Next-Gen SecOps

Use a Proven Methodology to Plan, Build and Run Your Next-Gen Security Operations

Like many cyber security leaders, you have invested substantially over the years (or will invest) in advanced "next-gen" technologies to improve prevention, detection and response capabilities. But how can you make it all work together and find skilled talent in the midst of an industry talent shortage? You are also likely struggling from alert fatigue, prioritizing incidents and following written workflows that are too complex. The consequences are platforms in siloes, low staff morale, high risk exposure and an inability to measure your progress.

62%

percent of enterprise security decision makers report not having enough security staff, while

65%

*percent state that finding employees with the right skills is a challenge.**

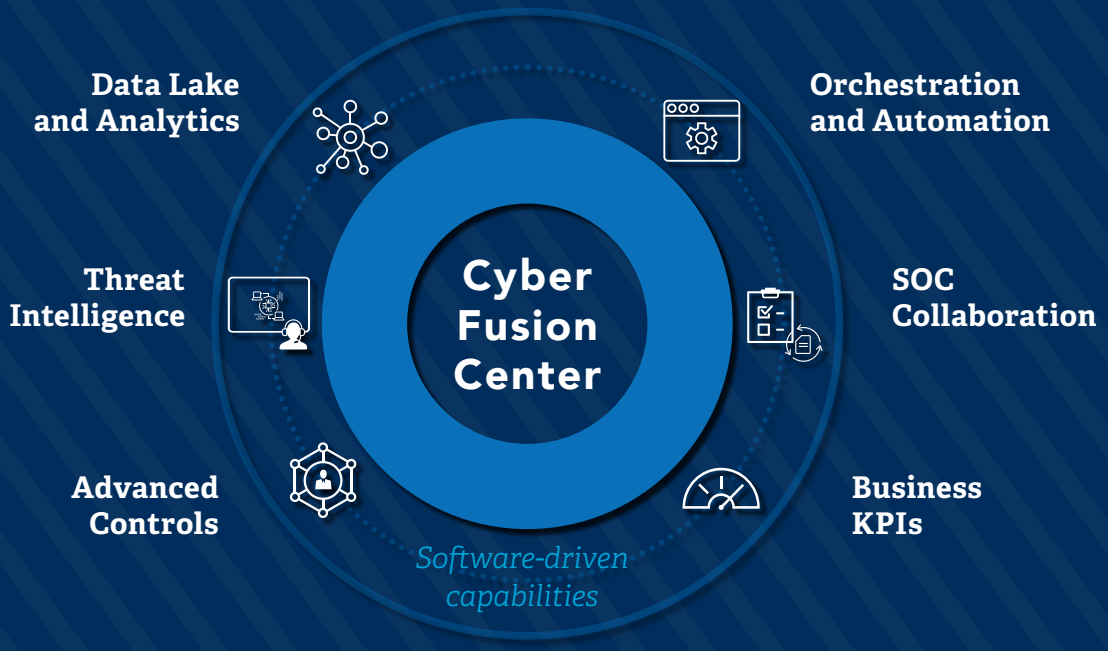
* Breakout Vendors: Security Administration and Orchestration (SAO) report, Forrester Research, Inc., April 2017

SecOps Challenges

- Evolving Attacker Techniques
- Rapid Event Growth
- Integrating Disparate Technologies
- Unable to Find Talent
- Efficient SOC Delivery and Prioritiaztion

Putting Everything Together

A highly collaborative, effective and efficient security operation shouldn't be out of reach. It takes proper planning and expertise to integrate your disparate systems and accurately prioritize threat tasks. In addition, your platforms should be tuned in real-time to respond to the changing threat landscape by using advanced automation and analytics as a foundation.



Operationalize Your Security Program

Your advanced security controls should be part of an integrated program that covers detection, orchestration, automation, analytics, incident response, measurement and reporting.

Next-Gen SOC Design

Optiv has the depth of experience across security strategy, process development and security technology partnerships to operationalize your security program.

OPTIV

Enable Next-Gen SecOps With Optiv's Flexible and Customizable Capabilities

How We Do It

Workshop/Summit

Initial workshop/summit to review your existing environment and security stack to find opportunities to leverage existing tools.

Governance and Progressive Maturity Modeling

Apply proprietary governance and maturity models designed to measure progress and identify focus areas for improvement.

KPI Definitions and Reporting

Definition of key metrics and KPIs that align with your business to drive flexible reporting.

Next-Gen SOC Blueprint

Proven process for SOC plan, build and run phases that has been validated in large enterprise environments.

Use Cases, Playbooks and Process Workflows

Proprietary use case and IP catalog to build runbooks, a training methodology, hunting catalogs, automation and orchestration playbooks, and analytical models.

Talent Enablement

Proven methodology for mining, vetting, hiring and enabling role matching with top-notch cyber security talent.

Platform Integration, Configuration and Management

Integrate advanced controls and applications including orchestration and automation platforms within your existing infrastructure (including VMWare or AWS environments).

Platform Licensing and Connectivity

Ability to configure network connectivity, handle licensing and configure a platform environment (including LDAP, Active Directory setup, email setup, code repository, 2FA, SSL, etc.).

Threat Intelligence Integration

Achieve efficiency, human intelligence amplification, proactive protection and decision advantage.

OPTIV

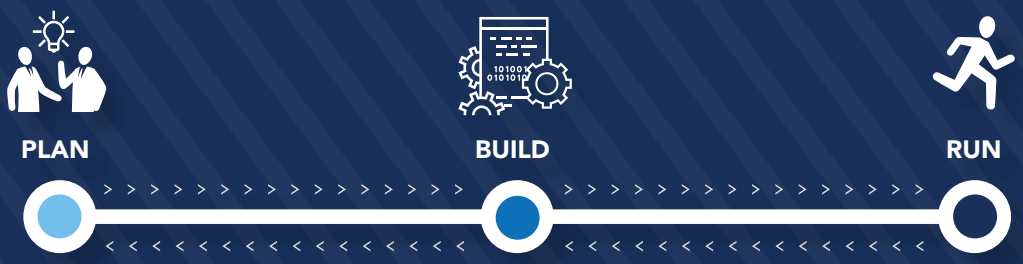
Key Outcomes Across Security Metrics

Optiv helps drive improvements across key metrics including:

- √ Higher return on overall technology investment
- √ Increased volume of incidents handled
- √ Faster mean time to resolution
- √ Improved average time between detection and response
- √ Faster time to ticket acknowledgment
- √ Improved time between initial alert and true positive/false positive determination
- √ Lower ratio of false positives
- √ Overall SLA improvements
- √ Reduced likelihood or impact of a successful cyber attack
- √ Reduction in actualized threats
- √ Reduced headcount for platform management and threat monitoring

A Solution for Every Aspect of Next-Gen SecOps

You require a partner with experience across strategy, process development and security technology. Only Optiv offers the required depth across these areas.



Next-Gen SOC Architecture

- Maturity model assessment and plan
- Runbooks, training methodology, catalogs and use cases
- KPI development and analytical models
- Comprehensive product evaluations

Custom Implementation

- Automation script development
- Data lake, analytics and machine learning
- Threat intelligence fusion
- Chat ops

Global SOC Enablement

- Next-gen platform management
- Orchestration and automation
- Incident response and remediation
- Threat hunting
- Global and local talent pools
- Reporting and measurement

OPTIV

Optiv is a market-leading provider of end-to-end cyber security solutions. We help clients plan, build and run successful cyber security programs that achieve business objectives through our depth and breadth of cyber security offerings, extensive capabilities and proven expertise in cyber security strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers. For more information, visit www.optiv.com or follow us at www.twitter.com/optiv, www.facebook.com/optivinc and www.linkedin.com/company/optiv-inc.

7.17 | F1.2