

Cybersecurity Services Handbook

For Cybersecurity Consulting, Managed Services
and Learning Services

Overview.....	3
A. Subscription Packages.....	3
1 Encase Software and Bricata Software Engagement Packages.....	3
2 Cyber Resilience Program (“CRP”).....	4
2.1 CRP Packages.....	4
2.2 CRP Units.....	5
3 Services Program Manager (“SPM”).....	5
4 Technical Account Manager (“TAM”).....	6
5 Cybersecurity Services.....	7
5.1 EnCase and Bricata Software Product Value Services.....	8
5.1.1 EnCase Software Implementation.....	8
5.1.2 EnCase Software Health Check.....	9
5.1.3 EnCase Software Upgrade.....	9
5.1.4 Bricata Deployment or Health Check Assistance.....	10
6 Additional Terms and Conditions Applicable to Cybersecurity Services (except learning services)	11
6.1 Fixed Fee.....	11
6.2 Location of Services and Travel Expenses.....	11
6.3 Duration of Services	11
6.4 Scheduling of Services; Cancellations.....	11
6.5 Regular Business Hours.....	12
6.6 Indemnification.....	12
6.7 Suspension of Services	12
6.8 Customer Responsibilities	12
B. LEARNING SERVICES.....	13
1 Program Specific Terms and Conditions.....	13
1.1 Standard Classes	13
1.2 Flex Training Package Program (“FTP”).....	13
1.3 On Demand Classes.....	15
1.4 OpenText Learning Subscription, Security Edition - Premium.....	15
1.5 OpenText Learning Subscription, Security Edition	16
1.6 Security Edition Premium Subscription Upgrade Program	17
1.7 Security Edition Subscription Upgrade Program	17
1.8 Security Edition Premium Subscription Transfer Program	18
1.9 Security Edition Subscription Transfer Program.....	18
1.10 Bricata Training Student Passes	18
2 Additional Terms and Conditions Applicable to Learning Services Packages.....	19
2.1 Enrollee’s Responsibilities.....	19
2.2 Ownership and Protection of Intellectual Property Rights	20
2.3 Privacy	20
2.4 No Warranties; No Indemnities.....	20
About OpenText.....	22

Overview

Open Text Corporation and its Affiliates (“OpenText” or “OT”) provide consulting services, managed services, and learning services for its Cybersecurity software, and also provide risk and compliance advisory services, digital forensic and incident response services, and managed security services through OT’s Professional Services group (“OT PS”). These services (“Cybersecurity Services”) are subscribed to on an applicable order form by OT’s customers (“Customer(s)”) as further described below. The Cybersecurity Services are governed exclusively by the terms and conditions as set forth in this handbook (“Handbook”) and the then-current version of the applicable OT Professional Services Agreement (the “PSA”, available upon request or at www.opentext.com/agreements) (collectively, the “Services Terms”), which are hereby incorporated into this Handbook by reference.

Your purchase of Cybersecurity Services or the commencement of performance shall constitute your acceptance of the Handbook and the Services Terms. Capitalized terms referenced in this Handbook but not defined herein shall have the meaning ascribed to them in the PSA; this Handbook shall be considered a SOW as that term is used in the PSA. In the event of any inconsistency or conflict between the terms and conditions of this Handbook, the PSA, and any other negotiated, signed agreement between OT and Customer, this Handbook shall prevail but only with respect to the Cybersecurity Services to be provided hereunder, but not for any additional or different terms that specifically reference the section(s) of this Handbook to be overwritten.

OT may utilize OT or non-OT software in connection with providing Cybersecurity Services hereunder. No rights whatsoever to such software are granted to Customer hereunder, and to the extent Customer requires a license, Customer must obtain a license separately and use per the applicable license terms for such software.

A. Subscription Packages

1 Encase Software and Bricata Software Engagement Packages

OT provides a fixed fee engagement model with OT PS for implementation, upgrades, and health checks for EnCase software or OpenText Network Detection & Response (“Bricata”) software through subscription packages. Engagements are staffed by qualified OT PS resources for delivery of the services related to EnCase software or Bricata software. Engagements are assigned and staffed by a Services Program Manager (“SPM”) devoted to managing the Customer relationship with OT, coordinating delivery of services (including scheduling) and engagement reporting (including available budget). See Section 3 for more details on the SPM. Customer acknowledges that the Cybersecurity Services contemplated in this Section 1 are contingent upon Customer maintaining its status as a duly licensed customer of the applicable OT software.

Customers can subscribe to an EnCase software or Bricata software engagement package by ordering from OT the following OT product codes:

Product code	Engagement Package	Tasks & Deliverables
1000050843 1000050844	<ul style="list-style-type: none"> • EnCase software upgrade, or • EnCase software health check 	See Section 5.1.2 for health check package and Section 5.1.3 for upgrade package.
1000050845	<ul style="list-style-type: none"> • EnCase Endpoint Investigator software implementation 	See Section 5.1.1 for implementation package.
1000050846	<ul style="list-style-type: none"> • EnCase Endpoint Security software implementation, or • EnCase Information Assurance software implementation 	See Section 5.1.1 for implementation package.
1000064208	<ul style="list-style-type: none"> • Bricata deployment or health check Assistance 	See Section 5.1.4 for deployment or health check package.
1000067800	<ul style="list-style-type: none"> • EnCase Endpoint Investigator software implementation, and • EnCase Information Assurance software implementation 	See Section 5.1.1 for implementation package.

2 Cyber Resilience Program (“CRP”)

2.1 CRP Packages

CRP (formerly known as EnCase Advisory Program or EAP) is a program-based engagement model with OT PS for Cybersecurity Services defined in Section 5, available through subscription to packages set out in the table below (“CRP Packages”) corresponding to a set number of CRP Units (as described in Section 2.2), usable over a 1-year term. Customers may subscribe to additional CRP Packages, with each package having its own 1-year term. CRP Packages are assigned to and staffed by a SPM devoted to managing OT’s relationship with the Customer, coordinating delivery of Cybersecurity Services (including scheduling), and reporting on the CRP (including available budget). See Section 3 for more details on the SPM.

Customers can subscribe to an CRP Package by ordering from OT at least one of the following OT product codes:

Product code	CRP Package	Units
1000056024	Cyber Resilience Program – CRP20 – 1-Year Term	20
1000056025	Cyber Resilience Program – CRP40 – 1-Year Term	40
1000056026	Cyber Resilience Program – CRP80 – 1-Year Term	80

Product code	CRP Package	Units
1000051021	Cyber Resilience Program – Standard– 1-Year Term	150
1000051022	Cyber Resilience Program – Enhanced– 1-Year Term	250
1000045654	Cyber Resilience Program – Bronze– 1-Year Term	500
1000045655	Cyber Resilience Program – Silver– 1-Year Term	1,000
1000051023	Cyber Resilience Program – Gold– 1-Year Term	1,500
1000045653	Cyber Resilience Program – Platinum– 1-Year Term	2,000
1000067862	Cyber Resilience FasTrak – 1-Year Term	80

2.2 CRP Units

CRP Packages are sold with a fixed number of “Units” as indicated in the table in Section 2.1. Each Unit is convertible into a corresponding number of service hours depending on the specific task requested to be performed by OT resources. Tasks performed by a SPM consume 0.86 Units per hour of work performed. Tasks performed by other resources consume Units at a rate of 1 Unit per hour of work performed, except when tasks related to an incident or breach response. Incident or breach response-related services consume Units at a rate of 1.38 Units per hour of work performed.

2.3 Cyber Resilience FasTrak

The Cyber Resilience FasTrak is equivalent to a CRP Package consisting of 80-units (i.e. equivalent to Product code 1000056026) where the Cybersecurity Services are limited to: (i) Security Health Check, (ii) Threat Hunting Service, (iii) Incident Response Simulation (a.k.a. Table Top Exercise), or (iv) other Cybersecurity Service listed on the order form.

3 Services Program Manager (“SPM”)

The SPM is a foundational component of the Services and delivery by OT of Cybersecurity Services (except learning services). The SPM will act as primary point of contact for OT during the term of the applicable engagement with OT. For Cybersecurity Services provided under an CRP, the SPM will consume a minimum of 1% of purchased Units or 1 Unit, whichever is higher, for each calendar month during the term of an CRP.

The SPM's responsibilities are set forth below:

- Cybersecurity Services liaison for Customer with OT
- Engagement kick-off planning and hosting
- Engagement issues and escalation management
- Engagement Status Calls
- Engagement planning (including project plan delivery, as appropriate)

- OT resources scheduling
- Represent OT at Customer internal meetings
- Engagement budget and delivery timeline reporting

4 Technical Account Manager (“TAM”)

The TAM is an OT PS resource providing advice, guidance and assistance to the Customer with deployment and operationalization of the OpenText Cybersecurity software. TAM is provided as a coverage-based engagement model with OT PS on a part time basis (up to 8-hours per week).

The TAM responsibilities are those set forth for the SPM (see Section 3) and as set forth below:

- Operations & Weekly Health Monitoring, Issue Identification and Remediation. The TAM will help conduct weekly health checks and assist with the mitigation and remediation of OpenText Cybersecurity software issues. All tasks, findings and remediations will be tracked and reported during cadence calls (i.e., bi-weekly status calls and quarterly business reviews).
- Priority Support - All support tickets will be prioritized and tracked by the TAM, who will act as a single point of contact for their resolution.
- Ongoing Deployment Support - Design and deployment guidance as Customer attack surface coverage is expanded and the environment changes. The TAM will serve as subject matter expert for the software.
- Integration - Review policy management to facilitate the successful integration of OpenText Cybersecurity software and related data sources to the Customer’s environment and other collection and analysis engines.
- Custom Content & Workflow Support - Support of purpose-built content to address custom use-cases and monitoring objectives for OpenText Cybersecurity software used for security operations. The TAM will provide technical expertise and support, as appropriate, new threat detection content, threat intelligence instrumentation, automation of analysis tasks, statistics, and profiling as well as the implementation of external plugins.
- On-the-Job Knowledge Transfer - Continuous coaching for Customer resources through informal cross-training events with Customer’s security operations, incident response or other cybersecurity resources. The TAM will regularly provide ad-hoc training to Customer resources in the management and usage of the OpenText Cybersecurity software.
- Documentation – The TAM will document, through interactions with the Customer resources, its understanding of the customer’s infrastructure, the OpenText Cybersecurity software deployment, the security program, the business needs to help increase the business value of the software and accelerate any issue resolution processes.
- Advocacy – The TAM will act as an advocate to ensure Customer’s priorities are visible and understood within OT, including OT’s software engineering and technical support departments.

Customers can obtain coverage from TAM by ordering from OT at least one of the following OT product codes:

Product code	TAM Coverage
1000064206	Technical Account Manager (TAM) - 90-Days

Product code	TAM Coverage
1000064197	Technical Account Manager (TAM) - 1-Year
1000064910	Technical Account Manager (TAM) – 30 Day

Service Assumptions

- Product code 1000064910 can only be obtained on an order combined with another product code in the table, above in this Section.
- Coverage starts upon purchase and is non-refundable.
- Purchasing multiple product codes on a single order does not cause multiple concurrent coverages, but rather additive single coverage. For example, purchasing a 90-day TAM and a 30-day-TAM on an order would result in a 120-day total concurrent coverage period from purchase.
- Customer purchasing product codes while under active coverage would not cause multiple concurrent coverages, but rather an extended single coverage. For example, a Customer active under a 1-year TAM who purchases another 1-year TAM would result in an extension of coverage for a total of 2-years.
- TAM will only provide coverage one (1) OpenText software during the term. Notwithstanding the previous two assumptions, OT can specifically allow purchasing of multiple TAMs, in writing on the order form at time of purchase.
- TAM weekly availability cannot be carried over to subsequent weeks.

5 Cybersecurity Services

OpenText provides security services for the OpenText Cybersecurity software (*i.e.*, product value), as well as risk and compliance advisory services, digital forensic and incident response services, and managed security services through OT PS. For more information on these professional services, contact OpenText, visit our website, or refer to the short list below:

Product Value	Risk & Compliance Advisory	Digital Forensics & Incident Response	Managed Security Services
<u>Value Realization</u> Solution Design, Implementation, Customization, and Integrations	Security Assessment / Security Health Check / ECS Security Assessment	DFIR Retainer	Managed Threat Detection & Response
<u>Value Optimization</u> Managed Services, Optimization Workshop, Migration, Health Checks, and Upgrades	Privacy Capabilities Assessment	Breach Response / Incident Response / Insider Threat Investigation	Managed SOC / Managed Threat Hunting

Product Value	Risk & Compliance Advisory	Digital Forensics & Incident Response	Managed Security Services
Value Discovery Strategy, Advisory Services, Cloud Transformation Workshops	Security and Incident Response Training Tabletop Exercises	Malware Analysis and Reverse Engineering	eDiscovery Case Management
Value+ Services Accelerated Innovation, End-to-End Outcome Orientation & Assistance, Flexibility Through Agility	Incident Response Readiness	Vulnerability Scanning and Penetration Testing	Managed Breach Review

5.1 EnCase and Bricata Software Product Value Services

Product Value Services (formerly known as Product Readiness Services) are designed to advise, guide, and assist Customers throughout the lifecycle of their OpenText Cybersecurity software. These services include implementation, upgrades, health checks, operational and managed services, advisory and other services related to of EnCase software or Bricata software.

EnCase software implementation, health checks and upgrades can be procured as (a) a fixed fee EnCase Software Package (see Section 1), which is limited to the tasks and deliverables defined in sections 5.1.1, 5.1.2 and 5.1.3, as appropriate, or (b) as an CRP Package (see Section 2.1). Bricata software implementation or health check can be procured as (a) a fixed fee Bricata Software Package (see Section 1), which is limited to the tasks and deliverables defined in section 5.1.4; or (b) as an CRP Package (see Section 2.1). Other Product Readiness Services can be procured as CRP (see Section 2).

5.1.1 EnCase Software Implementation

Designed to assist Customers with initial implementation of EnCase software, this Service includes the following tasks and deliverables:

- Two (2) planning meetings with OT designated resources and key Customer stakeholders, facilitated by the SPM:
 - (i) an engagement kick-off for OT set out its implementation service and to gather required information for kick-off deliverables, and
 - (ii) a technical discussion for Customer to fully brief OT resources on network infrastructure and deployment requirements.
- Documented Customer technical requirement for the EnCase software.
- Engagement roster of OT and Customer resources
- Project plan
- Hardware and software pre-requisites for Customer
- Documented Customer network infrastructure and EnCase software deployment requirements

- Documented recommendations, including processing environments, storage configurations and location of software components (including Examiners, SAFEs and databases).
- Implementation of core EnCase software components, up to two (2) SAFEs and five (5) examiners, on agreed target servers and workstations, deployment of agent on limited endpoints for testing purposes, and setup of EnCase connectors to repositories and file shares.
- Operational performance testing and data storage configuration review.
- Two (2) Value Discovery (Knowledge Transfer) sessions, up to 2-hours each
- Implementation report, including inventory of components installed and operational testing results.

Service Assumptions

- Customer sign-off on project plan, pre-requisite provisioning, recommendations and other planning deliverables required within 5 business days of delivery.
- Customer must provide pre-requisites within 10 business days of reception by OT.
- Customer failure to complete either of the above may result in schedule delays and/or increased in CRP units allocated to a project.
- OT will run concurrent projects for customers who purchased product code 1000067800.

5.1.2 EnCase Software Health Check

Designed to assist the Customer with proactive identification of potential configuration problems and usage of the EnCase software, this service includes the following tasks and deliverables:

- Kick-off meeting
- Validation of current deployment configuration
- Identification of current client objectives to improve effectiveness of EnCase software
- Testing of key components and configurations
- Summary of health check scope, testing/validation objectives, and associated results and recommendations.

Service Assumptions

- Customer sign-off on project plan, pre-requisite provisioning, recommendations and other planning deliverables required within 5 business days of delivery.
- Limited to implementation with no more than two (2) EnCase SAFEs and five (5) examiners.

5.1.3 EnCase Software Upgrade

Designed to assist Customer with the upgrade Encase software components, this service includes the following tasks and deliverables:

- Kick-off meeting
- Upgrade assessment, reviewing current system configuration (hardware, modules, index, database, patches, client components, integrations) for compatibility with target Encase software version.
- Documented recommendations for system improvements, including identifying optimal processing environments and storage configurations and recommending placement of core software components (Examiners, SAFEs, databases) on target machines.
- Implementation of core EnCase software components, up to two (2) SAFEs and five (5) examiners, on agreed target servers and workstations, deployment of agent on limited endpoints for testing purposes, and setup of EnCase connectors to repositories and file shares.
- Operational performance testing and data storage configuration review.

- Two (2) Value Discovery (Knowledge Transfer) sessions, up to 2-hours each
- Implementation report, including inventory of components installed and operational testing results.

5.1.4 Bricata Deployment or Health Check Assistance

Designed to provide Customer with up to 4-hours of assistance with Bricata software within a single remote work session. OT PS can perform a health check, perform an assessment of deployment best practices, perform a data tuning needs analysis, perform an integration configuration analysis, provide advice on network detection and response, troubleshoot a deployment, build documentation, or provide sensor deployment assistance. Customer can request the remote work session for these tasks through the SPM. This service includes the following deliverables:

- A report summarizing the tasks performed by OT PS and documenting any findings and recommendation.

Service Assumptions

- Customer must provide any required log bundles generated by the Bricata software (or any sensor devices) in advance of any tasks by OT PS.
- Customer must have, during the remote work session with OT PS, active participation by resource with administrator level access to the Bricata software GUI and CLI and by an IT networking expert familiar with Customer's infrastructure.
- System is deployed in some manner, licensed, etc.
- Customer acknowledges that 4-hours provided under this package may be insufficient to complete tasks, especially on very complex or large deployments. Customer may purchase an CRP Package (see Section 2.1) for additional work.
- Training in "side-by-side" fashion is excluded from Cybersecurity Services.
- Any advice, guidance and assistance (including troubleshooting) related to hardware matters are excluded from the Cybersecurity Services.

6 Additional Terms and Conditions Applicable to Cybersecurity Services (except learning services)

6.1 Fixed Fee

Notwithstanding anything to the contrary in the applicable PSA, and unless separately agreed in writing, Cybersecurity Services are provided on a fixed fee basis, as quoted by OT or as set forth within an applicable order form and are payable in advance.

6.2 Location of Services and Travel Expenses

Cybersecurity Services are delivered remotely from OT locations by OT resources, through customer provided connectivity between OT's internet point of presence and Customer's environment. Customer and OT may mutually agree to OT delivering from an alternate location by executing a mutually agreed change request. In such case, OT will invoice Customer for all pre-approved travel related expenses and travel time.

6.3 Duration of Services

Cybersecurity Services subscribed as an CRP Package must be used within one (1) year from the effective date of Customer's purchase. The Encase Software and Bricata Software Engagement Packages must be used within six (6) months from the effective date of Customer's purchase. If Customer fails to use these services within the applicable time period, any balance paid for such services shall be forfeited and will not be refunded by OT or applied to future Services orders.

6.4 Scheduling of Services; Cancellations

OT will schedule Cybersecurity Services in consecutive days based on Regular Business Hours and OT's standard delivery methodologies. OT requires confirmation of an-agreed upon performance schedule at least ten (10) days prior to commencement of remote Services, at least ten (10) days prior to onsite Services of OT consultants within the continental U.S., and at least fifteen (15) days prior confirmation for international onsite Services. If Customer confirms the start date but re-schedules or cancels such start date within ten (10) calendar days of such start date, OT reserves the right to (a) invoice Customer (and Customer agrees to pay such invoice) for OT's actual costs incurred as a result of such re-scheduling or cancellation, and (b) assess fifty percent (50%) of the number of CRP Units associated with the rescheduled or canceled activity, if OT, after making commercially reasonable efforts to do so, is unable to re-allocate the scheduled consultant(s) to another engagement during the scheduled dates.

6.5 Regular Business Hours

Unless otherwise agreed between OT and Customer, work shall be performed between the hours of 9am to 6pm (consultant's time zone location or local time zone for Alternate Locations), Monday to Friday, except public holidays ("Regular Business Hours").

OT schedules its resources by 2-hour increments, up to 8 hours per day during Regular Business Hours for work from OT locations. For Alternate Locations, OT schedules its consultants in 8-hour increments.

Services outside Regular Business Hours must be agreed in writing (email is sufficient) by OT and Customer. Customer hereby agrees that OT may charge additional amounts for Services to be performed on an urgent basis or outside Regular Business Hours. For CRP, the rates in Section 2.2 are valid for work within Regular Business Hours. Rates for any work outside Regular Business Hours are 1.5-times the rate(s) in Section 2.2 for work on weekdays, and 2.0-times the rate(s) in Section 2.2 for work on weekends and public holidays.

OT will schedule services in consecutive days based on Regular Business Hours and OT's standard delivery methodologies.

6.6 Indemnification

Customer will defend, indemnify and hold OT (and its officers, directors, agents and employees) harmless from any and all losses, liabilities, suits, damages, claims, demands, and expenses (including, without limitation, reasonable attorneys' fees)(collectively, "Claims"), whether based on contract, tort (including strict liability) or crimes, resulting from a claim by a third party (for clarity, the term "third party" includes but is not limited to a government entity, as well as Customer employees and agents) based on actions by OT undertaken upon the instructions of Customer, either as set forth in herein or as subsequently communicated to OT. The foregoing is in addition to any indemnification obligations set forth in the PSA.

6.7 Suspension of Services

In addition to any termination rights in the PSA, Customer agrees that OT shall have a right to notify law enforcement and terminate Services if, during the performance of the Services, OT (a) observes information that, in the opinion of OT, may constitute child pornography, (b) believes in its opinion that continued performance of the Services will commit or aid and abet any crime, or (c) discovers evidence of the planning of a future crime, OT shall (i) immediately notify Customer of such evidence and (ii) have a right to discontinue performance of Services and/or immediately terminate Services, without liability or penalty.

6.8 Customer Responsibilities

Customer shall ensure that OT has the necessary rights and credentials to (i) access its computing environment, inclusive of the OT Software operating within such environment, and (ii) perform the Services contemplated herein at no charge or expense to OT in accordance with the PSA.

6.9 Customer Responsibilities

When OT provides digital forensic and incident response services, it may use SentinelOne™ software. The Customer acknowledges and agrees to the customer license for SentinelOne published at <https://www.sentinelone.com/legal/limited-use-ir-license-agreement/>. Customer also authorizes OT to communicate contact information to SentinelOne and understands that SentinelOne may solicit their business for their software products. OT shall limit all use of SentinelOne™ software to no more than forty-five (45) days for any single Customer. Once OT uses SentinelOne™ software for a single engagement with the Customer, OT will require approval from SentinelOne for any subsequent use.

B. LEARNING SERVICES

These Terms and Conditions for enrollment in any OT software training class ("Terms") set forth the basis upon which OT will provide enrollee ("Enrollee") training classes using EnCase software or OpenText Network Detection and Response ("Bricata") software course materials ("EnCase Course Materials"). Your purchase of, attendance at, or use of any educational materials related to, a training class constitutes your agreement to these Terms in regard to such training class.

1 Program Specific Terms and Conditions

1.1 Standard Classes

Classes must be taken within 12 months of purchase date. Failure to take a class within 12 months of purchase will forfeit the fees paid. Tuition may be refunded up to 60 days after purchase date for unused classes.

1.2 Flex Training Package Program ("FTP")

- The FTP minimum purchase is five seats.
- Each individual attending a course will use one seat. Individuals attending multiple courses will use one seat per class.
- FTP seats may be used by any combination of people, but the FTP is not unlimited access to training courses.
- FTP seats are valid for 12 months. Unused FTP seats will be forfeited upon expiration.
- FTP seats may be used for any and all EnCase courses, provided that the prerequisites are met.
- FTP seats are only valid for classroom training at OT-owned training facilities in Pasadena, CA (Los Angeles, CA); Gaithersburg, MD (Washington, DC); and Reading, UK.
- FTP seats may be used for any and all EnCase® Training OnDemand courses, provided that the prerequisites are met.

- FTP seats may be used for any and all EnCase® Training vClass courses, provided that the prerequisites are met.
- FTP seats do not cover certification testing fees.
- All purchases are final, and there are no refunds or exchanges.

Please note: Registrations are not guaranteed; a class may be full or cancelled due to lack of enrollments. No discounts are available. The FTP Program cannot be combined with any other offer or program. This program is not offered at our Authorized Training Partners.

1.3 On Demand Classes

- Students have 60 days to complete each course. The 60-day period begins when the student has logged in and started viewing the online course content.
- OnDemand course manuals are only available in non-printable timed eBook format, physical manuals cannot be provided. The DRM program will prevent the manual from being printed or copied.
- Students must return unused materials within 60 days from the date of purchase to be eligible for a refund. All materials must be returned in resalable condition.
- The OpenText Learning Subscription, Security Edition and the OpenText Learning Subscription, Security Edition - Premium Subscription may be used for any of our Training OnDemand classes, provided that the holder meets the course prerequisites. Students may only be concurrently enrolled in two Training OnDemand classes.
- After purchasing an individual course, students have 12 months to use their Training OnDemand course credit (or for Annual Training Subscription holders, until the Subscription expires). Any unused credits will be forfeited after 12 months or when the Subscription expires.
- EnCase Training OnDemand students receive an electronic version of the same EnCase® certificate of completion as students participating in classroom training.
- Currently CPE credit is not available for Training OnDemand courses.

1.4 OpenText Learning Subscription, Security Edition - Premium

- Security Edition Premium Subscription orders will be processed when payment or pre-payments are received. The life of the Subscription will begin either when the first class is taken or 30 days from the order date, whichever comes first, and will run for one year.
- The name and e-mail address of the person who will be using the Subscription must be provided prior to order date.
- Security Edition Premium Subscription are transferable only under the Security Edition – Premium Subscription Transfer Program. A transfer fee may apply.
- Subscriptions may be used for any and all EnCase courses, provided that the prerequisites are met.
- Subscriptions are only valid for classroom training at OT-owned training facilities in Pasadena, CA (Los Angeles, CA); Gaithersburg, MD (Washington DC); and Reading, UK.
- Subscriptions may be used for any and all EnCase® Training OnDemand courses, provided that the prerequisites are met. Students may only be concurrently enrolled in two Training OnDemand courses.
- OnDemand course manuals are only available in non-printable timed eBook format, physical manuals cannot be provided. The DRM program will prevent the manual from being printed or copied.
- Subscriptions may be used for any and all EnCase® Training vClass courses, provided that the prerequisites are met.
- Subscriptions do not cover certification testing fees.
- Students enrolled in EnCase Training vClass courses will be responsible for returning any training materials received should they cancel from the class without rescheduling. Failure to return training materials from student-cancelled EnCase Training vClass courses will result in a cancellation fee.
- All purchases are final and there are no refunds or exchanges.

Please note: Registrations are not guaranteed; a class may be full or cancelled due to lack of enrollments. No discounts are available. The Subscription Programs cannot be combined with any other offer or program. This program is not offered at our Authorized Training Partners.

1.5 OpenText Learning Subscription, Security Edition

- Security Edition Subscription orders will be processed when payment or pre-payments are received. The life of the Subscription will begin either when the first class is taken or 30 days from the order date, whichever comes first, and will run for one or two years.
- The name and email address of the person who will be using the Security Edition Subscription must be provided prior to order date.
- Security Edition Subscriptions are transferable only under the Subscription Transfer Program. Logging into a course and partial viewing will consider the subscription as used.
- Security Edition Subscriptions may be used for any and all EnCase® Training Security Edition courses, provided that the prerequisites are met.
- OnDemand Subscriptions may be used to take any and all EnCase® Training Security Edition courses, one time each.
- Students may only be enrolled in two EnCase Training OnDemand courses concurrently.
- Security Edition course manuals are only available in non-printable timed eBook format, physical manuals cannot be provided. The DRM program will prevent the manual from being printed.
- Security Edition Subscriptions do not cover classroom courses or EnCase® Training vClass courses.
- Security Edition Subscriptions cannot be used for private onsite training classes.
- Security Edition Subscriptions do not cover certification testing fees.
- All purchases are final and there are no refunds or exchanges.

Please note: Registrations are not guaranteed; a class may be full or cancelled due to lack of enrollments. No discounts are available. The Subscription Programs cannot be combined with any other offer or program. This program is not offered at our Authorized Training Partners.

1.6 Security Edition Premium Subscription Upgrade Program

- Only individuals who purchased the single tuition of a course (OT classroom, OnDemand, or vClass courses) are eligible for the Subscription Upgrade program.
- Security Edition Premium Subscription Upgrades must be purchased within 30 days of the original course.
- Security Edition Premium Subscription Upgrades will run for one year from Upgrade purchase date.
- Security Edition Premium Subscription Upgrades are not transferrable and may only be used by the student who attended the original course.
- Security Edition Premium Subscription may be used for any and all EnCase courses, provided that the prerequisites are met.
- Security Edition Premium Subscription are only valid for classroom training at OT-owned training facilities in Pasadena, CA (Los Angeles, CA); Gaithersburg, MD (Washington DC); and Reading, UK.
- Security Edition Premium Subscriptions may be used for any and all EnCase® Training OnDemand courses, provided that the prerequisites are met. Students may only be concurrently enrolled in two Training OnDemand courses.
- Security Edition Premium Subscriptions may be used for any and all EnCase® Training vClass courses, provided that the prerequisites are met.
- Security Edition Premium Subscriptions do not cover certification testing fees.
- Students enrolled in EnCase Training vClass courses will be responsible for returning any training materials received should they cancel from the class without rescheduling. Failure to return training materials from student-cancelled EnCase Training vClass courses will result in a cancellation fee.
- All purchases are final and there are no refunds or exchanges.

Please note: Registrations are not guaranteed; a class may be full or cancelled due to lack of enrollments. No discounts are available. The Subscription Programs cannot be combined with any other offer or program. This program is not offered at courses taught by our Authorized Training Partners and may not be sold through resellers.

1.7 Security Edition Subscription Upgrade Program

- Only individuals who purchased the single tuition of a course (OnDemand courses) are eligible for the Security Edition Subscription Upgrade program.
- Subscription Upgrades must be purchased within 30 days of the original course.
- Subscription Upgrades will run for one year from Upgrade purchase date.
- Subscription Upgrades are not transferrable and may only be used by the student who attended the original course.
- Security Edition Subscriptions may be used for any and all EnCase® Training OnDemand courses, provided that the prerequisites are met. Students may only be concurrently enrolled in two Training OnDemand courses.
- Security Edition Subscriptions do not cover certification testing fees.
- All purchases are final and there are no refunds or exchanges.

Please note: Registrations are not guaranteed; a class may be full or cancelled due to lack of enrollments. No discounts are available. The Subscription Programs cannot be combined with any other offer or program. This program is not offered at courses taught by our Authorized Training Partners and may not be sold through resellers.

1.8 Security Edition Premium Subscription Transfer Program

- Unused Security Edition Subscriptions can be transferred at no cost. Security Edition Premium Subscriptions which have been used can also be transferred, but a transfer fee will apply.
- Transferred Security Edition Subscriptions may be used for any and all EnCase courses, provided that the prerequisites are met.
- Transferred Security Edition Subscriptions are only valid for classroom training at OT-owned training facilities in Pasadena, CA (Los Angeles, CA); Gaithersburg, MD (Washington DC); and Reading, UK.
- Transferred Security Edition Subscriptions may be used for any and all EnCase® Training OnDemand courses, provided that the prerequisites are met. Students may only be concurrently enrolled in two Training OnDemand courses.
- Transferred Security Edition Subscriptions may be used for any and all EnCase® Training vClass courses, provided that the prerequisites are met.
- Transferring a Security Edition Subscription does not extend the current term of the Security Edition Subscription. The expiration date of the Security Edition Subscription shall remain the same as the original term.
- Transferred Security Edition Subscriptions do not include certification testing fees.
- Students enrolled in EnCase Training Class courses will be responsible for returning any training materials received should they cancel from the class without rescheduling. Failure to return training materials from student-cancelled EnCase Training Class courses will result in a cancellation fee.
- All purchases are final and there are no refunds or exchanges.

1.9 Security Edition Subscription Transfer Program

- Unused Security Edition Subscriptions can be transferred at no cost. Subscriptions which have been used can also be transferred, but a transfer fee will apply.
- Transferred Security Edition Subscriptions may be used for any and all EnCase® Training OnDemand courses, provided that the prerequisites are met. Students may only be concurrently enrolled in two Training OnDemand courses.
- Transferring a Security Edition Subscription does not renew the current term of the passport. The expiration date of the subscription shall remain the same as the original term.
- Transferred Security Edition Subscriptions do not cover certification testing fees.
- All purchases are final and there are no refunds or exchanges.

1.10 Bricata Training Student Passes

Customers can purchase student passes to Bricata software training, delivered during an event organized by the Customer and led by an OT authorized instructor (subject to availability), defined in the table, below, and subject to these terms and conditions:

- Training events must occur on consecutive business days, except instructor's holidays.
- Each individual attending a training event requires usage of one (1) student pass.
- Each training event requires usage of four (4) student passes at a minimum.
- A training event may not exceed twelve (12) individuals.

- Customer is solely responsible for student passes usage. Instructor may stop a training event if attendance could cause an overage in student passes usage or exceeds the maximum number of individuals. In such case, Customer will forfeit usage of the student passes.
- Student passes expire 360-days from purchase.
- Student passes are non-refundable.
- Student passes do not include certification or accreditation.

Course title and description	Product code
<p><u>Bricata Specialist Training (BST)</u></p> <p>This one-day training event provides students with the basics of network monitoring methodology, deployment architecture and installation, policy management, alert management, and threat hunting workflow. Students spend time working with an OT authorized instructor through classroom modules as well as labs designed to provide hands on experience deploying Zeek scripts, Suricata policies, tuning alerts, and working with network metadata to perform basic proactive threat hunting activities.</p>	<ul style="list-style-type: none"> • 4 Student Pass: 1000064203 • 12 Student Pass: 1000064207
<p><u>Bricata Advanced Countermeasures Training (ACT)</u></p> <p>This two-day training event provides continues to build on the foundation laid in BST to enable students to leverage the Bricata software to build detections for behaviors in their environment. The event starts with students receiving in-depth instruction on the major components and concepts related to Bricata software's two primary network traffic classification engines, Suricata and Zeek. Then, the students will go through a guided lesson on threat hunting to develop a framework to find behaviors and build detections. After a review of each component's policy management interface, instruction will turn to the real-world scenarios where students will work through OT authorized instructor- guided exercises to detect threats and satisfy use-cases common to the operational use of the Bricata software.</p>	<ul style="list-style-type: none"> • 4 Student Pass: 1000064166

2 Additional Terms and Conditions Applicable to Learning Services Packages

2.1 Enrollee's Responsibilities

Enrollee shall satisfy the requirements for software training class as published or provided to Enrollee by OT prior to the start of such course. If Enrollee fails to do so, no refund or cancellation fee will be paid. Enrollee shall exhibit good conduct; OT reserves the right to refuse, limit or cancel any software training class if Enrollee in the opinion of OT has displayed unreasonable behavior or is deemed to be violent, abusive or disruptive. In such cases no refund or cancellation fee will be paid. Enrollee agrees that all

facilities and equipment licensed for use during the software training class shall at the end of the Software Training Class be in the same condition as initially provided, wear and tear excepted. Software Training Classes that are taught online require streaming Internet to deliver the appropriate classroom experience to the remote user. The quality and stability of the connection can be impacted by the bandwidth available to the user. OT recommends using a wired Internet connection for online classes, or a Wi-Fi connection that is capable of sustaining a minimum of a 5MB download/upload speed. OT is not responsible for the quality of video or for lost connections based on the Internet connection or capability of the student.

2.2 Ownership and Protection of Intellectual Property Rights

In addition to any intellectual property rights provisions set forth in the PSA, OT shall retain all intellectual property rights to the Software Training Class including any documentation, materials or other information provided therein (the “Software Training Class Materials”) and does not grant any rights in its intellectual property rights, except the right of Enrollee to attend and participate in the software training class, as described above. The Enrollee may not rent, disclose, lease, sublicense, assign, loan, sell, copy, or distribute any part of the Software Training Class or the Software Training Class Materials or make any other use of the Software Training Class or the Software Training Class Materials except his or her attendance at and participation in one training session of a Software Training Class. Enrollee shall have the limited right to use EnCase Course Materials solely for educational purposes. Enrollee agrees not to use recording equipment in any class without OT’s prior written consent.

2.3 Privacy

OT values and respects Enrollee’s privacy pursuant to OT’s Privacy Policy, available at <https://www.opentext.com/about/copyright-information/site-privacy>. Notwithstanding the forgoing, OT shall have no liability for disclosing information relating to the Enrollee which is: (i) already publicly known; (ii) discovered or created by OT without reference to Enrollee’s private information, as shown in records of OT; (iii) otherwise known to OT through no wrongful conduct of the receiving OT, or (iv) pursuant to a subpoena or equivalent; or (v) required to be disclosed by law or court order. However, OT may disclose Enrollee’s private information hereunder to its agents, attorneys and other representatives or any court of competent jurisdiction or any other party empowered hereunder as reasonably required to resolve any dispute between the parties hereto.

2.4 No Warranties; No Indemnities

THE PARTIES ACKNOWLEDGE THAT THIS IS AN AGREEMENT FOR EDUCATIONAL SERVICES AND THAT OT IS NOT SUPPLYING ANY GOODS. THE SERVICES ARE DELIVERED "AS IS", WITH NO WARRANTIES OF ANY KIND. OPENTEXT PROVIDES NO WARRANTY, EXPRESS, IMPLIED, OR STATUTORY, AND SPECIFICALLY DISCLAIMS ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON- INFRINGEMENT. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY OPENTEXT, ITS DISTRIBUTORS, AGENTS, CONTRACTORS, OR EMPLOYEES SHALL IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY OR DIMINISH THIS DISCLAIMER IN ANY WAY. THIS WARRANTY DISCLAIMER CONSTITUTES AN ESSENTIAL

PART OF THE AGREEMENT BETWEEN THE PARTIES, AND OPENTEXT WOULD NOT BE ABLE TO PROVIDE THE SERVICES WITHOUT SUCH LIMITATIONS.

About OpenText

OpenText enables the digital world, creating a better way for organizations to work with information, on-premises or in the cloud. For more information about OpenText (NASDAQ/TSX: OTEX), visit opentext.com.

Connect with us:

[OpenText CEO Mark Barrenechea's blog](#)

[Twitter](#) | [LinkedIn](#)