opentext™ | Cybersecurity

Data Sheet

ArcSight SIOC Primer

ArcSight SIOC Primer services are designed to help customers develop a plan for best practice security monitoring and incident response.

Overview

Develop Best Practices

ArcSight SIOC Primer Services Services by OpenText are designed to help customers plan the development of an internal security monitoring and incident response capability integrated with the ArcSight Security Information and Event Management (SIEM) by OpenText technology. This workshop includes security operations best practices uncovered by OpenText™ Security Services in working with hundreds of security operations groups.

This service is designed to help customers understand:

- The staffing models, training plans, and incident preparedness needed to help ensure your future intrusion analysts succeed
- The security operations processes and procedures for identifying and responding to threats is a consistent and repeatable fashion
- The Security Information and Event Management (SIEM) infrastructure and related technology to help ensure attacks are identified, analyzed, and remediated
- Key tasks, timelines, and resource requirements for establishing a security operations capability

Service Implementation

During the assessment, trained OpenText Security Services specialists will perform activities that may include:

- Educate the customer on best practices and lessons learned for establishing and maintaining security operations capabilities.
- Discuss the following Business and People-related topics:
  - Security operations business drivers (e.g., comply with regulations, limit the risk exposure, reduce down time, respond quickly to attacks, Operations cost components
  - Recommended org chart with current skills and expertise
  - Roles and responsibilities of the various people that will be in the operations group
  - Process to recruit and hire new personnel
  - Training program—to bring in new employees and keep existing employees current on new security topics
  - Skills assessment and tracking
- Discuss the following Process-related topics:
  - Process and procedure framework that will be used to standardize operations from person to person, shift to shift, and day to day
  - Overarching workflow that will be used to identify a security event, analyze, and then take the appropriate action
  - Knowledge base and documentation repository

Quick View

ArcSight SIOC Primer Services are designed to help customers plan the development of an internal security monitoring and incident response capability integrated with the ArcSight Security Information and Event Management (SIEM) technology.

- Discuss the following Technology-related topics:
  - Network and security device architecture
  - Security Information and Event Management (SIEM) technology (current or future) and its impact to security operations
  - Reporting strategy to provide the right information to the right audiences
- Provide a presentation to the customer team outlining the concepts discussed in the workshop
- Provide a Solution Roadmap with project phases on how best to build the security operations capability outlining business drivers, value propositions, and resource requirements based on identified requirements and business need.

Service Planning and Deployment

The OpenText Security Services specialist will schedule the delivery of this Service at a time mutually agreed upon between OpenText and the customer, which shall be during local OpenText standard business hours, excluding holidays, unless otherwise agreed by OpenText. Any services provided outside of standard business hours will be subject to additional charges.

The OpenText Security Services specialist perform activities that may include:

- Schedule and attend a kick-off meeting to review objectives, schedule, required audience and deliverables
- Meet with your key stakeholders in order to assess the business, people, process, and technology components of your security operations
- Share best practices and lessons learned applicable to building, operating, and maturing security operations capabilities integrated with ArcSight ESM by OpenText.
- Conduct a close-out meeting to discuss key findings and recommendations

The OpenText Security Services specialist will be available to answer questions during the onsite or remote portions of the service delivery.

Service Eligibility

Prerequisites

The customer must provide the following for delivery of this service:

- Conference room with white board and projector
- Access to key stakeholders for interviews and group discussions:
  - **IT Security Sponsor:** This is the CISO, CSO, Director of IT Security, IT Security leadership, IT Leadership, or champion of the Initiative that the SIEM implementation supports
  - **Security Operations Manager:** This is the person who leads day-to-day security operations
  - *Security Operations Personnel:* These are the people who perform review and analysis of security events in the SIEM
  - **Security Engineering:** These are the people responsible for the management of the SIEM, security devices, or other security technology
  - **Ancillary Security Functions:** This term refers to any other security personnel that might have a vested interest in the security operations (e.g., incident response, compliance, risk, etc.)

Service Limitations

This service will be delivered as a single, continuous event as per the terms outlined in the Duration section of the document. Environments requiring multiple engagements or phases over longer periods of time are not included in this Service, but can be accommodated at additional cost through a Statement of Work. Activities such as, but not limited to, the following are excluded from this Service:

- Installation and configuration of OpenText software or appliances
- Racking of appliances or servers
- Development of FlexConnectors
- Delivery of standard Education offerings
- Performance testing or modeling services that, in the opinion of OpenText, are required due to unauthorized attempts by non-OpenText personnel to install, repair, maintain, or modify hardware, firmware, or software
- Services required due to causes external to the OpenText-maintained hardware or software
- Any services beyond the license limitations of the included products
- In addition, the customer will be responsible for all applicable data backup.

Customer Responsibility

- Contact an OpenText Security Services specialist within 90 days of the date of purchase to schedule the delivery of the service
- Coordinate Service deployment on third-party-maintained hardware/software (if applicable) with OpenText Software.
- Assign a designated person from the customer's staff who, on behalf of the customer, will grant all approvals, provide information, attend meetings, and otherwise be available to assist OpenText in facilitating the delivery of this service
- Ensure that all Service prerequisites as identified in the Service Eligibility section are met
- Retain and provide to OpenText upon request all original software licenses, license agreements, license keys, and subscription service registration information, as applicable for this Service.
- The customer shall provide reasonable access and working space at the site as OpenText may reasonably request.

The customer will provide OpenText and OpenText subcontractor staff standard telephone and dial-up or comparable data access to OpenText's network at industry standard speeds. OpenText shall observe the customer work rules and security and safety policies while performing OpenText Services at the site of which OpenText is informed of in writing in advance and that are not inconsistent with OpenText's own business practices.

Duration

Delivery of this Service will not exceed a total of 80 service hours. This Service will be delivered by two (2) OpenText Security Services specialists and includes one (1) onsite visit for up to two (2) days in duration.

Terms

This offering consists of a consulting and training effort and is governed by the OpenText Customer Terms. All capitalized terms used in this Data sheet, but not otherwise defined, will have the meaning assigned to them in the Terms. For purposes of this Data sheet, "services" mean consulting, integration, professional services or technical services performed by OpenText under this Data sheet. Services excludes hardware maintenance and repair, software maintenance, education services, or other standard support services provided by OpenText; software as a service, and outsourcing services.

Acceptance of Deliverables occurs upon delivery.

Hiring of Employees. You agree not to solicit, or make offers of employment to, or enter into consultant relationships with, any OpenText employee involved, directly or indirectly, in the performance of services hereunder for one (1) year after the date such employee ceases to perform services under the terms of this Data Sheet. You shall not be prevented from hiring any such employee who responds to a general hiring program conducted in the ordinary course of business and not specifically directed to such OpenText employees.

Authorization to Install Software. During the provision of services, OpenText may be required to install copies of third-party or OpenText-branded software and be required to accept license terms accompanying such software ("Shrink-Wrap Terms") on your behalf. Shrink-Wrap Terms may be in electronic format, embedded in the software, or contained within the software documentation. You hereby acknowledge that it is your responsibility to review Shrink-Wrap Terms at the time of installation, and hereby authorizes OpenText to accept all Shrink-Wrap Terms on its behalf.

Intellectual Property. OpenText may provide OpenText tools, templates, and other pre-existing intellectual property of OpenText during the course of providing services ("OpenText Pre-existing IP"). OpenText Pre-existing IP does not include, nor is considered a part of, either the Deliverables or OpenText software products. OpenText retains all intellectual property ownership rights in such OpenText Pre-existing IP. All OpenText Pre- existing IP is OpenText Confidential Information. OpenText Pre-existing IP may be governed by additional license terms that are embedded in the OpenText Pre-existing IP.

Payment and Validity

This offering will be pre-billed. You agree to pay invoiced amounts within thirty (30) days of the invoice date. If applicable, you must schedule delivery of the offering to be completed within a period of one (1) year from the date of purchase. Notwithstanding the previous sentence, OpenText's obligations to deliver the offering under this Data Sheet are considered fulfilled and your rights of receipt of the offering under this Data Sheet will expire one (1) year from the date of purchase.

Pricing for the offering may vary by country.

Connect with Us

www.opentext.com

Cancellation

To avoid a Cancellation Fee as defined herein, you shall notify OpenText in writing of cancellation or rescheduling at least ten (10) business days prior to the offering start date. Cancellations or rescheduling with less than ten (10) business days notification will incur 100% of the offering fee ("Cancellation Fee"). If you cancel with ten (10) or more business days in advance of scheduled delivery, you may reschedule only if delivery will be complete within one year from the purchase date.

Change in Scope

Changes in scope are not allowed. You can request additional or different services, if available and at additional cost, through a statement of work or change order.

SKU PS-AA673

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

760-000046-002 | O | 10/23 | © 2023 Open Text