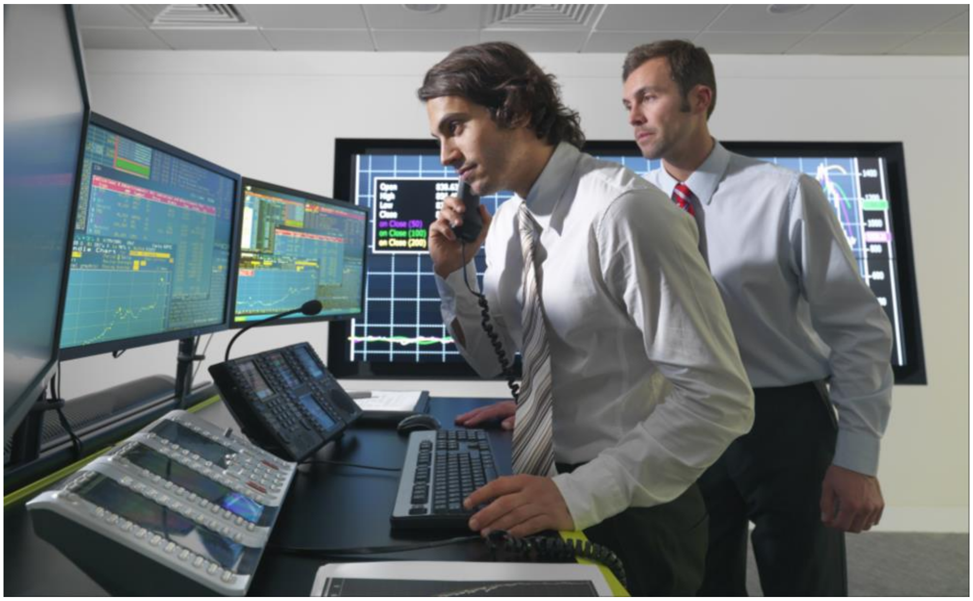
AT&T Business

AT&T Cybersecurity Consulting Services- Security Automation and Orchestration



IT organizations are being asked to do more with less – provide more service in less time using fewer people. Infrastructure operations teams manage increasingly complex enterprises while security teams must respond to an ever-growing volume of cyber threats.

Benefits

- Help increase agility and operational efficiency - execute actions in minutes instead of days/months
- Help reduce costs of repetitive tasks and routines
- Help see value of investments in existing infrastructure and cybersecurity tools through smart integration
- Help Increase accuracy and reduce manual configuration errors across the network

AT&T Cybersecurity Services offer **Security automation and orchestration solutions** that can help your operations and security teams achieve operational efficiency in cloud, on-premise and hybrid environments, enabling you to meet evolving demands of digital transformation. This solution is a force multiplier for your teams, allowing them to focus on more valuable activities by enabling faster, more scalable, and more efficient delivery of operations and security services.

Enterprise Security Orchestration & Automation (ESOA)

As customers embrace Cloud and Software Defined technologies, and other more comprehensive security models are established (e.g., Zero Trust), customers are shifting focus to maturing their overall security programs and re-architecting their networks to accommodate this maturity and advanced technology.

Transforming security operations in one of those steps can come in different forms. A Customer can transform their Security Operations Center (SOC) by optimizing and integrating their overall people, processes and technologies, or they can transform through automation and orchestration, or both. For that reason, this service is offered through two independent services that are joined to form ESOA: SOC Optimization and Security Orchestration & Automation.

Security Operations Center (SOC) Optimization

AT&T Cybersecurity Consulting's SOC Optimization Service provides the breadth and depth of knowledge from over 100 years of cumulative operations experience protecting telecommunication networks domestically and internationally. We help you streamline implementation, accelerate maturity of capability and address security operational requirements with a best in class service management approach. This unique methodology not only addresses a comprehensive scope of operations but also, the holistic integration of technology, process, operational skills and functional organization enabling the achievement of service excellence in Security Operations.

ESOA Engagement

- Operations Maturity Review
    - Discover current SOC state & information security program
    - Understand security operational capabilities
- SOC Analysis & Service Alignment
    - Determine current and future state gaps
    - Analyze tools and technologies
    - Service intersection and interoperability analysis
- Security Orchestration & Automation Analysis
    - Technical review of orchestration and automation
    - Utilize technology to automate tasks
    - Identify full or selective automation
- Strategy & Roadmap development
    - Develop a step-wise, program approach to achieve next-gen, optimized and automated state
    - Present findings and target next phase

The service provides clients professional advisory, design, and implementation services to help them improve their SOC to better identify and manage cyber threats that could harm the business. Custom scoped and designed to an organization's specific threat management needs, the AT&T Consulting solution helps a client design and implement the right combination of people skills, operational processes and technology to provide the right level of threat analytics and incident response capabilities.

Security Orchestration & Automation (SOA)

Orchestration and Automation are often used interchangeably as synonyms, but they are somewhat different. Orchestration is the ability to coordinate informed decision making and formalize and automate responsive actions based on measurement of the risk posture and the state of an environment. Automation is a subset of orchestration. It allows multiple tasks (commonly called "playbooks") to execute numerous tasks on either partial or full elements of a security process.

Two forms of security operations automation are often encountered: one focusing on automating the workflow and policy execution around security operations; the other automating the configuration of compensating controls and threat countermeasure implementation.

Security Automation and Orchestration builds upon the output of a SOC Optimization engagement, but it can also work on its own. Customers that currently have mature SOCs with integrated services and effective runbooks may only want to automate security services within their environment without service alignment and service management. SOA will perform a technical evaluation of a client's security services, identify what process steps can be automated with existing tools/technologies or with recommended orchestration platforms, and it will provide a roadmap output for a customer to build those automated playbooks or build those automated playbooks for the customers.

© 2018 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo and other marks are trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners.
The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.