Service Brief

Security Operations: Digital Risk Protection Management

Enhance threat visibility beyond your perimeter.

Identifying when and how your organization may be attacked requires going beyond the perimeter. You need a complete, holistic view of your digital footprint. Most organizations don’t have the capabilities and skills needed to conduct threat hunting and analyze intelligence in order to detect and respond to potential attacks. This inability to intercept and remediate information available on the clear, deep and dark web threatens to damage brand reputation and business outcomes.

Organizations need an efficient and tailored threat intelligence gathering process, resulting in actionable information that can be used quickly and easily to provide an improved security posture.

How Do We Do It?

HOLISTIC
A security-first perspective with a holistic approach to infrastructure and programs that improve overall security posture.

COMPREHENSIVE
Methodologies that include program-level root-cause analysis and remediation guidance, going beyond the compliance check-box.

FLEXIBLE
A tailored, adaptive threat management program built to fit your business and industry needs.

Digital Risk Protection Workflow

Client  Optiv

- Asset Register
- Request Remediation
- Resolve
- Request Remediation
- Resolve
- Remediation Actions Completed
- Escalate
- Investigate Alerts
- Monitor Assets
Expand your security program capabilities “beyond the perimeter” through access to investigative resources to collect, analyze and correlate threat intelligence in order to better identify cybersecurity threats.

How We Do It Better

- Certified experts drive operations, shape policy and lead response efforts for our clients, leveraging threat intelligence from Optiv’s gTIC (Global Threat Intelligence Center) and Malware Analysis and Countermeasures (MAC) team.
- Optiv manages the technology, allowing our clients to spend their time on what matters instead of installing tools.
- Optiv provides Tier 1 and Tier 2 resources, freeing up the client to focus on more pressing issues instead of worrying about staffing or lots of noisy alerts.
- Optiv can provide full-function remediation services with client permission.
- When Optiv manages or co-manages a client’s SIEM, we can also provide a full case management integration through the Client Portal (MSS) or Case Management system (AFC).

The Optiv Advantage

The Optiv Advantage: Optiv helps businesses in every industry connect information security policies, procedures and practices with business goals. Our security leadership experts, backed by our team of consultants, can provide the experience you need to take your program to the next level.

EXPERT MINDS
Optiv’s security professionals are dedicated to helping you achieve results and realize value. Our team of 1,000+ highly skilled client managers and security practitioners work hard to deliver superior results and cutting-edge research to solve your complex, real-world security problems.

LEADING BEST PRACTICES
Our knowledge of leading best practices helps Optiv formulate security recommendations tailored to meet your specific business objectives.

CLIENT-FIRST CULTURE
Optiv’s passion for security and our commitment to quality results means we focus on the right solutions to meet your specific needs.

PROVEN METHODOLOGIES
Optiv has developed proven methodologies to help ensure superior outcomes for your projects and programs.