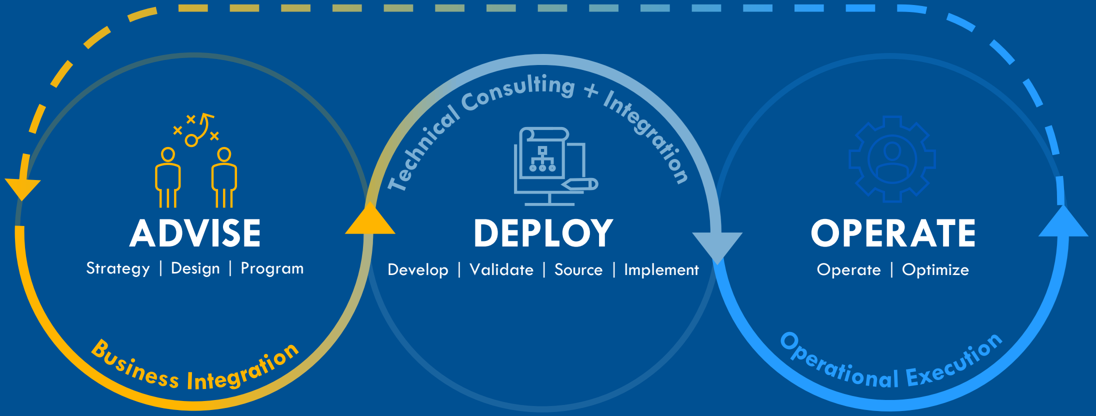
Security Operations

MEDR with Microsoft Defender for Endpoint For Customers

OPTIV

There For You Every Step of the Way

Continuous Security Solutions Support


ADVISE
Strategy | Design | Program
Business Integration
Technical Consulting + Integration
DEPLOY
Develop | Validate | Source | Implement
OPERATE
Operate | Optimize
Operational Execution

Applications: App Development App Operations/Security

Data: Data Governance Data Security Data Analytics

Identity: Identity Governance User Lifecycle Mgmt Digital Access Mgmt CIAM

Infrastructure: IoT OT/ICS Cloud Security Endpoint Security Network Security

Offensive Security: Attacker Simulation Assessments OEM Security Readiness

Operations: Threat Detection & Response Threat Intel Change Management O&A Analytics Incident Response Insider Threat & Fraud Detection

Privacy: Privacy Program Development

Physical Security: Material Threats Human Threats Resilience

Risk: Program Development Compliance

OPTIV

Optiv Security Operations Centers

Operational Integration

OPERATE

Operate | Optimize

Operational Execution

6	24/7/365	50B
Global Delivery Centers	Round the Clock Coverage Worldwide	Events Managed Annually

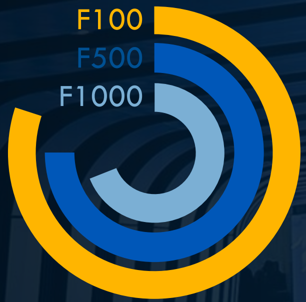
Clients Across All Industries

100	110	85	150
Healthcare	Education	Retail, Hospitality and Travel	Financial
100	60	90	
Tech, Media and Telecom	Government	Manufacturing	

Optiv

Who We Serve

7,000+ clients with 790,000+ hours delivered



80% of Fortune 100

75% of Fortune 500

69% of Fortune 1000

570+ Educational Institutions

830+ Government Agencies and Departments

Fortune 500 Industry Client Share

64% Healthcare

78% Retail, Hospitality and Travel

81% Financial Services and Insurance

83% Utilities and Energy

80% Media and Telecommunications

69% Professional Services

68% Manufacturing

OPTIV

Common Challenges

Time To Compromise Reduced

Most attackers can compromise an organization within minutes of an attack.

Detecting And Isolating Threats Quickly

Use of threat data to lock down other infected machines needs to happen faster than you can react.

Limited Access To Threat Analysts And Intelligence

Today's enterprise requires access to threat experts to assess suspicious samples and respond quickly.

Managing And Responding To Incidents

Most security operations teams lack a sophisticated incident response capability.

OPTIV

Microsoft Defender for Endpoint

The Optiv Approach - Delivering Actionable Findings

Technical Project Manager

Dedicated Technical Project Manager throughout service integration

Certified Experts

Certified engineers drive operations, shape policy and lead response efforts for our clients leveraging threat intelligence from Optiv's gTIC (Global Threat Intelligence Center).

Client Success Manager

Designated Client Success Manager advocates for the client to ensure maximum value is being derived from Optiv services.

Future-proof Planning

Develop a strategy

OPTIV

Introducing Optiv & Microsoft Defender for Endpoint

Provides clients with collaborative service components to ensure preventative and ongoing real-time operational measures

Change Management

Implements changes to configuration and security policies.

Security Alert Monitoring

Provides monitoring, alerting and reporting of security events.

Incident Management

Delivers device health and performance monitoring, alerting and reporting.

Platform Management

Maintains software currency.

Solution: Managed Endpoint Detection & Response Windows Defender For Endpoint

OFFERS REAL-TIME PROTECTION ACROSS ALL ENDPOINTS

- Prevents known and unknown threats in real time.
- Ability to stop an attack before it becomes a breach
- Allows organizations to resume regular business activity, faster
- Effective threat hunting in real time, not months after

EXPERTLY MONITORS CLIENT ENDPOINTS 24/7/365

- Notifies clients if a security breach is detected
- Fast and accurate response to security incidents
- Functions as an extension of client's security team

COST EFFECTIVE SOLUTION AND PREDICTABLE PRICING

- 24/7/365 threat monitoring and response by Optiv expert SOC at an affordable price point compared to hiring internal resources.
- Logs endpoint activity and retains logs
- Simple and easy to understand pricing model with flexible payment options (monthly or annual).

Service Deliverables

+

FREQUENCY

–

Threat Intelligence Reports

Daily

Client Status Report

Weekly

Executive Summary Report

Monthly

Quarterly Business Review

Quarterly

OPTIV

Service Components

Detection and Response

Optiv's Detection and Response team provides quick and detailed analysis on events

- Alert Ingestion
- Event Analysis
- Malware Analysis

Incident Management

Events containing suspicious or potentially malicious activity that could impact the client are escalated to the client for further investigation

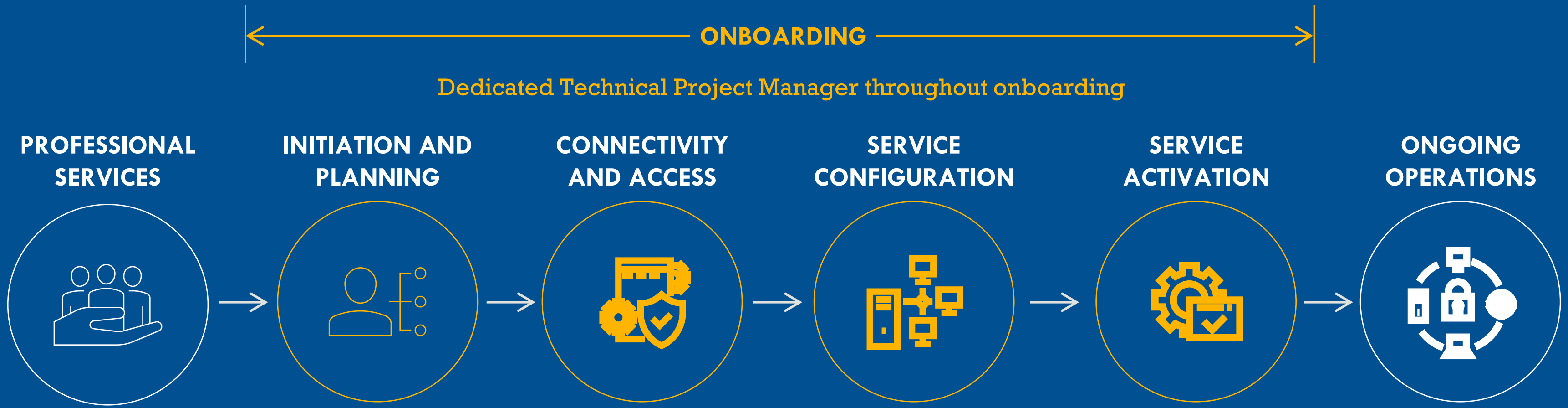
- Incident Escalation
- Remediation Support
- Host Containment
- Incident Closure

Console Management

Optiv provides support for the console, policies, and sensors covered by the Vendor product

- Reputation Management
- Sensor Upgrades
- Onboarding

Security Operations Service Integration Process



ONBOARDING

Dedicated Technical Project Manager throughout onboarding

PROFESSIONAL SERVICES

- Maturity checks
- SOC assessment
- Tool rationalization

INITIATION AND PLANNING

- Welcome packet
- Kickoff calls
- Client workbook

CONNECTIVITY AND ACCESS

- Optiv SOC portal setup
- Network connectivity and logical access
- Validation and confirmation
- Optiv Cybersecurity Education portal setup

SERVICE CONFIGURATION

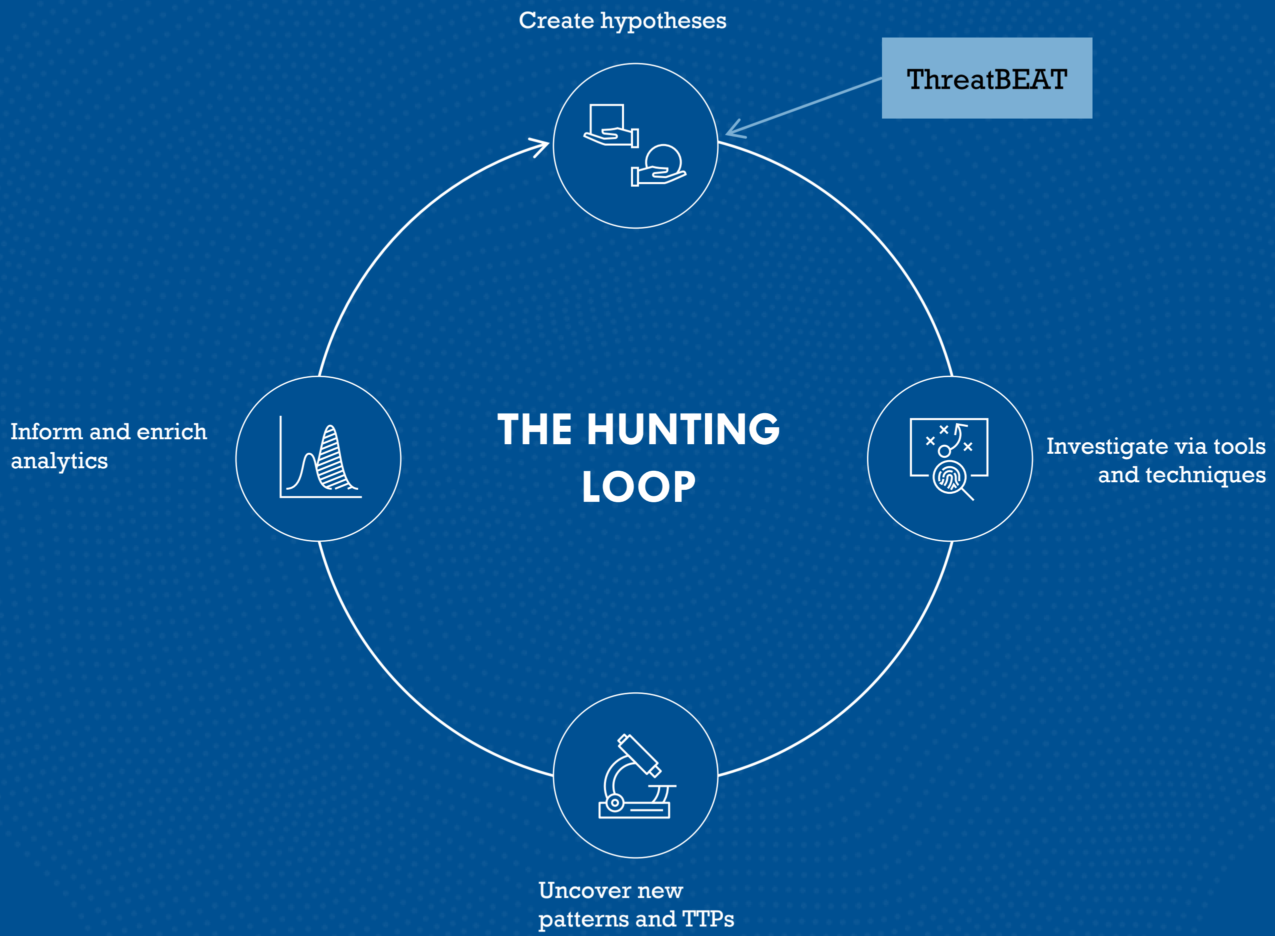
- Configure solutions for service delivery
- Tuning
- Client escalation sequence
- Deliver Optiv SOC portal credentials

SERVICE ACTIVATION

- Service integration validation
- Operational transition to service delivery
- Commencement of service period

ONGOING OPERATIONS

- SOC triage and threat analysis
- Reporting



Create hypotheses

ThreatBEAT

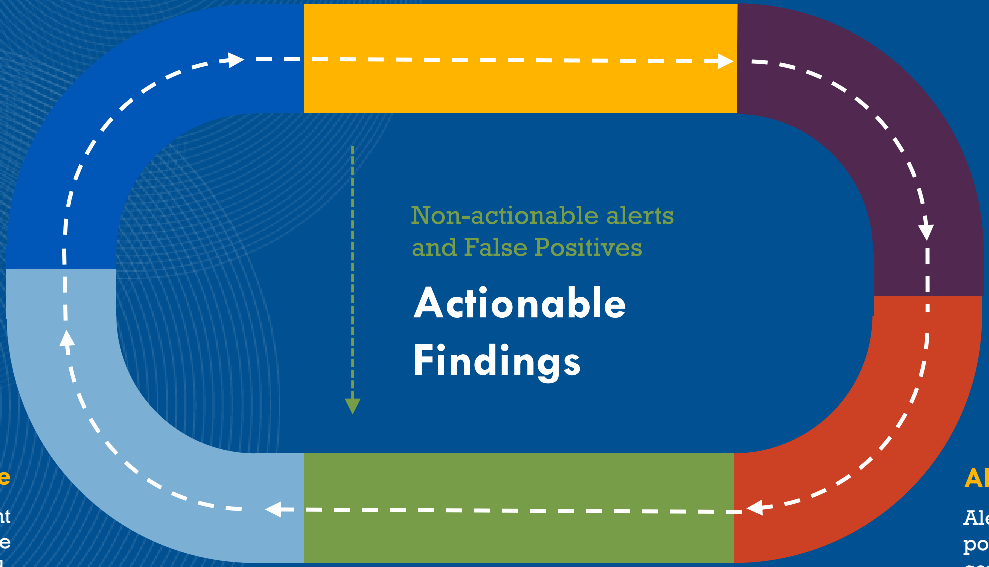
THE HUNTING LOOP

Investigate via tools and techniques

Uncover new patterns and TTPs

Inform and enrich analytics

24/7/365 Alert Monitoring



START

Alert Ingestion

Threat analyst acknowledges and reviews security alert within the Portal's prioritized alert queue that is monitored 24/7/365.

Alert Triage

Threat analyst uses intelligence queries, history and events to determine need for further investigation or if it is non-actionable/a false positive.

Alert Analysis

Security alerts are investigated using human analysis and automation.

Alert Escalation

Alerts containing suspicious or potentially malicious activity that could impact client may be escalated for further investigation.

Alert Remediation Support

Optiv SOC staff collaborate with client in support of remediation efforts.

Incident Closure

Optiv SOC staff close incident upon client confirmation that the incident has been resolved.

OPTIV

Why Optiv for Microsoft

Microsoft Partner
Microsoft
Gold Cloud Platform
Silver Application Development

Member of
Microsoft Intelligent Security Association
Microsoft

Extension of Microsoft Team

Extension of in-house expertise in Access Management, Identity Governance and Data Governance & Protection across Microsoft technologies

Secure Cloud Adoption

Optiv supports clients as they move to the cloud with security-by-design as a core principle for secure cloud adoption

Business Alignment

Map strategy to measurable business outcomes (i.e. full optimization of O365 investment)

Leverage our Strengths

Optiv, as a Cyber Provider and Solutions Leader, goes beyond consulting with implementation, migration and management capabilities to enable clients through their Microsoft security journey

Holistic Approach

Optiv approaches Microsoft technologies with end-to-end services from multiple practices such as Cyber Operations, Threat, Risk, etc.

Agile and Proactive

Optiv's approach can advance how Microsoft features are securely used and consumed – with a keen eye for identifying security gaps

Industry Expertise

Unique and proven methodology quickly shows value leveraging Optiv best practices and Microsoft's guidelines

OPTIV

QUESTIONS

Thank You!

OPTIV

Secure greatness™

OPTIV

OPTIV