Common Criteria and Protection Profiles: How to Evaluate Information

Kathryn Wallace
Common Criteria and Protection Profiles: How to Evaluate Information Technology Security

Kathryn Wallace
Practical Version 1.4b

Summary
The purpose of this paper is to discuss the standards of Common Criteria and the security framework provided by the Common Criteria. In addition, this paper will review the background and applicability of Common Criteria Protection Profiles established to evaluate specific Information Technology (IT) functional and assurance security requirements. The Common Criteria (CC) security framework establishes a methodology to apply security standards to an IT system or product and establishes the understanding of how specific Protection Profiles (PP) fit into the overall CC process.

CC baselines activities for IT systems and products assurance evaluations. Developers, consumers, or evaluators of IT systems and products may use the CC security framework to institute a level of security assurance. This paper will document the CC process and explore its importance to IT security.

Common Criteria Overview
Common Criteria (CC) is the set of internationally and nationally recognized technical standards and configurations that allow for security evaluations of Information Technology (IT) products and technology. The individual set of common criteria technical standards or configurations developed for a specific product or technology is qualified as a protection profile.

The first set of United States Federal technical standards for security evaluations was the DoD Trusted Computer System Evaluation Criteria (TCSEC) commonly referred to as the "Orange Book published in August 1983." Independently, organizations in other countries were developing IT standards for their own governments to use. In June 1993, the sponsoring organizations of the existing US, Canadian, and European criterias started the CC Project to align the separate standards into a single set of IT security criteria.

Figure 1: Common Criteria Source Documents Development

Orange Book (TSEC) v.1985
UK Confidence Levels 1989
German Criteria 1991
French Criteria
ITSEC 1991
Federal Criteria v.1993
Canadian Criteria 1993
Common Criteria V1.0 1996 V2.0 1998
The following seven governmental organizations (collectively called “the Common Criteria Project Sponsoring Organizations”) are joint holders of the copyright of CC for IT security evaluations and retain the right to use, distribute, translate, and modify the CCs they see fit.

Canada: Communications Security Establishment (CSE)
France: Direction Centrale de la Securite des Systemes d'Information (DCSSI)
Germany: Bundesamt für Sicherheit in der Informationstechnik (BSI)
Netherlands: Netherlands National Communications Security Agency (NLNCSA)
United Kingdom: Communications-Electronics Security Group (CESG)
United States: National Institute of Standards and Technology (NIST)
United States: National Security Agency (NSA)

The international community enforces the standards of the CC through the Common Criteria Recognition Arrangement (CCRA), which states that participating members agree to accept the results of CC evaluations performed by other CCRA members.

The National Institute for Standards and Technology (NIST) and the National Security Agency (NSA) jointly operate United States CC activities under the National Information Assurance Partnership (NIAP). NIAP is a U.S. Government initiative designed to meet the security testing needs of both information technology producers and users. The Common Criteria Evaluation and Validation Scheme (CCEVS) was established by NIAP to implement the CCRA compliant evaluation scheme within the US.

**Common Criteria Paradigm**

To effectively implement or evaluate according to the CC standards the security concepts and CC terminology are aligned in a Common Criteria Evaluation and Validation Scheme (CCEVS) hierarchical security framework.

The terminology used in the common criteria process is unique to the process and the semantics are fundamental to understanding the CC activities. The CC terms are requirements of the CC methodology and correspond to steps of the CCEVS security framework.

The first step of evaluating a system or application using common criteria methodology is to identify a Target of Evaluation (TOE). The TOE is a system, application, or IT product that is selected to be evaluated according to CC standards. The second step is to develop a set of Security Targets (ST). The ST is the set of criteria to applied for the evaluation of the TOE. For specific technologies or IT products, previously established protection profiles may be used as the ST criteria.

With each step of the security framework, the CC evaluation process requires increasingly detailed information regarding the application or system security profile.
### Figure 2: Common Criteria Evaluation and Validation Scheme (CCEVS) Security Framework

#### Security Environment
Laws, organizational security policies, etc., which define the context in which the TOE is to be used. Threats present in the environment are also included.

#### TOE – Target of Evaluation
An Information Technology (IT) product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

#### Security Objectives
A statement of intent to counter the identified threats and/or satisfy intended organizational security policies and assumptions.

- **ST - Security Target**: Set of security requirements and specification to be used as the basis for evaluation of an identified TOE. The ST may claim conformance to one or more Protection Profiles (PPs) and forms the basis of the evaluation.

#### TOE Security Requirements
The refinement of the IT security objectives into a set of technical requirements for security functions and assurance, covering the TOE and its IT environment.

- **TSP – TOE Security Policy**: A set of rules that regulate how assets are managed, protected, and distributed within a TOE.

- **SF – Security Function**: A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

- **SFP – Security Function Policy**: The security policy enforced by a SF.

#### TOE Security Specifications
Define an actual or proposed implementation for the TOE.

- **TSF - TOE Security Functions**: As set security functions for all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

- **SOF - Strength of Functions**: Qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.

- **TSC - TSF Scope of Control**: The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

- **TSFI - TOE Interface**: Set of interfaced, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.

#### TOE Implementation
The realization of a TOE in accordance with its specifications.
The resulting product of progressing through the CC Security Framework steps is an IT product or system that meets a baseline set of security criteria and/or processes that institute fundamental security techniques. Specific security mechanisms or techniques for IT products and technology are addressed through the Common Criteria Protection Profiles.

**Applying the Common Criteria**

There are three sections to the Common Criteria (CC) version 2.0. These three sections are Introduction and General Model (section one), Security Functional Requirements (section two), and Security Assurance Requirements (section three). The CC general audience, groups who would apply CC standards, is comprised of IT system or product consumers, developers, and evaluators. The three CC sections provide guidance on how CC establishes baseline security requirements for buying, developing, or evaluating an IT system or product.

The technical specifications of applying IT security are provided in the second and third sections, security functional and assurance requirements, of the CC. These security requirements are grouped into high-level sets of related security requirements defined for the purposes of the CC as classes. The classes of related security requirements are unique to the either security functional requirements or security assurance requirements. Functional and assurance requirement classes guide consumers, developers, and evaluators on how to apply the security requirement components to meet security policy or counter threats.

**Section One – Introduction and General Model**

Security defines information technology attributes and assurance mechanisms for protecting the confidentiality and integrity of information, and availability of critical services. Common Criteria proposes that all security specifications and requirements should come from a general security context that protects assets from threats and categorizes these threats in accordance to their potential.

The CCEVS security framework establishes a logical progression where a security environment is described (e.g. TOE) and then security objectives are determined based on the indicated security environment (e.g. ST). The TOE security function, TSF, is the set of information technology attributes and assurance mechanisms that support individual security function policies (SFP). Essentially, the TSF is the functional and technical logic built into the TOE system or technology required to meet established TOE security requirements or policy (e.g. TSP).

The confidentiality, integrity, and availability of the system are enforced through the security specifications of the TOE. The strength and scope of the security mechanisms are designed and implemented to secure the TOE Interface (TSFI).

While the steps of the CCEVS security framework progressively detail the TOE environment and require security objectives to be established, it does not fully
explain the detailed security configuration requirements for a TOE operational and production environment. The CC general model of the TOE establishes the logical interdependencies of security policies and the security functions to establish the technical expression of security techniques (e.g. TSF).

The TSF security techniques provide the mechanism by which users access and interface with the TOE. The TOE Security Function Interface (TSFI) is the layer of the TOE where users, either human users or remote IT products gain access into the TOE environment.

**Figure 3: Common Criteria “TOE” General Model**

---

**Section Two – Security Functional Requirements**

The security functional requirements establish a set of functional components (e.g. classes) as a standard to express the TOE security functional requirements. Consumers, developers, and evaluators use these functional requirements as guidance and for reference when developing and interpreting security function
statements, formulating functional TOE specifications, and assessing compliance of a TOE to the required security functions.\textsuperscript{xii}

The eleven classes of security functional requirements including the CC class short name and purpose are:

\textbf{Security Audit} (FAU) – monitor, capture, store, analyze, and report information related to security event.\textsuperscript{xiii}

\textbf{Communication} (FCO) – Assure the identity of originators and recipients of transmitted information; non-repudiation.\textsuperscript{xiv}

\textbf{Cryptographic Support} (FCS) – Management and operational use of cryptographic keys.

\textbf{User Data Protection} (FDP) – Protect user data and the associated security attributes within a TOE and data that is imported, exported, and stored.\textsuperscript{xv}

\textbf{Identification & Authentication} (FIA) – Ensure unambiguous identification of authorized users and the correct association of security attributes with users and subjects.\textsuperscript{xvi}

\textbf{Security Management} (FMT) – Management of security attributes, data, and functions and definitions of security roles.\textsuperscript{xvii}

\textbf{Privacy} (FPR) – Protect users against discovery and misuse of their identity.\textsuperscript{xviii}

\textbf{Protection of the TOE Security Functions} (FPT) – Maintain the integrity of the TSF management functions and data.\textsuperscript{xix}

\textbf{Resource Utilization} (FRUO) – Ensure availability of system resources through fault tolerance and the allocation of services by priority.\textsuperscript{x}

\textbf{TOE Access} (FTA) – Controlling user session establishment.\textsuperscript{x}

\textbf{Trusted Path Channels} (FTP) – Provide a trusted communications path between users and the TSF and between the TSF and other trusted IT products.\textsuperscript{x}

\textbf{Section Three – Security Assurance Requirements}

The security assessment requirements establish a set of assurance components (e.g. classes) as a standard to express the TOE assurance requirements.\textsuperscript{xxii}

Consumers, developers, and evaluators use these assurance requirements as guidance and for reference when determining assurance levels and requirements, assurance techniques, and evaluation criteria.\textsuperscript{xxiv}

The ten classes of security assessment requirements CC class abbreviation, and purpose are:

\textbf{Protection Profile Evaluation} (APE) – Demonstrate that the PP is complete, consistent, and technically sound.\textsuperscript{xxv}
**Security Target Evaluation** (ASE) – Demonstrate that the ST is complete, consistent, technically sound, and suitable for use as the basis for a TOE evaluation.\textsuperscript{xvii}

**Configuration Management** (ACM) – Control the process by which a TOE and its related documentation is developed, refined, and modified.\textsuperscript{xviii}

**Delivery & Operation** (ADO) – Ensure that the delivery, installation, generation, and initialization of the TOE.\textsuperscript{xix}

**Development** (ADV) – Ensure that the development process is methodical by requiring various levels of specification and design and evaluating the consistency between them.\textsuperscript{xx}

**Guidance Documents** (AGD) – Ensure that all relevant aspects of the secure operation and use of the TOE are documented in user and administrator guidance.\textsuperscript{xl}

**Life Cycle Support** (ALC) – Ensure that methodical processes are followed during the operations and maintenance phase so that security integrity is not disrupted.\textsuperscript{xli}

**Vulnerability Assessment** (AVA) – Analyze the existence of latent vulnerabilities, such as exploitable covert channels, misuse or incorrect configuration of the TOE, the ability to defeat, bypass, or compromise security credentials.\textsuperscript{xlii}

**Maintenance of Assurance** (AMA) – Assure that the TOE will continue to meets its security target as changes are made to the TOE or its environment.\textsuperscript{xlii}

**Tests** (ATE) – Ensure adequate test coverage, test depth, functional and independent testing.\textsuperscript{xlii}

### Protection Profile Overview

The Common Criteria methodology establishes the core set of processes by which organizations can approach computer security evaluations and/or apply Protection Profile (PP) criteria. PPs provide a detailed level of security requirements and standards pertinent to a specific technology or security risk area based on the overall CC framework or specific to the evaluated IT product or technology.

Each PP provides a reusable set of IT security requirements that can be certified as complete, consistent and technically sound in addressing threats that exist in a specified environment.\textsuperscript{xliii} A PP would be appropriate in the following cases:

- A consumer group wishes to specify security requirements for an application type (e.g. electronic funds transfer)
- A government wishes to specify security requirements for a class of security products (e.g. firewalls)
- An organization wishes to purchase an IT system to address its security requirements (e.g. patient records for a hospital).\textsuperscript{xliii}
The international CCRA supports PP development by providing certificates on PPs that can be accepted among the CCRA participants. PPs have been developed to provide mechanisms to defend and support fundamental areas of security risk to the network, infrastructure, system boundary, and computing environment.

**Defense-In-Depth Strategy**

The Information Assurance Technical Framework (IATF) recognizes support and defense of these four areas of security risk to be the basis of the security-in-depth strategy. The IATF provides technical guidance for protecting information and information infrastructures defining a systematic process for developing information assurance and the security requirements for the hardware and software components.

The Defense-in-Depth strategy is to provide information infrastructure protection in the of the following four core technology layers through defense and support mechanisms:

1. Defend the Network and Infrastructure,
2. Defend the Enclave Boundary,
3. Defend the Computing Environment, and
4. Supporting Infrastructures.

**Protection Profile Categorization**

The Protection Profiles (PP) provide detailed technology techniques and solutions to implement the defense-in-layers strategy. NIAP categorizes PPs according to the four core technology defense and support layers. Products and technology evaluated in compliance to established PPs are recognized by NIAP to provide means to defend and support the TOE against major security risks to the system or product environment (e.g. TOE).

![Figure 4: NIAP Protection Profile Evaluation Groupings](image)
A PP is intended to be reusable and to define TOE requirements that are known to be useful and effective in meeting identified functional and assurance security objectives.iii PPs permit security objectives independent of the implementation of a TOE or set of TOEs that complies fully with a set of security requirements and provides justification for security objectives and security requirements.iii

In total there are 30 evaluated, developed, and drafted recognized PPs which address technologies, hardware/software, operations, manpower, and services.iv The area of Defense-in-Depth strategy the PPs address separates these PPs out.

**Certified, Developed, and Draft Protection Profiles**

*Defend the Network & Infrastructure*

PPs to defend the network and infrastructure address the availability, confidentiality, and management requirements of large transport networks and various other transmission and switching capabilities.iv

<table>
<thead>
<tr>
<th>Entry Label</th>
<th>Type</th>
<th>Title</th>
<th>Supplier</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>PP-024</td>
<td>Switches &amp; Routers</td>
<td>Protection Profile for Switches and Routers</td>
<td>NSA</td>
<td>Draft</td>
</tr>
<tr>
<td>PP-023</td>
<td>WLAN</td>
<td>Peer-to-Peer Wireless Local Area Network (WLAN) for Sensitive But Unclassified Environments - V0.6</td>
<td>Booz·Allen &amp; Hamilton/ NSA / Tresys Technology</td>
<td>Draft</td>
</tr>
<tr>
<td>PP-027</td>
<td>WLAN</td>
<td>Infrastructure Wireless Local Area Network (WLAN) For Sensitive But Unclassified Environments</td>
<td>Booz·Allen &amp; Hamilton/ Tresys Technology</td>
<td>Draft</td>
</tr>
</tbody>
</table>

*Defend the Enclave Boundary (System Boundary)*

PPs to defend the enclave boundary deal with perimeter defenses.iv An enclave boundary is the points of connection for Local Area Network (LAN), a Wide Area Network (WAN), or similar networks to the service layer of another network.iv This category includes: protection for network access; protection for remote access from both remote enclaves and traveling laptops; and protection during interoperation across security level.ix
### Defend the Computing Environment

PPs to defend the computing environment attend to the security considerations for end user workstations, servers, applications, and operating systems.\(^{14}\)

<table>
<thead>
<tr>
<th>Entry Label</th>
<th>Type</th>
<th>Title</th>
<th>Supplier</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>PP-004</td>
<td>Access Control</td>
<td>Role-Based Access Control Protection Profile Version 1.0</td>
<td>NIST</td>
<td>Certified</td>
</tr>
<tr>
<td>PP-009</td>
<td>Access Control</td>
<td>Role-Based Access Control Protection Profile Version 1.0</td>
<td>NIST</td>
<td>Certified</td>
</tr>
<tr>
<td>PP-001</td>
<td>Access Control</td>
<td>Directory for US Department of Defense Class 4 PKI PP</td>
<td>NSA</td>
<td>Certified</td>
</tr>
<tr>
<td>PP-002</td>
<td>Access Control</td>
<td>Trusted Platform Module (TPM) Protection Profile</td>
<td>Trusted Computing Platform Alliance (TCPA)</td>
<td>Develop</td>
</tr>
<tr>
<td>PP-014</td>
<td>Access Control</td>
<td>Privilege Directed Content Protection Profile</td>
<td>Authorizer Ltd.</td>
<td>Certified</td>
</tr>
<tr>
<td>PP-008</td>
<td>Databases</td>
<td>Oracle DBMS Protection Profile</td>
<td>Oracle Corporation</td>
<td>Certified</td>
</tr>
<tr>
<td>PP-030</td>
<td>Databases</td>
<td>Oracle Government Database Management System</td>
<td>Oracle Corporation</td>
<td>Certified</td>
</tr>
<tr>
<td>PP-005</td>
<td>Firewalls</td>
<td>Traffic Filter Firewall Protection Profile For Medium Robustness Environments</td>
<td>NSA</td>
<td>Certified</td>
</tr>
<tr>
<td>PP-010</td>
<td>Firewalls</td>
<td>Traffic Filter Firewall Protection Profile for Low Risk Environments (Version1.1)</td>
<td>NSA</td>
<td>Certified</td>
</tr>
<tr>
<td>PP-011</td>
<td>Firewalls</td>
<td>Application Level Firewall Protection Profile for Low Risk Environments (Version1.d)</td>
<td>NSA</td>
<td>Draft</td>
</tr>
<tr>
<td>PP-015</td>
<td>Firewalls</td>
<td>Application-level Firewall Protection Profile For Medium Robustness Environments</td>
<td>NSA</td>
<td>Certified</td>
</tr>
<tr>
<td>PP-026</td>
<td>VPN</td>
<td>A Goal VPN Protection Profile For Protecting Sensitive Information - V2.0</td>
<td>NSA</td>
<td>Draft</td>
</tr>
</tbody>
</table>

### Defend the Enclave Boundary

<table>
<thead>
<tr>
<th>Entry Label</th>
<th>Type</th>
<th>Title</th>
<th>Supplier</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>PP-016</td>
<td>Biometrics</td>
<td>U. S. Department of Defense Biometrics Office, Biometric System Protection Profile For Medium Robustness Environments, v0.01</td>
<td>DoD Biometrics Management Office (DoD BMO)</td>
<td>Draft</td>
</tr>
</tbody>
</table>
**Supporting Infrastructures**

PPs to support infrastructures address the security capabilities for supporting infrastructures of defense-in-depth requirements. This includes incident handling, Key Management Infrastructure (KMI), and Public Key Infrastructure (PKI) technologies.

<table>
<thead>
<tr>
<th>Entry Label</th>
<th>Type</th>
<th>Title</th>
<th>Supplier</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>PP-006</td>
<td>Certificate</td>
<td>Certificate Issuing and Management Components</td>
<td>NSA</td>
<td>Certified</td>
</tr>
<tr>
<td>PP-017</td>
<td>IDS</td>
<td>Intrusion Detection System Analyzer - Draft 3</td>
<td>NSA</td>
<td>Draft</td>
</tr>
<tr>
<td>PP-018</td>
<td>IDS</td>
<td>Intrusion Detection System Sensor - Draft 3</td>
<td>NSA</td>
<td>Draft</td>
</tr>
<tr>
<td>PP-019</td>
<td>Key Recovery</td>
<td>Key Recovery for Third Party Requestors Ver. 1.0</td>
<td>NSA</td>
<td>Draft</td>
</tr>
<tr>
<td>PP-020</td>
<td>Key Recovery</td>
<td>Key Recovery for Agent Systems Ver. 1.1</td>
<td>NSA</td>
<td>Draft</td>
</tr>
<tr>
<td>PP-021</td>
<td>Key Recovery</td>
<td>Key Recovery for End Systems Ver. 2</td>
<td>NSA</td>
<td>Draft</td>
</tr>
<tr>
<td>PP-028</td>
<td>Smart Card</td>
<td>Smart Card Protection Profile</td>
<td>SCSUG</td>
<td>Certified</td>
</tr>
<tr>
<td>PP-029</td>
<td>PKI</td>
<td>The PKI Secure Kernel Protection Profile</td>
<td>PKI PP Working Group</td>
<td>Certified</td>
</tr>
</tbody>
</table>
Conclusion

Common Criteria standards and the technology specific Protection Profiles institute worldwide criteria for evaluating information technology operational security. Organizations recognized and sponsored by the United States government; NIST, NSA, NIAP, and the IATF Forum; are coordinating security assessment techniques and standards for use throughout the United States government. Information Technology developers, consumers, and evaluators who must implement or assess security within a system or product can use the Common Criteria and Protection Profiles to establish an internationally recognized baseline of security requirements and techniques.
REFERENCES


13. National Information Assurance Partnership (NIAP). “Validated Products List (by Type)”


ENDNOTES

i Trusted Product Evaluation Program (TPEP) Overview  
http://www.radium.ncsc.mil/tpep/process/overview.html


http://www.commoncriterion.org/docs/PDF/CCPART2V21.PDF

http://www.commoncriterion.org/docs/PDF/CCPART2V21.PDF

vi NIST CSRC. “Common Criteria for IT Security Evaluation, Common Language to Express Common Needs”  
http://csrc.nist.gov/cc/index.html

vii NIAP. “Introducing the National Information Assurance Partnership”  
http://niap.nist.gov/howabout.html

viii NIAP. “CC Evans”  
http://niap.nist.gov/cc-scheme/defining-ccEvans.html

ix CC Organization. “CC: An Introduction” pg 4  

x CC Organization. “CC: An Introduction” pg 4  

xi CC Organization. “CC: An Introduction” pg 5,  

•••(this diagram is an original analysis of concepts and definitions spread through the CC documentation)

xii CC Organization. “CC: An Introduction” pg 4  

xiii CC Organization. “CC: An Introduction” pg 4  

xiv CC Organization. “CC: An Introduction” pg 4  

xv CC Organization. “CC: An Introduction” pg 4  

xvi CC Organization. “CC: An Introduction” pg 7  

(this diagram is an original analysis of several diagrams into one CC framework environment overview)
Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46
“Protection Profile List - All?”
http://www.commoncriteria.org/ccc/protection_profiles/ppinfo.jsp?id=99&status=Certified

DLA. “Defense-wide Information Assurance Program: Definitions”

CC Organization. “Protection Profile List - All?”
http://www.commoncriteria.org/ccc/protection_profiles/ppinfo.jsp?id=99&status=Certified

CC Organization. “Protection Profile List - All?”
http://www.commoncriteria.org/ccc/protection_profiles/ppinfo.jsp?id=99&status=Certified

Page 18 of 18
<table>
<thead>
<tr>
<th>Course</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Amsterdam August 2020 Part 1</td>
<td>Amsterdam, NL</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS FOR508 Canberra August 2020</td>
<td>Canberra, AU</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam August 2020 Part 2</td>
<td>Amsterdam, NL</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Virginia Beach 2020</td>
<td>Virginia Beach, VAUS</td>
<td>Aug 31, 2020 - Sep 05, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Philippines 2020</td>
<td>Manila, PH</td>
<td>Sep 07, 2020 - Sep 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London September 2020</td>
<td>London, GB</td>
<td>Sep 07, 2020 - Sep 12, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Fall 2020</td>
<td>Baltimore, MDUS</td>
<td>Sep 08, 2020 - Sep 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Threat Hunting &amp; Incident Response Summit &amp; Training 2020</td>
<td>New Orleans, LAUS</td>
<td>Sep 10, 2020 - Sep 17, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>OnlineUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>