensive training and increased visibility across an entire organization. Many organizations struggle with maintaining a strong security posture due to a lack of security technology expertise and resources. This inability to effectively deliver ongoing operational support limits an organization’s ability to prevent, detect and respond to today's challenging security threats.

Optiv and CrowdStrike have revolutionized cybersecurity. By combining CrowdStrike, a market leader in endpoint detection and response and Optiv, an industry leader in managed detection and response we provide clients with a holistic cybersecurity solution that extends beyond the endpoint. Together, we deliver the detection, investigation and response to threats as well as isolate and contain affected security incidents. Our partnership provides clients with a fully managed security solution that maximizes their technology investment.

Why Clients Choose Optiv for CrowdStrike

- 7+ Years of dedicated partnership
- Platinum level partner
- Dedicated and certified CrowdStrike experts
- #1 Seller of CrowdStrike products
- Optiv awarded CrowdStrike Solution Partner of the Year in 2019
- 6 Global Delivery Centers
- 300 Full-Time Security Practitioners
- 80+ Threat Management Analysts
- 350+ Industry and Vendor certifications
- 1,000+ Clients Served
- 24x7x365
- 50B Events Managed Annually
- 250k Cases Managed Annually
- 20k Security Incidents Managed Annually

**How Optiv Delivers Threat Management**

**SECURITY MONITORING AND THREAT DETECTION**
Optiv’s MDR/XDR solution augments your CrowdStrike Falcon Complete’s endpoint detection capabilities by continuously monitoring alerts from all data feeds across your security platform and shortening your response time.

**TECHNOLOGY MANAGEMENT**
Optiv creates a direct connection to your network and devices to provide hands on device management. While also providing the management and maintenance of your CrowdStrike devices and any additional tools within your security program.

**CROWDSTRIKE’S FALCON ENDPOINT PROTECTION PLATFORM**
Optiv’s detection and response team works with clients for response planning, communications, analysis of detected threats, mitigation recommendations and improvements to strengthen your security posture. This is provided as a multi-instance solution leveraging CrowdStrike’s endpoint protection platform and services.
END TO END MANAGED DETECTION AND RESPONSE
Effective Detection, Rapid Response, Containment and Remediation of Security Threats

TOGETHER

CROWDSTRIKE FALCON COMPLETE Endpoint
• Client Onboarding to the Falcon Platform
• Falcon Platform Management
• Endpoint Alert and Policy Tuning
• Endpoint Security Monitoring
• Endpoint Threat Hunting on Falcon Platform
• Investigation Support on Falcon Platform
• Endpoint Isolation and/or Containment
• Eliminate Persistence Endpoint
• Removal of Endpoint Artifacts for Remediation

OPTIV MDR Integrated MDR Solution Across Client Technology Stack (SIEM, Endpoint, Network, Cloud and other Log Sources)
• Client Onboarding and Management of Optiv ThreatDNA™ Platform
• Data Driven Client Success Management and Reporting
• Management and Engineering support of client-side technologies such as SIEM, Network, Endpoint, VM, IDM and more
• Alert and Policy Tuning
• Threat Hunting
• Log/Alert/Event Data Ingestion, Integration and Retention
• Alert Enrichment, Correlation and Prioritization
• Expanded Situational Awareness and Increased Visibility
• Customized Use Cases based on entire client technology stack for automated response and remediation
• Integrated Intelligence

WHAT’S NEXT?
To get started, ask your local Optiv representative how Optiv and CrowdStrike can help you optimize your security program and secure your endpoints. Optiv and CrowdStrike can help you strengthen and optimize your program.

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, security operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more costefficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are modernizing cybersecurity to enable 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.

©2020 Optiv Security Inc. All Rights Reserved.