World Wide Technology

TECHNOLOGY RUNS ON GREAT PEOPLE

SECURITY OPERATIONS CENTER ASSESSMENT

Respond to intrusions in real time with a security operations center

With the increasing volume and complexity of security threats in today's IT environment, it is critical to have a well-organized capability for monitoring and responding to IT security incidents. The primary mission of the Security Operations Center (SOC) is to monitor, detect, analyze, and respond to IT security threats and reduce risk to business units, partners, and customers. To this end, World Wide Technology's (WWT) approach and methodology for a SOC begins at the foundational level of people, process, and technology.

> VALUE OF SOC

The value of a SOC lies in the capability of responding to potential intrusions in real time and with knowledge gained through historical trending of security-relevant data sources. This capability provides a company with situational awareness and reporting of cybersecurity incidents for response and remediation by responsible company parties.

The most time-consuming components involved with monitoring security-related events are the production and analysis of huge volumes of data. Combined with security audit logs and other data feeds, a typical SOC will collect, analyze, and store tens or hundreds of millions of security events every day. At the core of the SOC is a security information and event management (SIEM) solution that greatly automates the collection of data and detection of events, thus providing SOC analysts a method to sort through the large volumes of events associated with potential malicious or unwanted activities on the network.

> THE ASSESSMENT

WWT will assess each of the foundation-level elements of people, process, and technology. WWT will conduct this assessment using a variety of information-gathering and analysis techniques that include on-site interviews with senior management and key staff members who are in charge of or custodians of policy, procedure, governance, administration, infrastructure, network, application, and security management. The assessment will provide an understanding of the following areas:

- Daily operations being performed
- Chain of communication and escalation paths
- Inventory comparison
- Types of logs
- Monitoring and remediation processes
- Alerts and/or reports that are being generated
- Work flow health

Each of these foundation-level elements will be given a Capability Maturity Model Integration (CMMI) rating. This maturity rating is scored from 1 to 5, which mirrors other common approaches for defining the maturity of an organization or its specific operations.

After conducting the assessment, WWT will deliver a report that details the information gathered, identifies the organization's overall strengths and weaknesses, lists current and future maturity ratings, and provides recommendations for improvement.

GET STARTED TODAY

Call us at 800.432.7008 or visit www.wwt.com to schedule your assessment today and experience the power of WWT's solutions first hand.

Visit us online: www.wwt.com