|  |  |  |
| --- | --- | --- |
| **Data Source** | Cisco ASA firewall logs | Give this input or data source a name. |
| **Description:** |  | Provide a brief description of this input. What is the nature of the data? |
| **Ownership** |  | Who is the owner of this data? |
| **File Name** |  | Provide the file name, if applicable |
| **Location:**  **Server(s):**  **Directory:**  **Scripted Input:**  **API:**  **Network port:** | San Francisco, Ashburn COLO | Where is the data located? Is this data in a file? Can it be obtained via an API, network port, etc.? If the data must be obtained from an API, attach a description of the method for collecting the data - or supply a script to collect the data. |
| **Data Volume:**  **Average per day:**  **Peak:** |  | Are there special conditions that will cause a peak in data? Are there predictable patterns to the data volume? Does it vary by host? |
| **Retention:**  **Legal Requirement**  **Business Requirement**  **Search Requirement** | 90 days | How long must data be kept online? How often will offline data need to be retrieved for forensic purposes? What should be done with the data when it is archived out of Splunk? |
| **Legal Compliance** |  | Are there any laws or regulations that affect the collection, retention or accessibility of this data? |
| **Integrity** |  | Are there any special considerations for data integrity? Should the events be encrypted or auditable via Splunk? |
| **Format or sourcetype** |  | Describe the format of the data. Add additional pages with detailed field formatting information, if available. Provide the sourcetype if known. |
| **Timestamp** |  | Does the data contain a timestamp? If not, how should Splunk determine the time of the events? |
| **Collection Method** |  | How will this data get to the Splunk indexer? Are there transport or network issues that need to be addressed? |
| **Visibility / Access** | Security, IT Ops | Which individuals, teams or Splunk roles should be allowed access to this data? |
| **Searching** |  | How often will this data be searched or accessed? Will this data be used for alerts? |
| **Compression** |  | Actual/estimated compression ratio |

|  |  |  |
| --- | --- | --- |
| **Data Source** | Badge reader log | Give this input or data source a name. |
| **Description:** |  | Provide a brief description of this input. What is the nature of the data? |
| **Ownership** |  | Who is the owner of this data? |
| **File Name** |  | Provide the file name, if applicable |
| **Location:**  **Server(s):**  **Directory:**  **Scripted Input:**  **API:**  **Network port:** | San Francisco, Boston, London | Where is the data located? Is this data in a file? Can it be obtained via an API, network port, etc.? If the data must be obtained from an API, attach a description of the method for collecting the data - or supply a script to collect the data. |
| **Data Volume:**  **Average per day:**  **Peak:** |  | Are there special conditions that will cause a peak in data? Are there predictable patterns to the data volume? Does it vary by host? |
| **Retention:**  **Legal Requirement**  **Business Requirement**  **Search Requirement** | 6 months | How long must data be kept online? How often will offline data need to be retrieved for forensic purposes? What should be done with the data when it is archived out of Splunk? |
| **Legal Compliance** |  | Are there any laws or regulations that affect the collection, retention or accessibility of this data? |
| **Integrity** |  | Are there any special considerations for data integrity? Should the events be encrypted or auditable via Splunk? |
| **Format or sourcetype** |  | Describe the format of the data. Add additional pages with detailed field formatting information, if available. Provide the sourcetype if known. |
| **Timestamp** |  | Does the data contain a timestamp? If not, how should Splunk determine the time of the events? |
| **Collection Method** |  | How will this data get to the Splunk indexer? Are there transport or network issues that need to be addressed? |
| **Visibility / Access** | Security, | Which individuals, teams or Splunk roles should be allowed access to this data? |
| **Searching** |  | How often will this data be searched or accessed? Will this data be used for alerts? |
| **Compression** |  | Actual/estimated compression ratio |

|  |  |  |
| --- | --- | --- |
| **Data Source** | Cisco WSA Proxy | Give this input or data source a name. |
| **Description:** |  | Provide a brief description of this input. What is the nature of the data? |
| **Ownership** |  | Who is the owner of this data? |
| **File Name** |  | Provide the file name, if applicable |
| **Location:**  **Server(s):**  **Directory:**  **Scripted Input:**  **API:**  **Network port:** | San Francisco | Where is the data located? Is this data in a file? Can it be obtained via an API, network port, etc.? If the data must be obtained from an API, attach a description of the method for collecting the data - or supply a script to collect the data. |
| **Data Volume:**  **Average per day:**  **Peak:** |  | Are there special conditions that will cause a peak in data? Are there predictable patterns to the data volume? Does it vary by host? |
| **Retention:**  **Legal Requirement**  **Business Requirement**  **Search Requirement** | 1 month | How long must data be kept online? How often will offline data need to be retrieved for forensic purposes? What should be done with the data when it is archived out of Splunk? |
| **Legal Compliance** |  | Are there any laws or regulations that affect the collection, retention or accessibility of this data? |
| **Integrity** |  | Are there any special considerations for data integrity? Should the events be encrypted or auditable via Splunk? |
| **Format or sourcetype** |  | Describe the format of the data. Add additional pages with detailed field formatting information, if available. Provide the sourcetype if known. |
| **Timestamp** |  | Does the data contain a timestamp? If not, how should Splunk determine the time of the events? |
| **Collection Method** |  | How will this data get to the Splunk indexer? Are there transport or network issues that need to be addressed? |
| **Visibility / Access** | Security, IT Ops | Which individuals, teams or Splunk roles should be allowed access to this data? |
| **Searching** |  | How often will this data be searched or accessed? Will this data be used for alerts? |
| **Compression** |  | Actual/estimated compression ratio |

|  |  |  |
| --- | --- | --- |
| **Data Source** | Linux Logs | Give this input or data source a name. |
| **Description:** |  | Provide a brief description of this input. What is the nature of the data? |
| **Ownership** |  | Who is the owner of this data? |
| **File Name** |  | Provide the file name, if applicable |
| **Location:**  **Server(s):**  **Directory:**  **Scripted Input:**  **API:**  **Network port:** | All locations | Where is the data located? Is this data in a file? Can it be obtained via an API, network port, etc.? If the data must be obtained from an API, attach a description of the method for collecting the data - or supply a script to collect the data. |
| **Data Volume:**  **Average per day:**  **Peak:** |  | Are there special conditions that will cause a peak in data? Are there predictable patterns to the data volume? Does it vary by host? |
| **Retention:**  **Legal Requirement**  **Business Requirement**  **Search Requirement** | 90 days | How long must data be kept online? How often will offline data need to be retrieved for forensic purposes? What should be done with the data when it is archived out of Splunk? |
| **Legal Compliance** |  | Are there any laws or regulations that affect the collection, retention or accessibility of this data? |
| **Integrity** |  | Are there any special considerations for data integrity? Should the events be encrypted or auditable via Splunk? |
| **Format or sourcetype** |  | Describe the format of the data. Add additional pages with detailed field formatting information, if available. Provide the sourcetype if known. |
| **Timestamp** |  | Does the data contain a timestamp? If not, how should Splunk determine the time of the events? |
| **Collection Method** |  | How will this data get to the Splunk indexer? Are there transport or network issues that need to be addressed? |
| **Visibility / Access** | Security, IT Ops | Which individuals, teams or Splunk roles should be allowed access to this data? |
| **Searching** |  | How often will this data be searched or accessed? Will this data be used for alerts? |
| **Compression** |  | Actual/estimated compression ratio |

|  |  |  |
| --- | --- | --- |
| **Data Source** | Windows Logs | Give this input or data source a name. |
| **Description:** |  | Provide a brief description of this input. What is the nature of the data? |
| **Ownership** |  | Who is the owner of this data? |
| **File Name** |  | Provide the file name, if applicable |
| **Location:**  **Server(s):**  **Directory:**  **Scripted Input:**  **API:**  **Network port:** | San Francisco | Where is the data located? Is this data in a file? Can it be obtained via an API, network port, etc.? If the data must be obtained from an API, attach a description of the method for collecting the data - or supply a script to collect the data. |
| **Data Volume:**  **Average per day:**  **Peak:** |  | Are there special conditions that will cause a peak in data? Are there predictable patterns to the data volume? Does it vary by host? |
| **Retention:**  **Legal Requirement**  **Business Requirement**  **Search Requirement** | 90 days | How long must data be kept online? How often will offline data need to be retrieved for forensic purposes? What should be done with the data when it is archived out of Splunk? |
| **Legal Compliance** |  | Are there any laws or regulations that affect the collection, retention or accessibility of this data? |
| **Integrity** |  | Are there any special considerations for data integrity? Should the events be encrypted or auditable via Splunk? |
| **Format or sourcetype** |  | Describe the format of the data. Add additional pages with detailed field formatting information, if available. Provide the sourcetype if known. |
| **Timestamp** |  | Does the data contain a timestamp? If not, how should Splunk determine the time of the events? |
| **Collection Method** |  | How will this data get to the Splunk indexer? Are there transport or network issues that need to be addressed? |
| **Visibility / Access** | Security, IT Ops | Which individuals, teams or Splunk roles should be allowed access to this data? |
| **Searching** |  | How often will this data be searched or accessed? Will this data be used for alerts? |
| **Compression** |  | Actual/estimated compression ratio |

|  |  |  |
| --- | --- | --- |
| **Data Source** | Symantec logs | Give this input or data source a name. |
| **Description:** |  | Provide a brief description of this input. What is the nature of the data? |
| **Ownership** |  | Who is the owner of this data? |
| **File Name** |  | Provide the file name, if applicable |
| **Location:**  **Server(s):**  **Directory:**  **Scripted Input:**  **API:**  **Network port:** | San Francisco | Where is the data located? Is this data in a file? Can it be obtained via an API, network port, etc.? If the data must be obtained from an API, attach a description of the method for collecting the data - or supply a script to collect the data. |
| **Data Volume:**  **Average per day:**  **Peak:** |  | Are there special conditions that will cause a peak in data? Are there predictable patterns to the data volume? Does it vary by host? |
| **Retention:**  **Legal Requirement**  **Business Requirement**  **Search Requirement** | 90 days | How long must data be kept online? How often will offline data need to be retrieved for forensic purposes? What should be done with the data when it is archived out of Splunk? |
| **Legal Compliance** |  | Are there any laws or regulations that affect the collection, retention or accessibility of this data? |
| **Integrity** |  | Are there any special considerations for data integrity? Should the events be encrypted or auditable via Splunk? |
| **Format or sourcetype** |  | Describe the format of the data. Add additional pages with detailed field formatting information, if available. Provide the sourcetype if known. |
| **Timestamp** |  | Does the data contain a timestamp? If not, how should Splunk determine the time of the events? |
| **Collection Method** | All end user systems interact with the Symantec EndPoint (EP) manager | How will this data get to the Splunk indexer? Are there transport or network issues that need to be addressed? |
| **Visibility / Access** | Security, IT Ops | Which individuals, teams or Splunk roles should be allowed access to this data? |
| **Searching** |  | How often will this data be searched or accessed? Will this data be used for alerts? |
| **Compression** |  | Actual/estimated compression ratio |

|  |  |  |
| --- | --- | --- |
| **Data Source** | Web logs | Give this input or data source a name. |
| **Description:** |  | Provide a brief description of this input. What is the nature of the data? |
| **Ownership** |  | Who is the owner of this data? |
| **File Name** |  | Provide the file name, if applicable |
| **Location:**  **Server(s):**  **Directory:**  **Scripted Input:**  **API:**  **Network port:** | Ashburn COLO | Where is the data located? Is this data in a file? Can it be obtained via an API, network port, etc.? If the data must be obtained from an API, attach a description of the method for collecting the data - or supply a script to collect the data. |
| **Data Volume:**  **Average per day:**  **Peak:** |  | Are there special conditions that will cause a peak in data? Are there predictable patterns to the data volume? Does it vary by host? |
| **Retention:**  **Legal Requirement**  **Business Requirement**  **Search Requirement** | 90 days | How long must data be kept online? How often will offline data need to be retrieved for forensic purposes? What should be done with the data when it is archived out of Splunk? |
| **Legal Compliance** |  | Are there any laws or regulations that affect the collection, retention or accessibility of this data? |
| **Integrity** |  | Are there any special considerations for data integrity? Should the events be encrypted or auditable via Splunk? |
| **Format or sourcetype** |  | Describe the format of the data. Add additional pages with detailed field formatting information, if available. Provide the sourcetype if known. |
| **Timestamp** |  | Does the data contain a timestamp? If not, how should Splunk determine the time of the events? |
| **Collection Method** |  | How will this data get to the Splunk indexer? Are there transport or network issues that need to be addressed? |
| **Visibility / Access** | Security, IT Ops, Sales Support | Which individuals, teams or Splunk roles should be allowed access to this data? |
| **Searching** |  | How often will this data be searched or accessed? Will this data be used for alerts? |
| **Compression** |  | Actual/estimated compression ratio |

|  |  |  |
| --- | --- | --- |
| **Data Source** | e-commerce logs | Give this input or data source a name. |
| **Description:** |  | Provide a brief description of this input. What is the nature of the data? |
| **Ownership** |  | Who is the owner of this data? |
| **File Name** |  | Provide the file name, if applicable |
| **Location:**  **Server(s):**  **Directory:**  **Scripted Input:**  **API:**  **Network port:** | Ashburn COLO | Where is the data located? Is this data in a file? Can it be obtained via an API, network port, etc.? If the data must be obtained from an API, attach a description of the method for collecting the data - or supply a script to collect the data. |
| **Data Volume:**  **Average per day:**  **Peak:** |  | Are there special conditions that will cause a peak in data? Are there predictable patterns to the data volume? Does it vary by host? |
| **Retention:**  **Legal Requirement**  **Business Requirement**  **Search Requirement** | 1 year | How long must data be kept online? How often will offline data need to be retrieved for forensic purposes? What should be done with the data when it is archived out of Splunk? |
| **Legal Compliance** |  | Are there any laws or regulations that affect the collection, retention or accessibility of this data? |
| **Integrity** |  | Are there any special considerations for data integrity? Should the events be encrypted or auditable via Splunk? |
| **Format or sourcetype** |  | Describe the format of the data. Add additional pages with detailed field formatting information, if available. Provide the sourcetype if known. |
| **Timestamp** |  | Does the data contain a timestamp? If not, how should Splunk determine the time of the events? |
| **Collection Method** |  | How will this data get to the Splunk indexer? Are there transport or network issues that need to be addressed? |
| **Visibility / Access** | Security, Sales Support | Which individuals, teams or Splunk roles should be allowed access to this data? |
| **Searching** |  | How often will this data be searched or accessed? Will this data be used for alerts? |
| **Compression** |  | Actual/estimated compression ratio |