Security Content Discovery and Dissemination Protocol

Use cases and workflows

Enterprise operators rely on a wide range of external content to support, maintain, and evolve the security posture of their enterprise. Security content includes, but is not limited to:

* Vulnerability alerts
* Patch announcements
* Security configuration guidance
* Automated security checking tools and instructions
* Meta-information about security-relevant infrastructure (e.g., SWID tags for software products)

Currently, most of this information is available to enterprise operators, but it is available via different methods depending on both the type of content and the party from which it is collected. Some tools (e.g., many Microsoft products, Firefox, etc.) have their own protocols by which they discover and download patches. Some vendors have automatic feeds (e.g., RSS or Atom) by which consumers can discover new vulnerability alerts. Different companies might make security guidance available via their web site over HTTP.

The result is that enterprise operators are forced to use many tools, contacting many different remote services in order to collect the information they need to secure their enterprises. Moreover, this large variety and the fact that many of these exchanges must be manually initiated by enterprise operators means that it is easy to overlook relevant information, or to fail to collect information in a timely manner.

This paper outlines a standard, called the Security Content Discovery and Dissemination (SCDD) protocol, by which security content information can be discovered and collected using a common interface. The common interface will allow enterprise operators to use a single tool to collect a large portion of the security content that they need. It will also allow them a single interface by which to monitor for new content that could be of interest. All of this makes it easier to identify and collect the security content enterprise operators need to protect their enterprises.

# Supported Use Cases

These are the use cases that the SCDD specification is designed to address:

## UC1 – Content Discovery

The repository includes the ability for users to understand the nature of the security content it contains. This includes an understanding of the type of content (e.g., patch alerts, vulnerability alerts, guidance, etc.), the format in which the content is expressed, and an understanding of its applicability (e.g., to what software/version/vendor does the content apply). A user is able to learn this information about the content without needing to download that content first. This can help operators determine which, if any, of the repository’s content is of interest to them.

## UC2 – Controlled Distribution

A content consumer can use SCDD to collect content from a repository. The content provider can control dissemination to only allow certain parties to retrieve certain content. This can be used to ensure sensitive content is only delivered to authorized parties and/or to require certain pre-conditions be met before download (such as having the user provide a payment). This allows operators to collect any content of interest using a single protocol while giving content providers the ability to control distribution of that content.

## UC3 – Change Monitoring

For any identified collection or specific piece of security content, a user can discover whether that collection or content has changed since some specific point in the past. Content consumers can discover changes to content of interest (for example, addressing an error in a previous piece of content) as well as the addition of new content that meets a given set of characteristics that a consumer identifies as being of interest.

## UC4 – Identification and Extraction of Related Content

Security content sometimes is related to other content. For example, a vulnerability alert might reference a patch that addressed the vulnerability, or a set of guidance might reference a set of checks that can automatically determine if that guidance is being followed. In fact, some content might have little value without other, associated content. To support this, SCDD supports annotating content as interrelated, and content consumers can use this to identify and collect content related to some other content of interest.

# Requirements

The following are requirements that SCDD must meet:

## R1 –Stateless

SCDD requirements can be met without requiring the content consumer or producer to retain long-term state. Producers and consumers might choose to add additional features that are not stateless – for example, a producer might allow consumers to establish subscriptions by which new content that meets certain criteria is automatically pushed to them. However, all use cases can be supported even if neither party retains session state between sessions.

## R2 – Provides Permanent References

Sometimes content needs to cross reference each other, occasionally between different repositories. SCDD must support the creation of permanent references for each piece of content so that specific content can be referenced. This is not to say that every piece of content must be referenceable indefinitely – content producers are allowed to remove content from distribution at will. Attempts to resolve non-existent content can be met with a redirect that suggests a replacement (such as if the reference content has been revised or replaced) or simply a note that the referenced content is no longer available. However, for content that is present, it needs a direct means for it to be referenced by external sources.

## R3 – Content Format Agnostic

SCDD has no dependency on the format of the security content that is discovered or disseminated. While some meta-information about each piece of content needs to be populated (e.g., the content format type, applicability statement, etc.) there is no expectation that this information can be automatically extracted from the content itself. In short, any format of content can be discovered or disseminated without requirement that the format be recognized by SCDD.

## R4 – Configuration of Content Security

Some security content might be sensitive and should not be disclosed to unauthorized parties while others might be open to the public. Some might be available to anyone, but they have to pay first. As such, SCDD must support requiring that consumers provide authentication credentials and support delivery of discovery information as well as delivery of content itself in a manner that protects data confidentiality. It must also support exchanges where these security mechanisms are not employed. In other words, SCDD must support authentication and confidentiality, but users of SCDD are not required to use these features in all cases.

## R5 – Content Format Inclusive

A content producer might possess two instances of the same content in differing formats. In order to ensure this affords consumers the ability to discover and download the given content in their preferred format, SCDD must be capable of recognizing that these multiple formats represent the same content, and allowing the consumer to select the specific instance to download based on its format. Concisely, SCDD must provide means for storing multiple formats of the same content while remaining format agnostic.

# Non-Use Cases

This describes use cases that are not explicitly supported or explicitly prohibited by the current version of SCDD, but that are interesting enough to warrant future investigation and consideration for inclusion in future versions of SCDD.

## NUC1 –Standardization of Automated Procedures to Populate Security Content Metadata

SCDD uses metadata associated with each piece of security content that can be discovered or downloaded using SCDD. While SCDD defines the format and contents of this metadata, it does not describe a standard procedure for the population of it. Population of this metadata is currently the responsibility of the content producer, but there may be value in standardizing the process for at least the required metadata fields.

## NUC2 – Automated Discovery of SCDD Servers

SCDD servers are discovered through usual means of discovering servers, such as DNS or advertising through other protocols (such as providing a link in a web page). Apart from specifying a standard port number for the service, the SCDD specification does not define a means to discover the presence or whereabouts of SCDD servers. In the future, the SCDD could standardize a way to locate SCDD content servers automatically, and with minimal human input.

## NUC3 – Subscription Based Notification System

SCDD uses a pull system to allow consumers to request updates from the producer. An optional push system that allows consumers to subscribe to a producer and receive update notifications could be supported in future versions of the specification.

# Workflow

The following provides a high-level description of how SCDD could be used.

1. A content producer establishes a server with some amount of security content. For each piece of content, the producer creates and attaches metadata that includes, at minimum, the type of content it is (selected from a set of high-level security content types), the format of the content, and information to determine applicability of the content. Other metadata could be included. The producer might be able to automatically build this metadata by extracting key pieces of the content, or they may need to build this metadata manually. The SCDD specification dictates the format and content of the metadata but does not provide guidance on its creation.
2. A content consumer identifies a SCDD content repository of interest. This could be done via information provided by the repository owner. The SCDD specification does not provide guidance on how one might identify the network address of SCDD servers.
3. A content consumer contacts a SCDD server. The nature of the contact depends both on the consumer’s interests and on their prior understanding of the content available. Possible interactions could be:
   1. Request for an index of content collections
   2. Request for an index of content that meets specific applicability requirements, is of a certain format, or is a certain type of security content
   3. Request for one or more specific pieces of content
4. The content producer may choose to reject the request, limit the response to a subset of available content, or deliver all requested content, depending on the nature of the content and whether or not the consumer has been authenticated as an authorized party. The content producer may choose to deliver content in a manner that preserves integrity.
5. Subsequently, the consumer may contact the producer again and determine if there has been any change relative to the results of their earlier request.