opentext™

Security Services

Program Service Catalog

opentext™

Contents

opentext™

Overview

Open Text Corporation and its Affiliates (“OT”) provide the enclosed services through OT’s Professional Services (“OT PS”). This catalog is provided solely for the purpose of evaluation of the services and is not intended to be used for any other purpose. The information within may be changed by OpenText at any time, without prior notice. No portion of this proposal may be reproduced without prior written approval by OpenText. This catalog will not create any legal rights or binding obligations on the part of OpenText or Customer. These services are governed solely by the terms and conditions as set forth in the EnCase Services Program Handbook and the then-current version of the applicable OT Professional Services Agreement, (both available upon request or at www.opentext.com/agreements, or any other negotiated, signed agreement between OT and Customer.

1. Introduction

Whether it's a risk posed by threat actors to a firm's financial, legal or reputation situation, or the ever growing legislation protecting data subjects and their privacy, organizations need to monitor and invest in their risk and compliance programs and security posture. Cyber security starts at the end point and with users, and then touches every aspect of an organization. Cyber resilience is no longer optional; it is an essential component of Information Management to protect the most valuable assets: data and business processes.

The best enterprise information security solutions provide deep visibility into digital security and investigation of potential risk across all endpoints and devices as they emerge. They also allow for greater automation and contextualization of security events for faster triage, more informed decision-making, data loss prevention and effective remediation. To deliver the best, OpenText Professional Services provides consulting services in the areas of:

- Product Readiness
- Risk and Compliance
- Digital Forensic and Incident Response
- Managed Security Services

OpenText's unique approach provides the opportunity for our organizations to add to or customize our services to meet their needs, ultimately creating the industry's most robust service offering.

The OpenText Security Services is a global team of security professionals focused on delivering business results through our advice, guidance, and assistance, and realizing helpful benefits such as:

- Detect unknown threats and reduce risk
- Get experienced security expertise
- Access a wide spectrum of security services
- Easy collaboration and straight-forward contracting model

opentext™

2. Product Readiness

OpenText EnCase solutions let you readily establish visibility to all your data, regardless of where and how it is store. See what matters on each and every network endpoint and in every data store in your organization, then transform that critical data into intelligence that fuels more effective security, risk and compliance, legal and internal investigations.

2.1 EnCase Installation / Health Check / Upgrade

Overview

The OpenText Security Services team delivers EnCase Product Readiness services, designed to:

- Assist customers with installation of software
- Support the customer with product upgrades, providing product enhancements, aligning the customer's use of the software to best practices
- Provide staff augmentation
- Carry out periodic health checks to ensure maximum product efficiency

Benefits

- High-level design/scoping of initial deployment of EnCase products
- Recurring health checks / upgrades
- Scoped to network configuration and business goals

Outcomes

OpenText helps its customers by providing technical resources certified and proficient in the installation of EnCase products, ensuring a seamless deployment to production and business usage.

The EnCase Installation / health check / upgrade service's key deliverables are as follows:

- Installation / health check / upgrade report
- Customer architecture document

2.2 EnCase Enablement

Overview

Work with Professional Services to get the most out of your EnCase environment. From best practices to automations, our consultants have the skillsets to script, automate, and integrate the EnCase products to enhance your workflows and provide access to greater efficiencies.

Benefits

- Workflow development
- Best practice knowledge transfer
- Incident and problem management to agreed SLAs
- Product customizations (examples below)

opentext™

Examples of customizations and integrations

EnCase eDiscovery	
EnCase Workstation Collection Portal	Web app that kicks off collections
Druva Connector	The Druva Connector takes data the was backed up to Druva and collects it into a eDiscovery Case
eDiscovery API	The eDiscovery API allows a programmer to access most of the eDiscovery functionality programatically
LXY	LXY collects files, adds them to a LEF, creates a eDiscovery case and adds the LEF to the case
VeritasConnector	I believe that this connector collects data from Veritas eVault for ingestion into eDiscovery
EnCase Endpoint Investigator	
SIEM Event Handler	The SIEM Event Handler program will process "SIEM events" and trigger EnCase jobs to gather the required information from the target machine
HSBCSweeper	The MachineSweep program will trigger EnCase scripts to gather the required information from the target machine
Collector	This app allows a user to specify files to be collected (UNC or target machine) and places them in a LEF
EnCase Endpoint Security	
Event Logger	The Event Logger program will gather "Endpoint Security Events" and output the data to a file that can be ingested by LogRhythm.
HashList Maintenance	This app gathers hashes from MISP and imports them into Endpoint Security
MISP Event Generator	The event generator pulls event data from Endpoint Security and sends it to MISP
CreateCriteriaAPI	Created basic criteria in Endpoint Security for integration with Demisto
SplunkEventGenerator	The event generator pulls event data from Endpoint Security and sends it to Splunk
Splunk Integration	Connector to allow analyst to right click and start collections from alerts as needed
ShutdownAutoCollect	The AutoCollect system will trigger EnCase scripts to gather the required information from the target machine (VDI) at shutdown

Outcomes

Upon completion of the engagement, a final report will be issued which will include the following:

- Executive Summary
- Identified issues
- Recommendations for improvement

2.3 EnCase Assist

Overview

Proactive implementation services to ensure the EnCase environment is up to date. By working with our team members on a regular basis as new releases are developed this will ensure you are leveraging the most out of the EnCase products.

Benefits

- Enhanced proactive and preventative services
- Dedicated Services Program Manager to ensure delivery
- Continuous improvement and operation optimization
- Case work / engagement support / staff augmentation

Outcomes

Throughout the engagement, OpenText Security Services will prepare and provide status reports regarding the status and progress of the project.

Upon completion of the engagement, a final report will be issued which will include the following:

- Executive summary
- Identified issues
- Recommendations for improvement

2.4 EnCase Manage

Overview

Your EnCase environment is mission critical. Use audits and the up-time of the application is pertinent. Leverage our consultants on a regular cadence for health checks, upgrades, audits, and quarterly business reviews to stay ahead of environment maintenance for your EnCase applications.

Benefits

- Enhanced, proactive and preventative services delivered directly by OpenText Professional Services experts
- Dedicated Services Program Manager to ensure delivery
- Continuous improvement and operation optimization
- Recurring monthly audits
- Recurring quarterly health checks
- Quarterly business reviews
- Bi-annual upgrades

Outcomes

Throughout the course of the engagement, OpenText Security Services will prepare and provide the following documents to the customer:

- Status reports
- Health check report
- Installation report
- Acceptance test report

3. Risk and Compliance Advisory

Reducing risk in an organization's environment can be challenging when there is no solid understanding of the security posture.

The Risk and Compliance Advisory services start with evaluating the customer's cyber security controls and internal processes against industry benchmark standards, and its ability to comply with various regulatory frameworks. Vulnerabilities in the customer's environment are identified, and training on best practices is conducted to reduce potential risks.

3.1 Security Assessment

Overview

OpenText Security Assessment Service helps effectively manage security efforts by benchmarking to best practices. Through a consultative approach, the OpenText Security Services team provide an assessment of cyber and compliance risks, the maturity of control capabilities and a roadmap to improving security posture in a short time frame.

Benefits

The goal of the Security Assessment Service is to provide better visibility into the inherent risk and maturity of a security program to prevent, reduce and mitigate cyber risks that could have regulatory, financial, legal, or reputational impacts.

Outcomes

The Security Assessment service's key deliverable is a security assessment report featuring the following items:

- Executive summary
- Control maturity benchmarks
- Identified issues
- Recommendations for improvement

3.2 Security Health Check

Overview

A resilient cyber program must maintain a clear understanding of it's capabilities. In addition, compliance requirements necessitate that an organization assess their risks regularly to ensure that security controls are in place and operating effectively. An OpenText Security Health Check is a great way to achieve these objectives.

Benefits

The Security Health Check provides organization visibility on their standing against 6 foundational security control areas according to NIST 800-53r4, NIST CSF and CIS CSF standards:

- Inventory and control of hardware assets
- Inventory and control of software assets
- Continuous vulnerability management
- Controlled use of administrative privileges
- Secure configuration for hardware and software
- Maintenance, monitoring and analysis of audit logs

Outcomes

At the conclusion of the Security Health Check, the following items are included in the final report:

- Executive summary
- Risk / control matrix
- Identified issues
- Recommendations for improvement

3.3 Privacy Capability Assessment

Overview

The OpenText Privacy Capabilities Assessment service benchmarks your organization's controls against the National Institute of Standards and Technology's (NIST) Privacy best practices. Through a consultative approach, the OpenText Security Services Team provides an assessment of your current privacy program maturity and roadmap to improve privacy capabilities within a short time frame.

Benefits

- Enable compliance capabilities with better visibility into current controls capabilities
- Maturity benchmarking against NIST Privacy Framework tiers
- Deliver actionable recommendations to improve current privacy controls and reduce risk
- Build trust by improving transparency and protection of individual's privacy

Outcomes

The Privacy Assessment Service's key deliverable is a security assessment report featuring the following:

- Executive summary
- Current privacy security control maturity benchmarks
- Identified issues
- Recommendations for improvement

3.4 Policy and Procedure Documentation Review

Overview

Having appropriate policies, procedures, controls, tools, and properly trained employees are all key to ensuring that an effective cyber security program is in place. OpenText Security Services Team focus on control design, existence, and benchmarking of the following current cyber security control activities:

- Inventory and control of hardware assets
- Inventory and control of software assets
- Continuous vulnerability management
- Controlled use of administrative privileges
- Secure configuration for hardware and software on mobile devices, laptops, workstations, and servers
- Maintenance, monitoring and analysis of audit logs

Benefits

The OpenText Security Services Team leverage a collaborative approach to benchmark policy, plans and procedure documentation against NIST 800-61r2 to improve:

- Digital Forensics and Incident Response (DFIR) readiness across the organization
- Timeliness and completeness of communication procedures
- DFIR activity procedure documentation
- OpenText solution usage
- A roadmap to draft and maintain documentation

Outcomes

Upon completion of the engagement, a final report will be issued which will include the following:

- Executive summary
- Identified issues
- Recommendations for improvement

3.5 Table-Top Exercises

Overview

OpenText table-top exercises are discussion-based exercises, where personnel with roles and responsibilities meet in a classroom setting or in breakout groups, aimed at reviewing roles during an emergency and the responses to an incident. This includes:

- Curating the exercise based on updated policies, plans and procedures
- Event design and planning, including solidifying topics, scope, objectives, participants and coordinating logistics
- Provide executive summary and results from the exercise with recommendations for improvement

Benefits

- Curated table-top exercises reinforce cyber security best practices and use of OpenText solutions in responding to incidents
- Security awareness workshops on cyber security best practices

Outcomes

The following results from the table-top exercises are provided to the participants:

- Executive summary
- Table-top scenarios
- Recommendations for improvement

3.6 Enterprise Content Systems (ECS) Security Assessment

The OpenText Enterprise Content Systems (ECS) Security Assessment Service helps effectively manage security efforts by benchmarking to best practices to secure your OpenText ECS Systems. Through a consultative approach, the OpenText team provides an assessment of security risks, maturity of an organization's ECS security control capabilities, and actionable recommendations to improve their security posture within a short time frame.

Overview

A key goal of the Security Assessment Service is to provide better visibility into the inherent risks in the existing security program for the ECS solution. The service makes concrete recommendations towards mitigating cyber risks that could have regulatory, financial, legal, and reputational impacts on an organization.

Benefits

- Review of current implementation documentation
- High-level review of customizations and enhancements
- Workshop to discuss documentation and processes
- Analysis of the inputs and results of the workshop, to benchmark the implementation against established good practices.

Outcomes

Throughout the engagement, OpenText will prepare and provide weekly status reports regarding the status and progress of the project.

Upon completion, a final ECS Security Assessment Report will be prepared and provided.. The ECS Security Assessment Service provides a security assessment report featuring the following:

- Executive summary
- Control maturity benchmarks
- Recommendations for improvement

opentext™

4. Managed Security Service Program

OpenText MSSP services integrate the best of breed technologies with custom workflows leveraging machine learning and MITRE ATT&CK framework reducing time to detection and increasing the ability to respond to threats.

4.1 Managed Security Service

Overview

We believe in people, process and technology as being the core of any managed security service provider. Here at OpenText, we have highly skilled and trained security analysts with identified workflows to detect real-time threats and perform continuous response and remediation activities.

Benefits

- Custom workflows leveraging machine learning and MITRE ATT&CK framework
- Real time, 24 × 7 security monitoring and threat detection
- Next generation cloud based SIEM for log management and improved visibility

Outcomes

Upon completion of the engagement, a final report will be issued which will include the following:

- Executive summary
- Identified issues
- Recommendations for improvement

4.2 Threat Detection and Response

Overview

OpenText Security Services will detect threat in minutes not days. Having complete visibility of a customer's environment (network, endpoints, e-mail, mobile and cloud) allows us to provide a rapid response to isolate and remediate any threats within minutes of detection.

Benefits

- Network log optimization to improve visibility and response capabilities.
- Customization of firewall rules, access controls and reporting to maximize protection.
- Improve endpoint visibility and response capabilities.
- Intrusion detection and prevention configuration to improve protection and monitoring capabilities.
- Web gateway appliance configuration and monitoring.
- Advanced threat detection and timely response actions to protect critical assets.

Outcomes

Upon completion of the engagement, a final report will be issued which will include the following:

- Executive summary
- Identified issues
- Recommendations for improvement

5. Digital Forensics and Incident Response (DFIR)

The Digital Forensics and Incident Response (“DFIR”) services consist of forensic investigations performed by OpenText Security Services team to detect and respond to actual breachesand breach scenarios existing throughout a customer’s organization.Investigating, responding, mitigating, and preventing security incidents requires skillsets and tools that many organizations do not have in-house.

The OpenText Security Services can help with the following:

- Preventative – Threat hunting and vulnerability scanning/penetration testing services
- Reactionary – Insider threats and breach response services
- DFIR experts
- OpenText tools
- Ability to investigate and analyze all points where data resides or has been transmitted

5.1 Threat Hunting

Overview

The OpenText Threat Hunting service delivers advanced threat intelligence to enable quick identification and monitoring of threats and attacks. The OpenText Security Services team use the tools needed to discover malware and suspicious behavior that, if undetected, can offer access to cyber-criminals for months or years. The service can uncover anomalies, such as non-human patterns, spikes of activity outside normal business hours and other red flags that may indicate an attack, insider theft or intentional destruction of data.

Benefits

- Provide preventative, proactive support to identify or validate the existence of threats and/or malicious activity within and across the cyber kill chain.
- Quick identification of patterns, relationships, and indicators of compromise.
- Insight to potential zero-day threats before they can attack the environment, both on-premises and in the cloud using their Ai & Machine Learning tools.
- Threat hunting beyond network logs to cover endpoints and expand security measures.
- Remediation, risk, and compliance recommendations to close gaps in security protocols and policies.

Outcomes

Upon completion of the engagement, a final report will be issued which will include the following:

- Executive summary
- Identified issues
- Recommendations for improvement

5.2 Breach Response

Overview

OpenText Security Services uses the best in breed technologies with custom workflows leveraging machine learning and MITRE ATT&CK frameworks. Breach response is carried out in real-time reducing the time to remediate exponentially. Our breach response team can begin within 24-hour notice and come equipped with the tools, know-how, and extensive DFIR experience.

Benefits

- Provide reactive incident containment to detect persistence, impact, and evasion behavior providing a root cause analysis
- Provide control remediation recommendations
- Identify and secure evidence in support of potential breach scenarios

Outcomes

Upon completion of the engagement, a final report will be issued which will include the following:

- Executive summary
- Identified issues
- Recommendations for improvement

5.3 Insider Threat / Investigations

Overview

Insiders have a significant advantage over external attackers. Historically, organizations focused on external-facing security mechanisms such as firewalls, intrusion detection systems, and electronic building access systems. Insiders, however, are not only aware of their organization's policies, procedures, and technology but are also often aware of their vulnerabilities, such as loosely enforced policies and procedures or exploitable technical flaws in networks or systems. In some cases, the malicious insider can even be the one who configured the organization's security.

Benefits

- Forensic investigations of endpoints, mobile devices, and the cloud
- Detection of malicious insider actions within corporate environments
- Determine organizational risk and data exposure resulting from malicious inside behavior
- Insider threat incident response plan
- Prevention, detection, and response infrastructure

Outcomes

Upon completion of the engagement, a final report will be issued which will include the following:

- Executive summary
- Identified issues
- Recommendations for improvement

5.4 Vulnerability Scanning and Penetration Testing

Overview

Our penetration testing is focused around identifying vulnerabilities that arise from improper configuration and patch management processes. OpenText consultants will use OWASP and other frameworks to identify high-risk areas and determine the impact, should they be penetrated.

Benefits

- Vulnerability scanning of operating systems, services, and applications to discover improper configurations or risky end-user behavior
- Vulnerability scanning in support of compliance requirements such as Open Web Application Security Project's (OWASP) top-ten security controls, PCI, or HIPAA
- Web application pen-testing using offensive techniques attackers leverage in exploiting web application servers to discover security gaps

Outcomes

Upon completion of the engagement, a final report will be issued which will include the following:

- Executive summary
- Identified issues
- Recommendations for improvement

opentext™

6. EnCase Advisory Program (EAP)

The EnCase Advisory Program (EAP) is a professional services relationship that maximizes the customer's return on investment in OpenText's EnCase suite of software products by focusing on analysis, planning, environment support, and continuous assessment of the customer's utilization and needs. EAP enables access to technical resources, including professional services, technology, industry knowledge, and executive support. OpenText customizes each EAP to meet the customer's specific business needs, considering the customer's current infrastructure status, assessing current practices, and allowing for planned growth.

EAP packages are sold with a fixed number of "Units" that are convertible into a corresponding number of consulting hours depending on the specific task requested to be performed. OpenText resources may consume units at different rates based on the task assigned.

Overview

The EnCase Advisory Program (EAP) is designed to give customers the ability to purchase OpenText Security Services using a single order.

EAP Package	Number of Units
EAP 150	150
EAP 250	250
Bronze	500
Silver	1,000
Gold	1,500
Platinum	2,000

Benefits

EAP customers use their package for **EnCase Product Readiness, Risk & Compliance, Managed Security Services**, or **Digital Forensic & Incident Response** services through a single contract with built in discounted rates:

- Rates are determined by the customer commitment
- Fees are prepaid and expire in 12 months

Outcomes

The EnCase Advisory Program provides the flexibility for our customers to approach their unique needs and requirements under one package.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn

opentext.com/contact