Diverse IT, LLC

Security Intelligence and Operations Consulting (SIOC)

Get the most from your Diverse IT® Security Analytics, Automation, and SIEM solutions.

Securing the Enterprise

Diverse IT Security Intelligence and Operations Consulting takes a holistic approach to building cyber defense and security operations solutions that support the risk management, security, and regulatory compliance needs of enterprises around the globe. We use a combination of operational expertise—yours and ours—and proven methodologies to deliver fast, effective results and demonstrate ROI. Our proven, use-case-driven solutions combine Diverse IT market-leading technology together with sustainable business and technical process executed by trained security professionals.

Our Mission

- To enable customers to establish a security intelligence and analysis capability that can proactively detect, respond, and recover from significant security events and protect critical business assets: its applications, data, and users.
- To ensure customers are successful with Diverse IT security products by establishing a SOC capability that provides the right people, builds the right processes, and effectively uses technology.

Proven Expertise

SIOC is strategically capable to optimize and draw value from your Security Operations solutions. To date, our years of experience and proven expertise have resulted in thousands of success stories in core vertical markets the world over, including the following:

- Financial services
- Energy
- Services
- Retail
- Telecommunications
- Healthcare
- Government (defense, transportation, law enforcement, utility regulations)

Diverse IT' SIOC team has delivered over 200 assessments of more than 140 distinct Security Operations Centers worldwide. This insight (of where organizations are succeeding and failing in cyber defense) enables our consultants to share years of SOC know-how with customers and to accelerate the success of your organizations. Our consultants bring decades of field expertise across verticals, and most have been experienced security leaders within Fortune 100 enterprises or public sector organizations.

Our Successes

- Assessed security operations and provided industry-comparison score cards for maturity and roadmaps for improving security for over 140 companies and organizations.
- Built business cases for investment with customer security staff to articulate the need for improved security operations capability and demonstrate return on investment.
- Worked with dozens of Fortune 500 companies to build or mature their security operations, in vertical markets for retail, financial, telco, manufacturing, IT, gaming, service integrators, managed security services providers, and public sector organizations.
- Provided and/or trained customer security operations staff including SOC manager, SOC leads, senior SOC analysts, Level 1-3 SOC analysts, compliance analysts, hunt analysts, data engineers, content developers, and security engineers.
- Designed internal and external service offerings and associated marketing materials to support both internal cost-recovery funding for operations and external for-profit MSSP service offerings.
- Leverage a library of hundreds of use cases to quickly obtain value-producing content for customer's SIEM implementations.
- Accelerate the creation of policies, processes, and procedures for security operations by leveraging a mature and continually improved reference library and framework.
- Implement continual improvement programs that include efficient and effective solutions to monitor and measure security operations.
- Introduce best-practices for building security operations and compliance teams—sharing key insight on critical tasks from employee retention and career progression to effective staffing models and task rotation.
- Integrate the people, process, and technology into world-class security operations.

Roles Provided

Security Intelligence Advisors

Senior Security Global Services consultants work closely with customers as a trusted

Concept of Cyber Security Intelligence & Operations

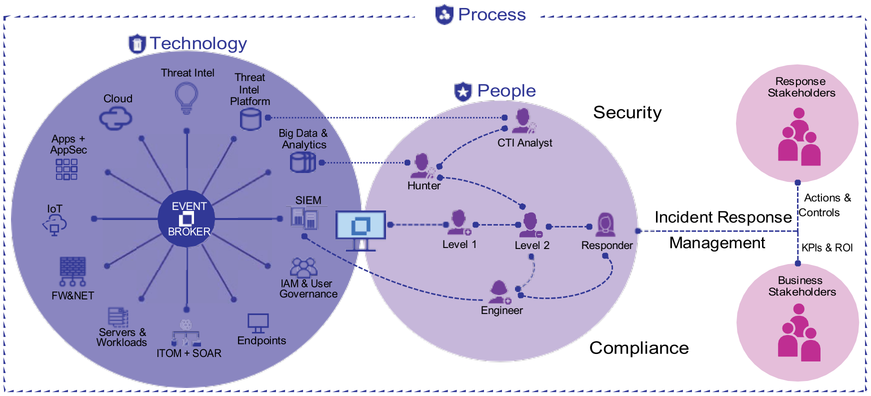

Figure 1. SIOC model

advisor, assisting with operational decisions and leveraging knowledge from previous engagements and industry experience. Use when you want to leverage best practices in your security operations focused on specific operational areas such as SOC or incident response processes and procedures.

Security Operations Leads

Experienced security operations center leaders lead and mature security operations alongside or on behalf of customers. Use when you need a leader for your security operations to mentor and guide someone new to the position or as a temporary measure while filling a full-time position.

Security Analysts

Analysts, from entry to senior levels, trained in using security solutions integrated to your Diverse IT tools and operating within the SIOC best practices customized to your environment work as members of your security operations or compliance teams. Use when you need temporary analysts to expand operations or to backfill openings. SIOC Services also has the ability to help you build your analyst team through local sourcing and training of analyst resources.

SIEM Security Content Engineers

Consultants skilled at optimizing the use and configuration of Diverse IT security solutions perform the creation of correlation rules, dashboards, reports, and systems integration to fulfill client requirements, gain efficiencies through automation and enable effective security operations and intelligence.

Solution Architects

Architects gather requirements and design Security solutions for clients including SIEM architecture, log collection design, use case planning, system integration, distributed correlation, workflow automation, hybrid cloud, and other business drivers to help customers protect critical assets.

SIEM Engineers

SIEM engineers work alongside or on behalf of customers to perform installation, configuration, and administration of Security environments and infrastructures.

Program Managers

Consultants adapt at program management manage large-scale projects encompassing multiple solutions, resources, and/or complex environments.

Protect Critical Assets

Diverse IT SIOC offers customized solutions to address your business needs. These solutions include:

- Risk Management, Security. and Regulatory Compliance
- Hybrid Solutions & Diverse IT Solution Management Services
- Playbook Development and Workflow Automation through SOAR

Contact us at:
www.diverseit.co

Like what you read? Share it.

- HUNT Analysis, Threat Intelligence, and Incident Response
- User Behavior and Insider Threat
- Universal Log Management, Detection, and Event Retention
- Data Privacy Monitoring
- Advanced Persistent Threat
- Secure Software Assurance
- Application and Transaction Monitoring
- Security Intelligence and Operations

Learn more at
www.diverseit.co/cyber-security/

Diverse IT, LLC