Articulate (and Act On) Data Quickly

Security in the digital transformation (DX) era hinges on your ability to process data quickly and intelligently—how well can you extract high-value threat signals from all the noise? There’s one problem, though: the sheer amount of data organizations must filter makes finding anomalies like finding salt grains in a sandbox. The strain on staff, time and budgets is as huge as it is predictable.

Many organizations are deploying machine learning (ML) solutions, which automate and accelerate data processing and action, to alleviate these burdens. Not only are such tools capable of discerning and prioritizing threats faster than their human counterparts, but they also learn from their experiences to improve detection results continuously.

Optiv Solutions

Optiv’s Machine Learning for Threat Detection service helps organizations implement and optimize their ML environment to address evolving cyber threats—whether they stem from external actors or insider threats. Our project team and data scientists analyze your current ML architecture and apply a tailored best practices blueprint aimed at boosting threat detection capabilities. We’ll enhance alignment with your business goals, unite data ingestion and delivery, clarify staff roles and streamline your ML lifecycle for rapid development of additional use cases. The result is efficient data processing tailored to your organization, allowing for faster threat detection and rapid mitigation or remediation.

Our Approach

**Visioning**
We align with your ML process’s stakeholders to set objectives and design your enhanced capabilities roadmap

**Assessment**
We’ll evaluate your existing ML architecture and processes in depth, providing access to subject matter experts and reviewing alternatives with teams

**Blueprint**
We share and customize our comprehensive Machine Learning in Production blueprint, providing hands-on, step-by-step instructions for establishing ML programs at scale

**Build & Deploy**
Our project team helps develop the infrastructure and/or actual models to achieve machine learning success

**Run & Operate**
We provide analytics as-a-service in a managed plan for regular “checkups” on your process and development
The Optiv Advantage

**Built for business, our comprehensive ML solutions solve for:**

- **talent shortages** with automation and orchestration
- **technology proliferation** and poor integrations
- **compliance demands**, catching up to regulations and responding to policy changes
- **trust issues** by securing digital interactions in a shared IT responsibility model
- **data explosion** through understanding, managing and creating insight from business- and security-relevant data

They also reduce:

- **risk** by discovering and managing what is really happening
- **reliance** on scarce security skills
- **costs** through secure automation and consolidation

Optiv’s Cyber Digital Transformation Expertise

- **16 YEARS**
  The average experience of Optiv’s Cyber Digital Transformation team

- **EMERGING TECHNOLOGY EXPERTISE**
  Data analytics, DevSecOps, public/private/hybrid cloud, orchestration and automation, robotic process automation

- **CERTIFIED PROFESSIONALS**
  AWS - Professional, CISSP, CCSP, GIAC, CCSK, Google Cloud Professional, MCSE, Databricks, Elastic, NERC CIP, IEC 62443, GICSP and more

- **INSPIRED THOUGHT LEADERS**
  Speaking engagements at leading industry conferences, including: Microsoft Ignite, AWS Re:Invent, RSA Conference, Spark Summit, Black Hat and more

Case Study

A top retail and apparel company struggled with big data processing and bringing customized UEBA models to production, hampering its ability to detect insider threats quickly. Optiv helped the client enhance its UEBA platform, refactor its data pipeline, speed threat detection times and implement a development process that ferries use cases from ideation to production.

**CHALLENGES**

- Tedious process for procuring, processing and extracting value from data
- Glacial pace for identifying insider threats
- Chaotic development practices, standards and efficiencies
- Delays getting new models from idea to production

**SOLUTION**

- Developed a customized best practices blueprint for ML at scale
- Clarified development and production environment roles and capabilities
- Shifted code base to be modular, testing new and existing code before production
- Refactored data pipeline to cultivate relevant insights faster

**RESULTS**

- Reduced UEBA threat alerts timeline from a day to a few minutes
- Significantly reduced production issues
- Boosted signal-to-noise ratio for alerts
- Automated tickets and alerts for high-value detections
- Evaluated data flows, identified and cleared bottlenecks
- Accelerated development of additional use cases

Secure greatness™

Optiv Security is the cyber advisory and solutions leader, delivering strategic and technical expertise to more than 7,000 companies across every major industry. We partner with organizations to advise, deploy and operate complete cybersecurity programs from strategy and managed security services to risk, integration and technology solutions. With clients at the center of our unmatched ecosystem of people, products, partners and programs, we accelerate business progress like no other company can. At Optiv, we manage cyber risk so you can secure your full potential.