CSIRT Education Services

FIRST Final Draft

CSIRT Services Framework

Introduction

The following is a list of services that a Computer Security Incident Response Team (CSIRT) organization may consider implementing to address the needs of their constituency, and the mechanisms to address gaps in the ability to do so. This list is meant to capture both traditional services performed by CSIRTs as well as services that have recently emerged and are being undertaken by existing teams and organizations as they evolve. This document is a listing of the services that should comprise a CSIRT Services Framework.

Each service below is broken down into the primary functions and sub-functions that support a CSIRT's performance of that service in support of its broader mission. Please note that while they are represented here as unique, many of the functions and sub-functions are used to effectuate the delivery of multiple services and/or functions, and can be interdependent. Although this document recognizes that those relationships exist, it does not seek to define these interrelationships at this stage.

History

The CERT/CC CSIRT Services List has been used in many cases to serve as a consistent and comparable description of CSIRTs and their corresponding services. In recent assessments of existing CSIRT services lists, it was determined that although it was broadly used and adapted, the CERT/CC list was outdated and missing key components that represent the mission of modern-day CSIRTs. FIRST, interested in enabling the global development and maturation of CSIRTs, recognized that this was a key piece in framing the development of a comprehensive CSIRT education program. Given the geographical and functional span of the membership of FIRST, it was determined that the community that it assembles would be an appropriate source for definitive capture and representation of the services provided by CSIRTs.

As used in this document, we are defining the use of certain terms:

- **Service** – the action of helping or doing work on behalf of or for the constituency
- **Function** – a means to fulfill the purpose or task of a specified service
- **Capability** – a measurable activity that may be performed as part of an organization's roles and responsibilities. For the purposes of the CSIRT services framework the capabilities can either be defined as the broader services or as the requisite functions, sub-functions or tasks.

- **Capacity** – the number of simultaneous occurrences of a particular capability that an organization can execute before they achieve some form of resource exhaustion.

- Maturity – how effectively an organization executes a particular capability within the mission and authorities of the organization.

Service 1 Incident Management

Function 1.1 **Incident Handling:** Services related to the management of a cyber-event, to include alerting constituents and coordinating activities associated with the response, mitigation, and recovery from an incident. Incident handling is dependent upon analysis activities, which are defined in the "Analysis" section.

Sub-Function 1.1.1 Information Collection: Services related to the intake, cataloging, and storage of information related to events and incidents to include:

- **Incident Report Collection:** Collection of reports regarding malicious or suspicious events and incident reports from constituents and 3rd parties (such as other security teams or commercial intelligence feeds), whether manual, automated or machine readable forms.
- **Digital Data Collection:** Gathering and cataloging of digital data that may be, but are not guaranteed to be, useful in understanding incident activity (e.g., disk images, files, network logs/flows).
- **Other data types (non-digital):** Gathering and cataloging of non-digital data (physical sign in sheets, architecture diagrams, business models, site assessment data, policies, enterprise risk frameworks etc.).
- **Artifact Collection:** The business and technical processes used to intake, catalog, store, and track artifacts believed to be remnants of adversary activity.
- **Evidence Collection:** The business of collecting information and data for possible use in law enforcement activities, often including capturing metadata regarding the source, method of collection, and owner and custody information.

Sub-Function 1.1.2 Response: Services related to reducing the impact of an incident and working to restore business functions within the constituency.

- **Containment:** Stopping immediate damage and limiting the extent of malicious activity through short-term tactical actions (for example, blocking or filtering traffic); can also involve regaining control of systems.
- **Mitigation:** Preventing further damage through eradication, implementing a work-around, or implementing more in-depth and comprehensive containment strategies.
- **Repair:** Implementing changes in the affected domain, infrastructure or network necessary to fix and prevent this type of activity from reoccurring. This includes

strengthening the organizational defensive posture and operational readiness by policy changes and additional training and education.

- **Recovery:** Restoring the integrity of affected systems and returning the affected data, systems and networks to a non-degraded operational state.

Sub-Function 1.1.3 Coordination: Information sharing and advisement activity both internal and external to the CSIRT. This primarily occurs when the CSIRT is reliant on expertise and resources outside of direct control of the CSIRT to effectuate the actions necessary to mitigate an incident. By offering bilateral or multilateral coordination, the CSIRT participates in the exchange of information to enable those resources with the ability to take action to do so or to assist others in the detection, protection or remediation of on-going activities from adversaries.

Sub-Function 1.1.4 Incident Tracking: Documenting information about actions taken to resolve an incident, including critical information collected, analysis performed, remediation and mitigation steps taken, closure and resolution.

Function 1.2 **Vulnerability, Configuration and Asset Management:** Services related to the understanding and remediation of vulnerabilities, configuration issues and inventory of assets.

Sub-Function 1.2.1 Vulnerability Discovery Research: The identification of new vulnerabilities through research and experimentation (i.e., fuzz testing and reverse engineering).

Sub-Function 1.2.2 Vulnerability Reporting: The business and technical processes used to intake, catalog, store, and track vulnerability reports.

Sub-Function 1.2.3 Vulnerability Coordination: Notifying appropriate organizations of a vulnerability to effect repairs and to limit the potential impacts from exploitation.

Sub-Function 1.2.4 Vulnerability Root Cause Remediation: Implementation of the formal corrective actions necessary to correct an identified vulnerability. Typically done by the product vendor.

Service 2 Analysis

Function 2.1 **Incident Analysis:** Services related to identifying and characterizing information about events or incidents such as scope, affected parties, involved systems, timeframes (discovery, occurrence, reporting), status (ongoing versus completed).
[Note: More in-depth analysis of an incident occurs through other, more focused analysis tasks such as artifact, misconfiguration, vulnerability, network, or forensics information analysis.]

Sub-Function 2.1.1 Incident Validation: Conclusively verifying that a reported incident in fact occurred and has had some impact on the involved systems.

Sub-Function 2.1.2 Impact Analysis: Identifying and characterizing the impact to the business function supported by involved systems.

Sub-Function 2.1.3 Lessons Learned: After-action review to identify improvements to processes, policies, procedures, resources, and tools to help mitigate and prevent future compromise.

Function 2.2 **Artifact Analysis:** Services related to the understanding of the capabilities and intent of artifacts (e.g., malware, exploits, spam, and configuration files) and their delivery, detection, and neutralization.

Sub-Function 2.2.1 Surface Analysis: Identifying and characterizing basic information and metadata about artifacts (e.g., file type, strings output, cryptographic hashes, file size, filename); along with reviewing any public or private source information about the artifact.

Sub-Function 2.2.2 Reverse Engineering: In-depth static analysis of an artifact to determine its complete functionality, regardless of the environment within which it may be executed.

Sub-Function 2.2.3 Run Time Analysis: Understanding of an artifact's capabilities via observation while running the sample in a real or emulated environment (e.g., sandbox, virtual environment, and hardware or software emulators).

Sub-Function 2.2.4 Comparative Analysis: Analysis focused on identifying common functionality or intent, including family analysis of cataloged artifacts.

Function 2.3 **Media Analysis**: Services involving the analysis of relevant data from systems, networks, digital storage, and removable media in order to better understand how to prevent, detect, and/or mitigate similar or related incidents. These services may provide information for legal, forensic, compliance reviews or other historical reviews of information.

Function 2.4 **Vulnerability / Exploitation Analysis:** Services provided to enable a deeper understanding of the vulnerabilities that have been a factor in a cyber-incident.

Sub-Function 2.4.1 Technical (Malware) Vulnerability / Exploit Analysis: Understanding the weakness(es) leveraged to instigate an incident and the adversarial tradecraft utilized to leverage that weakness.

Sub-Function 2.4.2 Root Cause Analysis: The understanding of the "design" or "implementation" flaw that allowed the attack.

Sub-Function 2.4.3 Remediation Analysis: The understanding of the steps necessary to fix the underlying flaw that enabled the attack, and prevent this type of attack in the future.

Sub-Function 2.4.4 Mitigation Analysis: Analysis to determine the means to mitigate (prevent) the risks created as a result of an attack or vulnerability without necessarily remediating the underlying flaw that introduced it.

Service 3 Information Assurance

Function 3.1 **Risk / Compliance Assessment:** Services related to assessing risk or compliance assessment activities. This may include conduct of the actual assessment, to providing support to evaluate the results of an assessment. Typically done in support of a compliance requirement (e.g., ISO 27XXX, COBIT).

Sub-Function 3.1.1 Critical Asset/Data Inventory: Identification of key assets and data that are critical to completing the organization's mission. These assets and data may not necessarily be owned by the organization (e.g., cloud provider or external data set). This includes identifying their location, their owner, their information sensitivity level, their mission function, and their current status / level.

Sub-Function 3.1.2 Identify Evaluation Standard: Gaining Organizational Risk Policy(ies) and enumerated/identified Standards by Executives for evaluation of Security Level/Status. Suggesting criteria for assessment or benchmarking for Enterprise Risk Managers and CISO's to consider. Examples of standards may include but are not limited to Basel II, COBIT, ITIL, Certification and Accreditation.

Sub-Function 3.1.3 Execute Assessment: Assist in conducting reviews and participating in assessments to ensure risk and security requirements are met / addressed.

Sub-Function 3.1.4 Findings & Recommendations: Developing and providing findings, reports and/or recommendations (e.g., report writing, using the tasks in publication of information).

Sub-Function 3.1.5 Tracking: Assist the CISO and/or Risk Manager in tracking both status of assessments and subsequent implementation of recommendations.

Sub-Function 3.1.6 Testing: Active testing for compliance with risk levels. Can include penetration testing, vulnerability scanning and assessment, application testing, auditing and verification, etc.

Function 3.2 **Patch Management:** Services that assist constituency with the capabilities necessary to manage the identification of inventory, systems to patch, deployment and verification of patch installation.

Function 3.3 **Operating Policies Management**: Services that develop, maintain, institutionalize, and enforce organizational concept of operations, and other policies.

Function 3.4 **Risk Analysis/Business Continuity Disaster Recovery Advisement:** Services provided to constituency related to organizational resilience activities based on risks identified. This could include a range of risk management activities, from conducting the actual assessment to providing analysis support in evaluating and mitigating the results of an assessment.

Function 3.5 **Security Advisement**: Services providing advice to a constituent or line-of-business on the execution and implementation of pertinent security operations or functions.

Service 4 Situational Awareness

Function 4.1 **Sensor/Metric Operations:** Services that focus on the development, deployment, and operation of systems and analysis methodologies to identify activities for investigation.

Sub-Function 4.1.1 Requirements Development: Understanding the needs of the constituency and securing the authorizations under which the CSIRT can operate.

Sub-Function 4.1.2 Identification of Necessary Data: Determining the data necessary to fulfill requirements.

Sub-Function 4.1.3 Data Acquisition Methods: Determining the methods, tools, techniques, and technologies used to gather necessary data.

Sub-Function 4.1.4 Sensor Management: Maintenance and continual improvement of sensor performance relative to defined requirements.

Sub-Function 4.1.5 Results Management: Triage and dissemination of information and metrics derived from sensors. Usually provided via a dashboard for view by various levels within an organization.

Function 4.2 **Fusion/Correlation:** Services that conduct analysis and inclusion of multiple data sources. Take feeds of information, regardless of the source, and integrate it into an overall view of the situation (Situational Awareness).

Sub-Function 4.2.1 Determine Fusion Algorithms: Determine the methods and techniques (algorithms) or technologies used to analyze (fuse) the information.

Sub-Function 4.2.2 Fusion Analysis: Analysis (fusing) of the data resources using the data in the knowledge management system to identify commonalities and relationships amongst the data.

Function 4.3 **Development and Curation of Security Intelligence:** Services provided to internal or external constituents in the interest of developing and curating third party sources of security intelligence. Security intelligence can be defined as security and threat information that provides either operational intelligence or threat intelligence. Services may include but are not limited to analysis, development, distribution, and management of security intelligence, including threat indicators, threat detection logic such as antimalware rules and signatures, and adversary tactics, techniques, and procedures. These services are dependent upon information exchange activities, which are defined in section 5.6, "Outreach/Communications".

Sub-Function 4.3.1 Source Identification and Inventory: Continual identification, maintenance, and integration of information sources into knowledge management and analysis processes.

Sub-Function 4.3.2 Source Content Collection and Cataloging: The acquisition of threat information source materials. These sources maybe both internal, external, open source and/or fee for service.

Function 4.4 **Data and Knowledge Management:** Services offered to constituents in support of capturing, developing, sharing, and effectively using organizational knowledge to include data markup (e.g., STIX, TAXII, IODEF, TLP), indicator databases, and malware / vulnerability catalogs.

- **Data Representation Management:** Standardization of how data is represented and exchanged (e.g., STIX, TAXII, IODEF, RID, etc.)
- **Data Storage Management:** The design, implementation and maintenance of storage management systems.
- **Data Digestion:** Processes and systems used to input, validate and store information.
- **Data Extraction:** Processes, policies and technical methods for extracting the information.
- **Tool Evaluation:** Evaluation and integration of tools used for data management, analysis, and collaboration.

Function 4.5 **Organizational Metrics**: Services that focus on identification, establishment, collection, and analysis of achievement of organizational performance goals; along with measuring organizational effectiveness.

Service 5 Outreach/Communications

Function 5.1 **Cybersecurity Policy Advisory:** Services that support the development and adoption of cybersecurity policy to positively shape the environment of the CSIRT, its constituency, and other stakeholders by providing subject matter expert advice to inform decision makers.

Sub-Function 5.1.1 Internal

- **Policy and Legal Consultation:** Conveying policy and legal implications input related to organizational and constituent authorities and mandates.
- **Authoring Policy**: Producing policy as it relates or affects an organizational or constituents operations and authorities.

Sub-Function 5.1.2 External

- **Provide Policy Input:** Providing advice on technical and security policy issues that may impact the organization and its constituency or other partners.
- **Influence Policy:** Providing authoritative information or subject matter expertise to guide revision of policies, regulations, or laws. This can include but is not limited to testifying before legislative, scientific, or other bodies, writing position papers, white papers or articles, blogs or social media, meeting with stakeholders, etc.
- **Standards or Best Practices Development**: Contributing to the efforts of industry, global, regional, and national standards or best practice organizations (IETF, ISO, FIRST) to enable normalization of processes / best practices to maximize compatibility, interoperability, safety, repeatability, or quality.

Function 5.2 **Relationship Management**: Services that focus on establishment and maintenance of relationships for the organization.

Sub-Function 5.2.1 Peer Relationship Management: Development and maintenance of relationships with organizations that may be able to enable the execution of the mission of the CSIRT. This may involve ensuring interoperability or fostering collaboration between or across organizations.

Sub-Function 5.2.2 Constituency Relationship Management: Development and implementation of practices, strategies and technologies used to identify, distinguish, understand, manage, track, and evaluate constituents and stakeholders.

Sub-Function 5.2.3 Communications Management: Management of lists used to distribute announcements, alerts, warnings, data feeds and other publications or information sharing.

Sub-Function 5.2.4 Secure Communications Management: Management of secure communication mechanisms used for email, web, instant messaging, or voice communications.

Sub-Function 5.2.5 Conferences / Workshops: Providing opportunities for the CSIRT and its constituency to spend time together discussing threats and challenges that they are facing, strengthen trust relationships, exchange contacts, and share best practices or lessons learned.

Sub-Function 5.2.6 Stakeholder Engagement/Relations: Includes coordination with sector / vertical organizations, and maintaining formal points of contact with both internal and external stakeholders. Engagement with executive levels within the organization to educate on the mission of the organization and ensure security awareness understanding.

Function 5.3 **Security Awareness Raising** Services that work within the constituency to raise the collective understanding of threats that they face and actions that can be taken to reduce the risk posed by these threats.

Function 5.4 **Branding/Marketing**: Services that ensure that stakeholders and constituents are aware of the CSIRT and the capabilities provided by the CSIRT, as well as how they should interact with the CSIRT to convey their needs.

Function 5.5 **Information Sharing and Publications**: Services that focus on broad communication, including notifications made by the organization to their constituency in support of operations. Examples include notations of training, events, organizational policies and procedures.

Sub-Function 5.5.1 Public Service Announcements: Dissemination of security related information to improve awareness of and implementation of organizational, constituent, sector or public security practices.

Sub-Function 5.5.2 Publication of Information:

- **Requirements Gathering:** Identifying what information is required to be disseminated, to whom, and in what manner and timeframe (scoping). Note: publication may be to a limited audience or more in-depth publication for partner audiences.
- **Development**: Defining the format and purpose of information products to fulfill requirements.
- **Authoring:** Accurately capturing information so that it is readily understood by the intended audience(s) (e.g., presenting the results of forensic, incident, vulnerability, and malware management activities).
- **Review:** Reviewing publication for clarity, accuracy, grammar, spelling, sensitivity, and adherence to information disclosure rules, and attaining final approval.
- **Distribution:** Delivery of information to intended audience via necessary and appropriate channels.

Service 6 Capability Building

Function 6.1 **Training and Education:** Capacity infers some level of capability at some level of maturity. Thus Capability is the core building block for CSIRT Services. Capability Building provides training and education to a CSIRT constituency (which may include organizational staff, but excluding functional items such as HR training for the team) on topics related to cybersecurity, information assurance and incident response.

Sub-Function 6.1.1 Knowledge, Skill, and Ability Requirements Gathering: Collecting knowledge, skill, and ability needs and the competence of a constituency in regards to determining what training and education should be provided.

Sub-Function 6.1.2 Development of Educational and Training Materials: Building or acquiring content of educational and training materials such as presentations, lectures, demonstrations, simulations, etc.

Sub-Function 6.1.3 Delivery of Content: Transfer of knowledge and content to "students". This can occur via various methods, such as computer-based training/online, instructor-led, virtual, conferences, presentations, lab, etc.

Sub-Function 6.1.4 Mentoring: Learning from experienced staff, through an established relationship, can involve on-site visits, rotation (exchange), shadowing, and discussion rationale for specific decisions and actions.

Sub-Function 6.1.5 Professional Development: Helping staff members successfully and appropriately plan and develop their careers. Can include attending conferences, advanced training, cross-training activities, etc.

Sub-Function 6.1.6 Skill Development: Providing training for organization staff on tools, processes, and procedures for daily operations functions.

Sub-Function 6.1.7 Conducting Exercises: Performing readiness testing of constituent "students" to test their ability to apply training and perform job or task functions. Can be in the form of virtual environments, simulations, field tests, table-tops, mock scenarios, or a combination.

Function 6.2 **Organizing Exercises:** Services offered by the organization to constituents that support the design, execution and evaluation of cyber exercises intended to train and/or evaluate the capabilities of individual constituents and the constituency as a whole. These types of exercises can be used to:

- **Test policies & procedures:** Team assesses whether there are sufficient policies and procedures in place to meet the event. This is generally a paper/tabletop exercise.
- **Test operational readiness:** Team assesses whether the right people are in place to respond to the event and whether procedures are executed correctly. This typically involves exercising procedures.

Sub-Function 6.2.1 Requirements: Understanding the intent of the exercise, specifically the objectives of all participants, to ensure that development incorporates these desires.

Sub-Function 6.2.2 Scenario and Environment Development: Development of exercise scenarios in support of constituency objectives.

Sub-Function 6.2.3 Participation in an exercise: An organization can have various levels of participation in an exercise due to their maturity level.

- **Evaluation:** Evaluate the outcomes of an exercise. Solicit feedback and identify lessons based on observation of the exercise.
- **Observation:** Observe a third party exercise.
- **Coordination:** Coordinate an exercise.
- **Participation:** Participate in a cyber-exercise. Participant gets to choose what level they participate and gain from the outcome of the exercise (e.g., have a third party evaluate their participation).

Sub-Function 6.2.4 Identification of Lessons Learned: Develop an after-action report which includes lessons learned or findings / best practices from the exercise.

Function 6.3 **Systems and Tools for Constituency Support:** Services that focus on recommending, development, provision and acquisition of cybersecurity related tools and services for a constituency. All of these systems and tools are related to CSIRT/security and not to general Information Technology; these systems could include messaging / alerting portals.

Function 6.4 **Stakeholder Services Support:** Services focused on technical capabilities offered by the CSIRT to assist in building capability, capacity, and maturity of CSIRT services to stakeholders. This is a maturation of service levels. Typical examples include:

Sub-Function 6.4.1 Infrastructure Design and Engineering: Assisting in the design and engineering of the infrastructure to support constituency requirements.

Sub-Function 6.4.2 Infrastructure Procurement: Assisting in the procurement of infrastructure, whether assisting in developing risk framework maturity or minimum-security requirements and standards for contract language (e.g., requiring compliance with a particular standard such as a product certification).

Sub-Function 6.4.3 Infrastructure Tool Evaluation: Evaluation of tools on behalf on the constituency.

Sub-Function 6.4.4 Infrastructure Resourcing: Assisting in acquiring needed infrastructure resources. (i.e., hardware vendors, service providers, etc.)

Service 7 Research/Development

Function 7.1 **Development of Vulnerability Discovery/Analysis/Remediation/Root Cause Analysis Methodologies**: Services that help define, identify new capabilities and improve methodologies for performing vulnerability related services or coordinating other organizations or commercial practices that can demonstrate the same.

Function 7.2 **Development of processes for Gathering/Fusing/Correlating Security Intelligence**: Services that define, identify new capabilities and improve methodologies for performing information analysis and sharing related services as it relates to operational and threat intelligences.

Function 7.3 **Development of Tools**: Services that develop, identify new capabilities and share approaches to new tools and to automate the execution of CSIRT related processes.

Supporting Resources

FIRST - https://www.first.org

CERT/CC - http://www.cert.org

STIX/TAXII - https://stix.mitre.org

TLP - https://www.us-cert.gov/tlp

IETF - https://www.ietf.org

ISO/IEC 27035 -
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44379

Glossary

Application Testing – An investigation conducted to provide stakeholders with information about the quality of the product or service under test.

Basel II – The second of the Basel Accords, which are recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision.

Capability – A measurable activity that may be performed as part of an organization's roles and responsibilities. For the purposes of the CSIRT services framework the capabilities can either be defined as the broader services or as the requisite functions, sub-functions or tasks.

Capacity – The number of simultaneous occurrences of a particular capability that an organization can execute before they achieve some form of resource exhaustion.

CERT/CC – Computer Emergency Response Team Coordination Center.

CISO – Chief Information Security Officer.

Cloud – A distributed computing environment that allows application software to be operated using internet-enabled devices.

COBIT – Control Objectives for Information and Related Technology.

Cryptographic Hash – A hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone.

CSIRT – Computer Security Incident Response Team.

External Data Set – A third-party collection of data.

FIRST – Forum of Incident Response and Security Teams.

Function – A means to fulfill the purpose or task of a specified service.

Fuzz Testing – A software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program.

Hardware / Software Emulator – Hardware or software that enables one computer system (called the host) to behave like another computer system (called the guest). Typically utilized to enable the host system to run software or use peripheral devices designed for the guest system.

IEC – International Electrotechnical Commission.

IETF – Internet Engineering Task Force.

IODEF – Incident Object Description Exchange Format, which is a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents.

ISO – International Organization for Standardization.

ISO/IEC 27000-Series (ISO27k) – Information security standards that provide best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series).

ITIL – Information Technology Infrastructure Library, which is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.

Maturity – How effectively an organization executes a particular capability within the mission and authorities of the organization.

Open Source – A development model that promotes universal access via a free license to a product's design or blueprint, and universal redistribution of that design or blueprint, including subsequent improvements to it by anyone.

Penetration Testing – An attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality and data.

Reverse Engineering – The process of extracting knowledge or design information from anything man-made and re-producing it or reproducing anything based on the extracted information.

RID – Real-time Inter-network Defense, which is an inter-network communication method to facilitate sharing incident handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms for a complete incident handling solution.

Sandbox – A security mechanism for separating running programs.

Service – The action of helping or doing work on behalf of or for the constituency.

STIX – Structured Threat Information eXpression, which is a collaborative community-driven effort to define and develop a standardized language to represent structured cyber threat information.

Strings Output – A resulting sequence of characters, either as a literal constant or as some kind of variable.

TAXII – Trusted Automated Exchange of Indicator Information, which is a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries.

TLP – Traffic Light Protocol. Used to ensure that sensitive information is shared with the correct audience.

Virtual Environment – An emulation of a particular computer system.

Vulnerability Scanning and Assessment – A security technique used to identify security weaknesses in a computer system.