Newer Cisco SBA for Government Guides Available

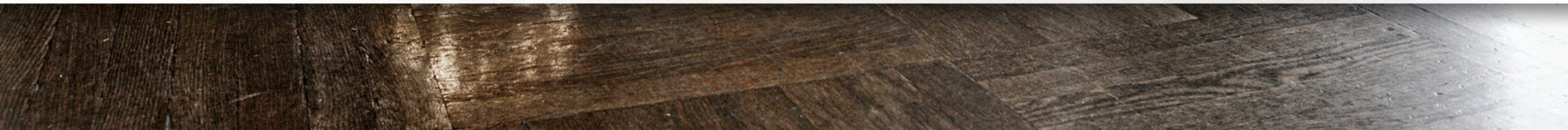
This guide is part of an older series of Cisco Smart Business Architecture for Government. To access the latest Cisco SBA for Government Guides, go to http://www.cisco.com/go/govsba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

Splunk SIEM Partner Guide

SBA FOR GOVERNMENT

Revision: H2CY10



The Purpose of this Document

This guide describes how to deploy Splunk security information and event management with Cisco security products.

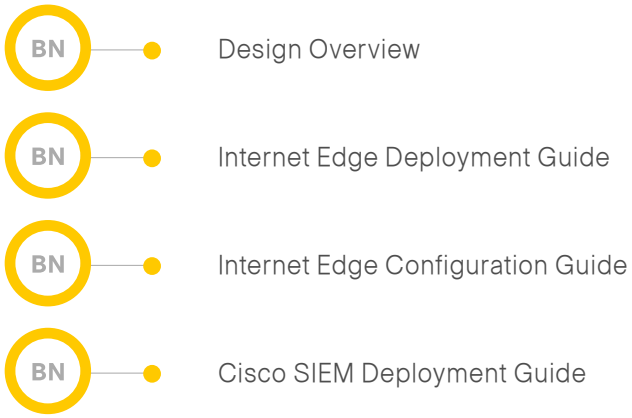
Who Should Read This Guide

This document is for the reader who:

- Has read the *Cisco Security Information and Event Management Deployment Guide* and the *Internet Edge Deployment Guide*.
- Wants to connect Borderless Networks to a Splunk solution
- Wants to gain a general understanding of the Splunk solution
- Has a level of understanding equivalent to a CCNA® Security certification
- Wants to solve compliance and regulatory reporting problems
- Wants to enhance network security and operations
- Wants to improve IT operational efficiency
- Wants the assurance of a validated solution

Related Documents

Before reading this guide



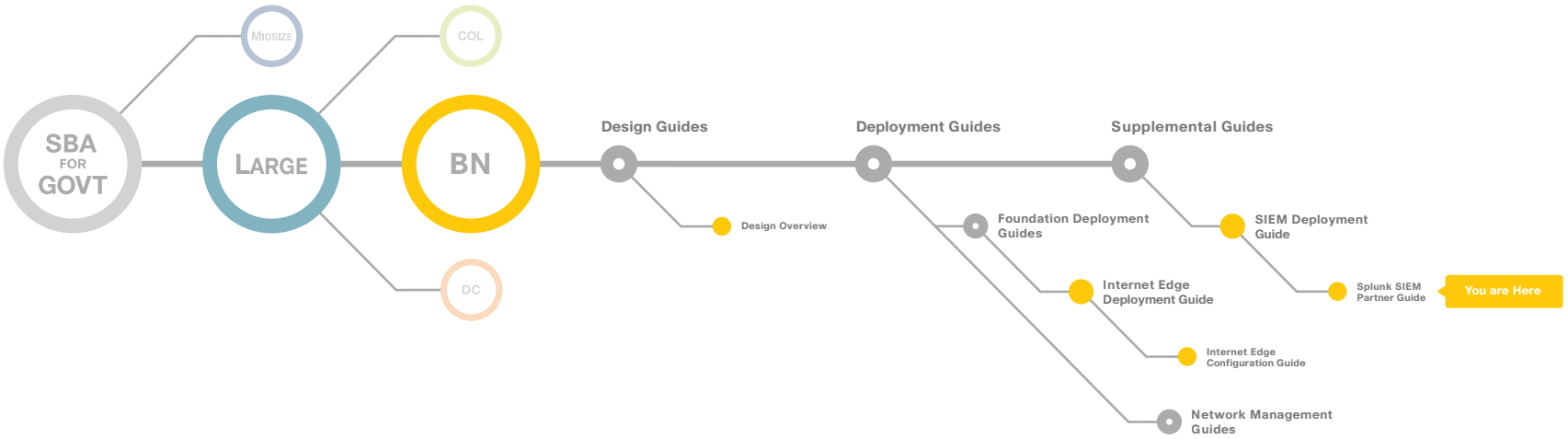
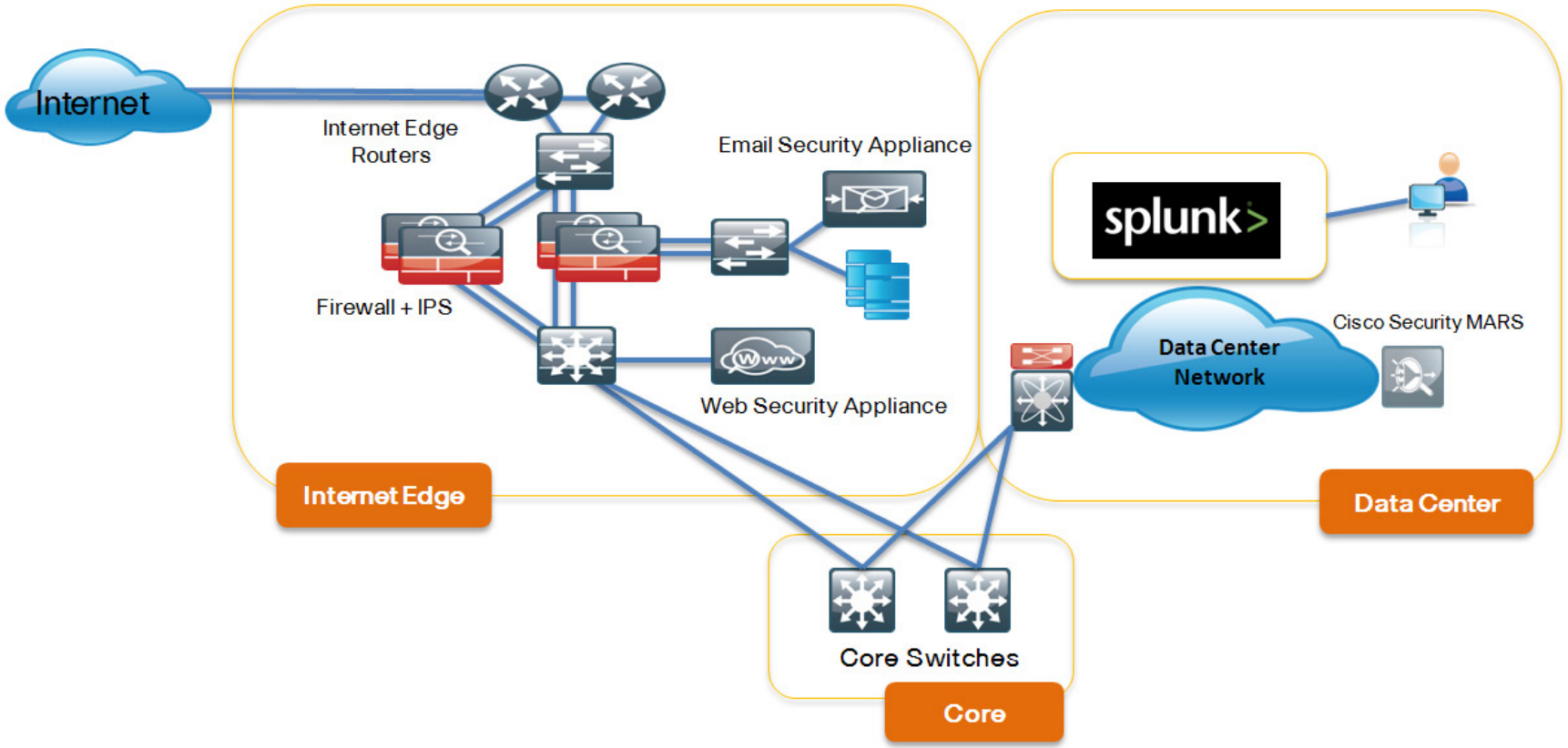


Table of Contents

Cisco SBA Overview

Cisco Smart Business Architecture (SBA) for Government Large Agencies—Borderless Networks (BN) offers partners and customers valuable network design and deployment best practices; helping agencies deliver superior end-user experience that include switching, routing, security and wireless technologies combined with the comprehensive management capabilities for the entire system. Customers can use the guidance provided in the architecture and deployment guiudes to maximize the value of their Cisco network in a simple, fast, affordable, scalable and flexible manner.

Figure 1. Splunk Integrated into Cisco SBA for Large Agencies—Borderless Networks



The modular design of the architecture means that technologies can be added when the agency is ready to deploy them. The architecture also provides Cisco-tested configurations and topologies which CCNA-level engineers can use for design and installation, and to support agency needs

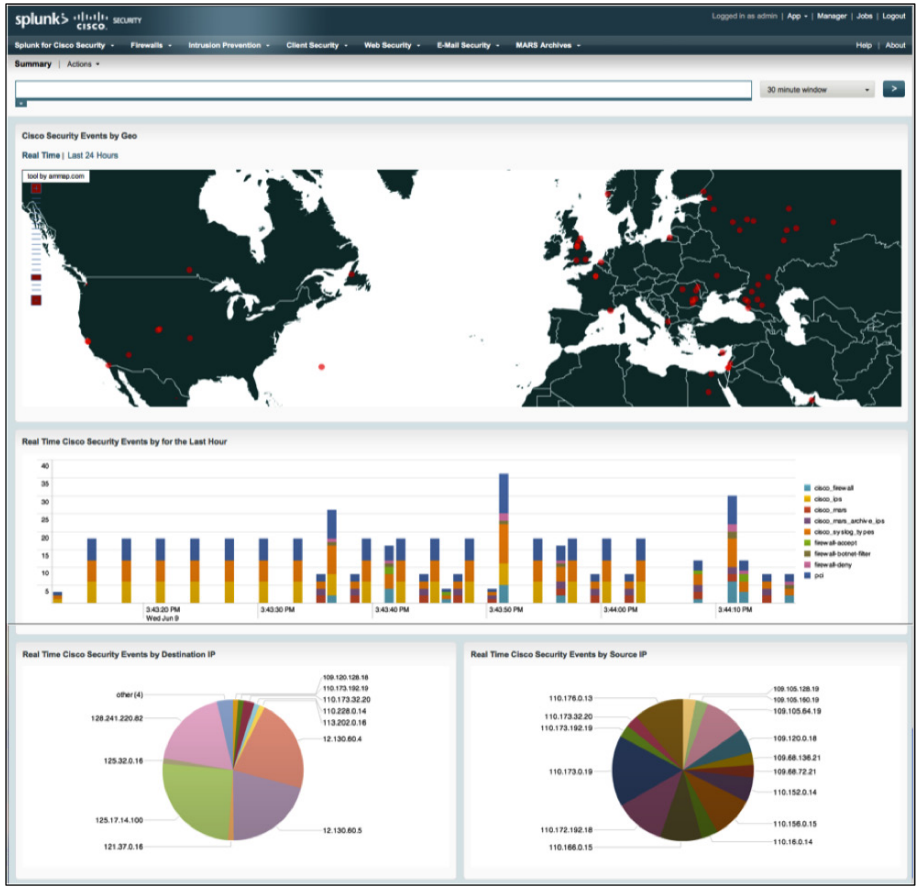
Cisco offers a number of options to provide security management capabilities. This guide is focused on our partnership with Splunk to provide an affordable, easy-to-use security management solution.

What is Splunk?

Splunk is software that provides a unique view across your entire IT infrastructure from one place and in real time. Splunk enables you to search, report, monitor and analyze streaming and historical data from any source, and speeds investigation of security incidents. Critical systems can be monitored to avoid service degradation or outages and compliance is delivered at lower cost. New operational insights are gleaned from your IT data.

Splunk can index any time-stamped ASCII text with none of the typical device support and new version restrictions seen from other products that accept log data. If new versions of Cisco data sources are released, Splunk makes the data sources available to you indexed and ready for use. You choose when and where to use the new data. Splunk also accepts multi-line application data without the need for translators or connectors.

Figure 2. Splunk for Cisco Security Real-Time Dashboard



Agency Benefits

Splunk helps its customers make better operational decisions by taking machine generated data and applying a forensics and analytics approach to security and event management as well as IT operations management.

- Any time-stamped ASCII text machine generated data can be indexed with Splunk, including custom application logs.
- Splunk's search language includes analytical commands used to create tables, counts, charts, and other objects that help make data compelling.
- Time charts and other graphical trending elements used in dashboards that can provide executives with a risk management picture customized to your data and your operational requirements.
- Splunkbase provides apps and add-ons to improve the user experience and provide out-of-the-box solutions to use cases.
- Splunk breaks down barriers between the IT operations and security teams, resulting in faster problem resolution.
- Security and application data can be viewed in context, and data trends examined, so that key performance indicators (KPIs) can be established and outliers identified.

Security Benefits

Splunk supports a forensics approach to security event management. Looking for patterns in log data from Cisco security devices and viewing them in context of other log data provides a comprehensive view of what's happening in your IT architecture. Using Splunk, the security team can harness their knowledge to model attack vectors and attack patterns based on conditions that might be see in log data can be modeled in Splunk.

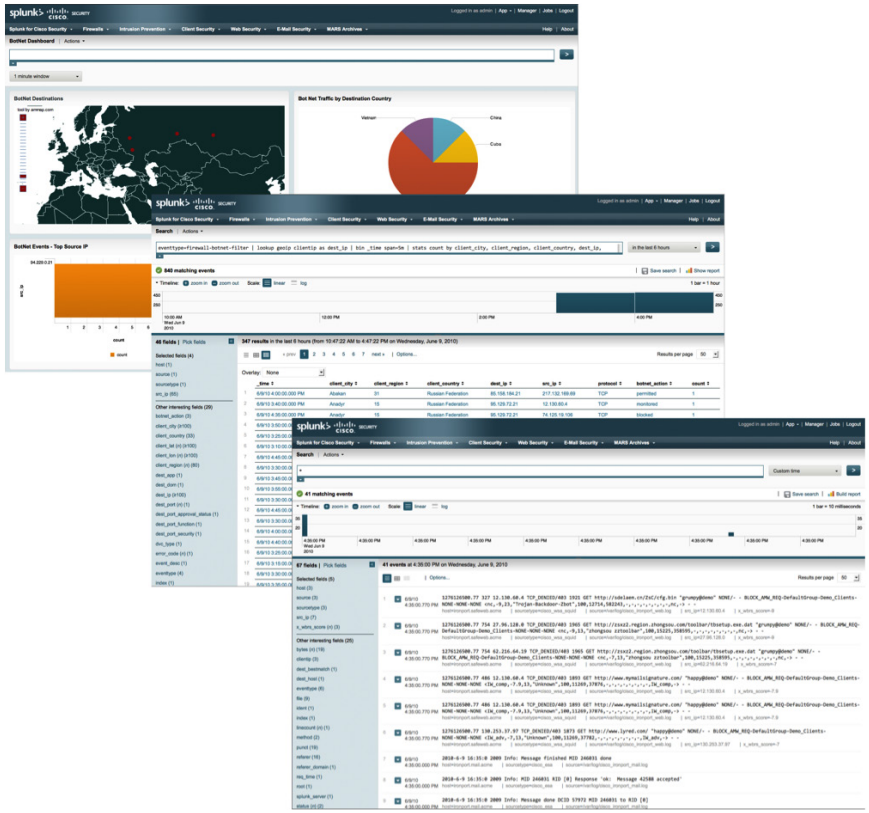
Examples:

- Review the series of events documented in log data that take place from the moment a piece of malware is downloaded into the environment.
- Set Splunk to report on levels of traffic between hosts or network segments that do not ordinarily communicate with each other.
- Augmentation of a data loss prevention system (DLP) by monitoring email traffic levels between individuals and the amount or size of attachments sent.

Depending on the environment, each of these scenarios can include one or more Cisco security solutions.

Splunk does not force the user to make compromises on what data the security team can collect due to either schema or scalability issues. When a search across data sources is constructed, the user can save, run, and send the search results and graphical reports to others in PDF format on a scheduled basis. The search can also become a security dashboard element for display. Existing Splunk customers use this display in their security operations center.

Figure 3. Drill Down from Graph to Report to Log Data



To add additional context to security events, Splunk has the ability to connect to external sources of data and pull this data into reports or dashboards in Splunk. Augmenting security data with information from an asset database about the asset owner, email, phone number, location, or department can help decrease response times. Asset databases also may contain information about asset classifications, priority, or whether the host has personal information on it. This information can also be displayed in Splunk.

- Splunk breaks down silo barriers between the IT operations and the security teams resulting in faster problem resolution.
- Direct drill-down from any part of a dashboard to the underlying logs speeds security investigations (Figure 3).
- Additional information from other data sources such as personnel databases, Active Directory, or asset management databases can be pulled into Splunk to add context to security and operations events.
- Search results from a security investigation—whether from single or multiple log sources—can immediately be turned into condition that can be monitored in real-time.

IT Operations Benefits

Understanding the effect of security issues on the IT operations team is critical for the reliability of key operational systems. Issues that affect top line revenue such as being able to receive orders for goods and services and reputation issues that could result from the loss of private data get visibility at the highest levels of the agency.

Splunk's ability to consume and report on application data and security data together dramatically speeds up forensics investigations. There are cases where operations and security teams have separate troubleshooting systems, which keep these teams in separate silos. This makes it harder for root cause analysis to be determined. The question "is it an application issue or a security issue," can take hours to completely comprehend. Being able to use the same system to understand the effect of security issues on mission critical applications and the data they contain is key to all tenets of security—confidentiality, integrity and availability.

- Splunk can provide a single pane of glass for the security and IT operations teams.
- Splunk can help the team understand and pinpoint infrastructure issues.
- Operational metrics and security metrics can be tied together enabling better operational decisions and metrics monitoring.

Splunk and Cisco working together have endeavored to provide a consolidated view into log data coming from some of the best and most popular Cisco security products while preserving the key capability of Splunk to accept and index any data from any source—including multiline application data—and apply analytics to searches resulting in new insight into security issues over time.

Technology Partner Product Overview

Splunk for Cisco Security consists of apps and add-ons to Splunk that are freely available on Splunk's website www.splunkbase.com. The Cisco apps and add-ons, once installed, provide the user with 12 dashboards and over 60 reports with views of historical data and real-time log data from Cisco security devices and software. This gives the user that has a Cisco-centric security environment situational awareness not only for each of these systems, but also in combinations that provide insight into security issues as they arise. The Cisco apps and add-ons are offered on a per solution basis so the user can download and install only those needed.

Figure 4. Main Menu Bar

The Cisco apps and add-ons are compatible with other apps and add-ons in Splunkbase. The user can download additional Apps or add-ons that are appropriate for their IT architecture. Once installed, the apps can be seen under the App pull down menu. The provided dashboards and reports are extensible. If the user want or needs additional reports, decides to re-arrange or add to a dashboard, or pull in contextual data from a third-party source, this is easily supported in Splunk.

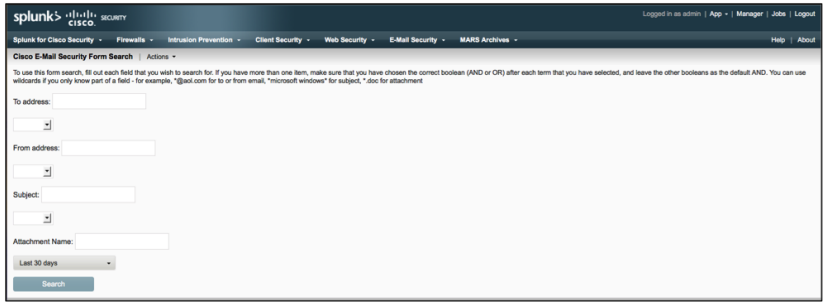
With the exception of the MARS archive, each supported Cisco solution has it's own overview dashboard and real-time information view. Any dashboard element or report can be clicked to provide a drill-down into the underlying log data and shows the data on a chronological timeline.

Solution Highlights

Cisco IronPort Email Security Appliance

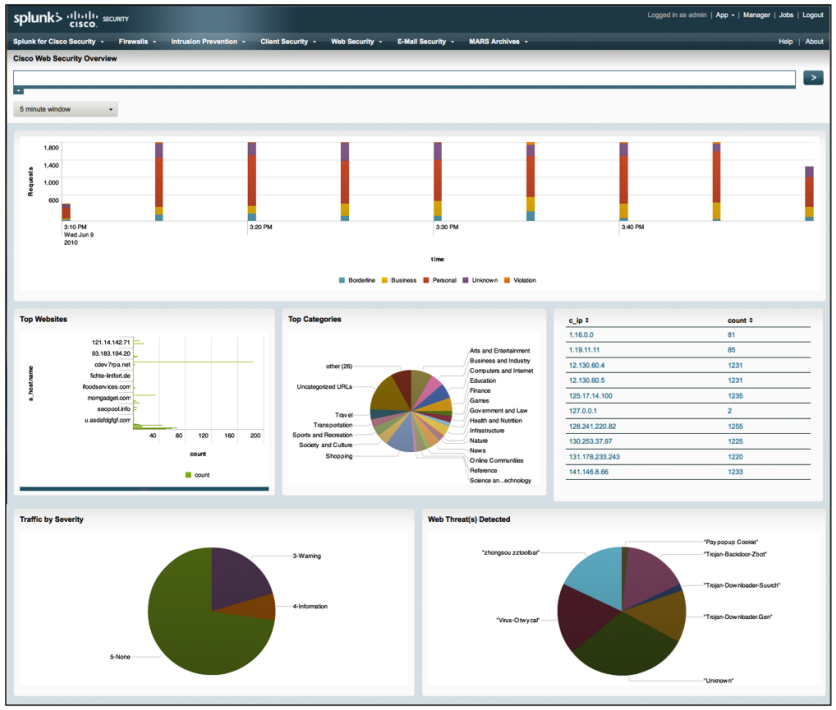
For all agencies email is a mission critical communications tool. Yet nearly 90% of email activity is invalid (spam, viruses, etc.). Because email is as an attack vector for viruses and other forms of malware, the security team needs to deploy a security solution that will provide appropriate protection against email-based attacks and cut the amount of invalid email traffic while still supporting the agency. The Cisco IronPort Email Security add-on makes transaction mining simple through form search dashboards that allow you to enter information about the mail transaction, sender, receiver and attachments and easily mine for any transaction nested in the Email Security Appliance logs. Splunk provides scalable, out-of-the-box reporting, and saved searches, that represent the most requested searches and analytics.

Figure 5. Cisco Email Form Search



Splunk and Cisco IronPort Web Security Appliance

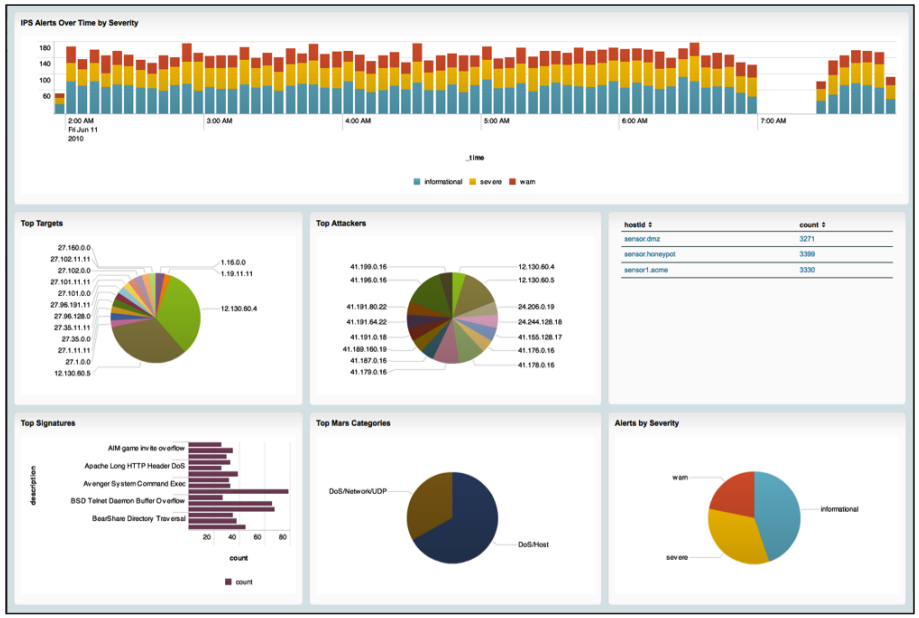
Figure 6. Cisco WSA Dashboard



The number of web-born security threats caused by simply surfing the Internet has reached record proportions. It's very easy for employees surfing the web to become complacent and click on a link that might result in the installation of a key-logger, root-kit, or some other form of malware. Surfing to certain destinations can violate appropriate use policies for employer-owned computer equipment. According to a recent survey, a rapid escalation in employee web surfing can be an indication of an employee that no longer values his or her employer's time, may be looking to leave the company and perhaps take proprietary company information with them. Splunk helps track and report on web surfing as reported by the Cisco IronPort Web Security Appliance (WSA). Splunk puts a human resources (HR) professional's perspective to work when analyzing data from WSA and supports security teams that regularly need to provide employee surfing histories as evidence in HR actions.

Splunk and Cisco Intrusion Prevention Systems

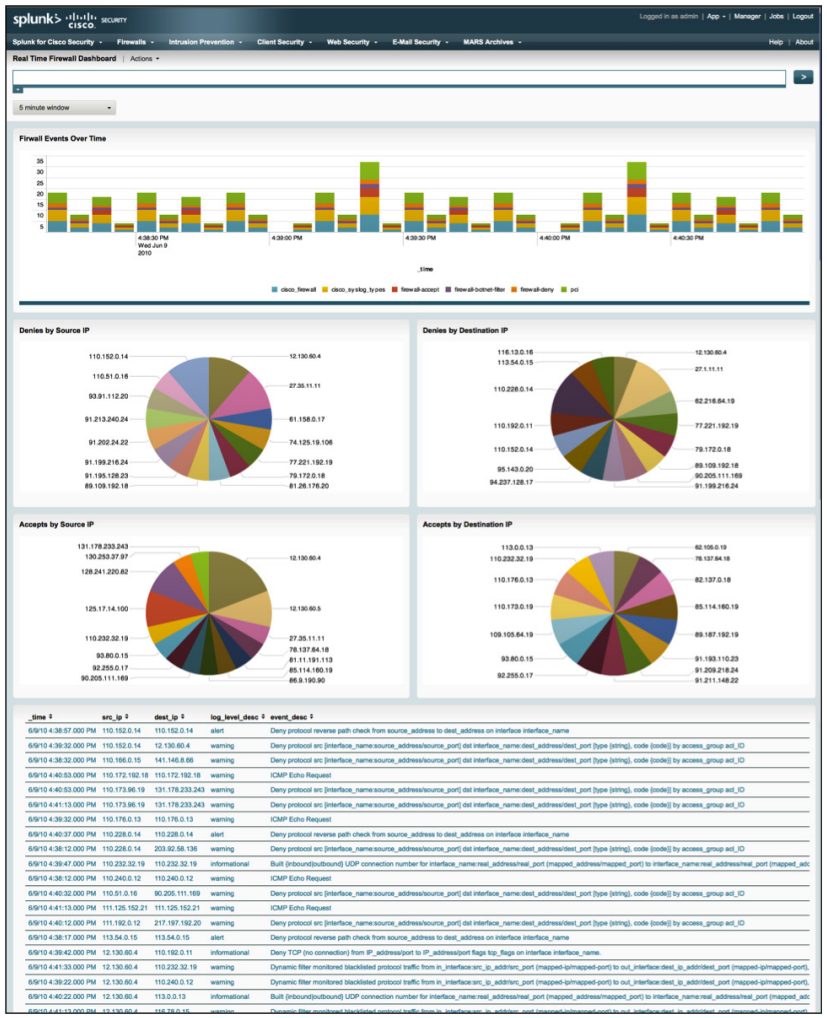
Figure 7. IPS Dashboard



Security Device Event Exchange (SDEE) is a specification for the message formats and the messaging protocol used to communicate the events generated by security devices. SDEE was implemented in the Cisco IPS 4200 Series Sensors beginning with v5.0, which in turn deprecated Cisco Remote Data Exchange Protocol (RDEP) for collecting Intrusion Prevention System (IPS) events. SDEE provides a richer level of reporting. IPS functionality is supported wherever the IPS module is implemented or installed. For example, Cisco routers and ASA 5500 Series Adaptive Security Appliances with an IPS module installed can also produce SDEE log data. The SDEE support extends to include Cisco's global threat correlation if available. The SDEE add-on provides a translation of the SDEE XML format to a key-value pair format easily understood by Splunk and is required for Splunk customers that need to view and report on IPS data.

Splunk for Cisco Firewall

Figure 8. Cisco Firewall Dashboard



The Cisco ASA 5500 Series Adaptive Security Appliance (ASA) represents an evolution that began with the Cisco PIX first released in 1994. As threats have evolved so has the Cisco perimeter firewall which in addition to firewall capabilities, includes IPS, VPN, and content security functionality. In the initial release of the firewall add-on, firewall and IPS log data (further addressed in the SDEE section) are collected and classified using tags, field extractions, and saved searches. Connections accepted and denied by port are just a small sample of the information available via the add-on.

Splunk for Cisco Security Wrapper

The Splunk for Cisco Security application is a wrapper app exposing additional searches, reports and dashboards from the supported Cisco add-ons. In addition, extended content supports Cisco's Global Threat Reputation and Botnet filtering features, and real-time geo-mapping of Cisco security events and attacks. Downloading and installing this add-on makes sense for those users that have two or more of the Cisco security solutions discussed above. The dashboards included in the wrapper reflect a richer experience for the security professional looking to perform root cause analysis.

The app requires you have the one or more of the supported add-ons installed:

- Splunk for Cisco Firewalls (add-on) http://www.splunkbase.com/apps/All/4.x/Add-On/app:Cisco+Firewalls+Add-On
- Splunk for Cisco IPS (add-on) http://www.splunkbase.com/apps/All/4.x/AddOn/app:Cisco+IPS+SDEE+Data+Collector
- Splunk for Cisco IronPort Web Security (app) http://www.splunkbase.com/apps/All/4.x/App/app:Cisco+IronPort+Web+Security+Application
- Splunk for Cisco IronPort Email Security (app) http://www.splunkbase.com/apps/All/4.x/Add-On/app:Cisco+IronPort+E-mail+Security+Add+On
- Splunk for Cisco Client Security Agent (add-on) http://www.splunkbase.com/apps/All/4.x/Add-On/app:Cisco+Client+Security+Agent+Add+On
- Splunk for Cisco Wrapper http://www.splunkbase.com/apps/All/4.x/App/app:Splunk+for+Cisco+Security
- Cisco Security MARS archives http://www.splunkbase.com/apps/All/4.x/app:Cisco+MARS+Archive+Add-on

Tech Tip

In order to automatically retrieve geographical info on public IP addresses you will need to install the MAXMIND Geo Location app on SplunkBase. The app can be found here: Geo Lookup Script http://www.splunkbase.com/apps/All/4.x/Add-On/app:Geo+Location+Lookup+Script

Cisco Product	Splunk Collection Method	
Log collection method	Splunk is scalable software that can be used as a lightweight forwarder, an indexer, and/or a search-head based on configuration settings.	
Number of Users (Admin)	Unlimited	
Cisco Devices (data format)	Syslog	
ASR	Syslog	
ASA	SDEE	
IPS	Syslog	
IOS	W3C	
ESA	Syslog (or Squid format)	
WSA	Syslog	
FWSM	Archive	
Cisco Security MARS		
Events Per Second	150,000+ depending on customer supplied hardware and solution architecture	Splunk scales to terabytes per day

Notes

Deployment Details

Splunk and the Cisco Applications and Add-Ons

This section outlines the steps required to configure the Splunk to process log data from Cisco devices, including the CS-MARS SEM product.

Process

Setting up Splunk

1. Splunk Installation Quickstart
2. Accepting Cisco Data Sources

Splunk will run on Windows, Linux, Solaris, Mac OS, FreeBSD, AIX, and HP-UX. This section provides an overview of how to set up Splunk on a single host. Additional information on scalability, using Splunk as a light-weight forwarder, and other Splunk documentation can be found on the Splunk website: (http://www.splunk.com/base/Documentation/latest/User/SplunkOverview).

Although much of what is described below are basic requirements for setting up Splunk for the first time, this document assumes that the user is setting up Splunk for the first time with additional Cisco Apps on a single four core commodity server with eight gigabytes of ram. The instructions below reflect running Splunk with a default Red Hat Linux installation.

Procedure 1 Splunk Installation Quickstart

Step 1: Install Splunk RPM.

To install the Splunk RPM in the default directory /opt/splunk:

rpm –i splunk_package_name.rpm

To install Splunk in a different directory, use the –prefix flag:

rpm –i –prefix=/opt/new_directory splunk_package_name.rpm

Step 2: Start Splunk. At the command prompt in a command shell type ./splunk start

After you start Splunk and accept the license agreement

Step 3: In a browser window, access Splunk Web at http://<hostname>:port.

- *hostname* is the host machine.
- *port* is the port you specified during the installation (the default port is 8000).

This will spawn two processes: Splunkd and Splunkweb

Step 4: The first time you log in to Splunk Enterprise, the default login details are:

Username: admin

Password: changeme

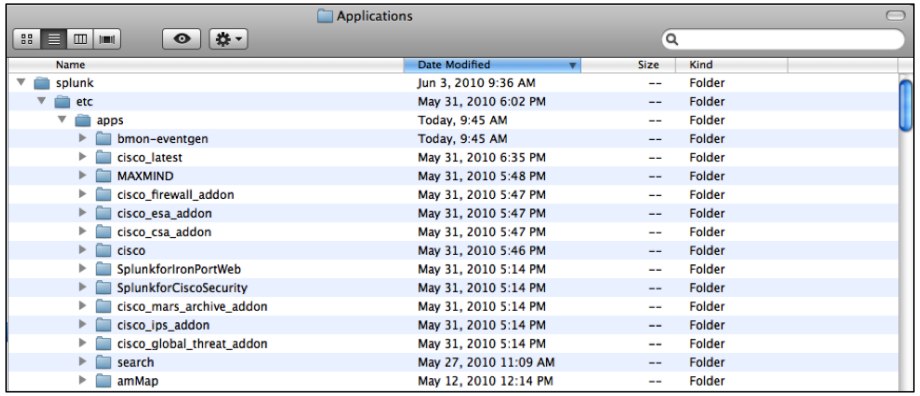
Tech Tip

The free version of Splunk does not have access controls. To switch from the free version to the paid version, purchase and apply the appropriately sized license.

Procedure 2 Accepting Cisco Data Sources

Each of the following apps and add-ons should be installed into the apps folder in the etc directory. For each app or add-on you install verify that the appropriate sourcetype is set when configuring the data input.

Figure 9. Apps installed into /splunk/etc/apps



Process

Receiving syslog from Cisco Firewalls

Step 1: To install this add-on, unpack this file into $SPLUNK_HOME/etc/apps and restart Splunk. In order to get the firewall data into Splunk you will need to configure a port on the Splunk server to listen for UDP or TCP traffic. Refer to http://www.splunk.com/base/Documentation/latest/admin/MonitorNetworkPorts for details on this process.

Step 2: Configure the firewall device to direct syslog traffic to the Splunk server. Refer to the Cisco Security Information Event Management Deployment Guide for details.

Step 3: (optional) The add-on will rename the sourcetype of your firewall events to cisco_firewall. If you have previously added Cisco Firewall data as a data source and would like to preserve the current sourcetype for reporting purposes, you can create an alias in the local directory of this app.

To create a sourcetype alias, add the following entry to props.conf under the local directory of this app ($SPLUNK_HOME/etc/apps/cisco_firewall_addon/local):

```
[cisco_firewall] rename = your_current_firewall_sourcetype
```

The field extractions are set to sourcetype=cisco_firewall which is keyed off of %ASA, %PIX and %FWSM. All of the reports use eventtype=cisco_firewall, the default cisco_firewall eventtype looks for %ASA, %PIX or %FWSM in your data.

The real time and overview dashboards as well as the included searches and reports in this add-on rely on the search: eventtype=cisco_firewall in order to report on firewall data. There is one scheduled search included in this add-on which creates an cache for the dashboard every 3 hours with a Splunk enterprise license.

To change the schedule you can edit the following search under the manager: Cisco Firewall – DataCube

Process

Receiving IPS Events Using SDEE

Step 1: To install this add-on, you will need to unpack this file into $SPLUNK_HOME/etc/apps create or modify local/inputs.conf and restart.

Step 2: Open the inputs.conf file located at $SPLUNK_HOME/etc/apps/cisco_ips_addon/local/inputs.conf

Step 3: Create an entry for each sensor you would like to monitor using the following stanza:

```
[script://$SPLUNK_HOME/etc/apps/cisco_ips_addon/bin/get_ips_
feed.py ]
sourcetype = cisco_ips_syslog
source = SDEE
disabled = false
interval = 1
```

The scripted input creates sensor_ip.run file in the $SPLUNK_HOME/etc/apps/cisco_ips_addon/var/run directory which is updated each time Splunk attempts to connect to a sensor. If you are having issues connecting to a sensor or are not seeing IPS data in Splunk the following search may be used for troubleshooting:

```
index="_internal" sourcetype="sdee_connection"
```

The real time and overview dashboards as well as the included searches and reports in this add-on rely on the search **eventtype=cisco_ips** in order to report on Cisco IPS data.

Tech Tip

Splunk creates an entry for each sensor you would like to monitor using the following stanza: **[script://$SPLUNK_HOME/etc/apps/cisco_ips_addon/bin/get_ips_feed.py <user> <pass> <ips_ip>]**

Step 4: (optional) There is one scheduled search included in this add-on which creates an cache for the dashboard every 3 hours with a Splunk enterprise license. To change the schedule you can edit the following search under the manager: Cisco IPS – DataCube

Process

Receiving Logs from a Cisco WSA

1. Getting WSA Data into Splunk
2. Extracting Relevant WSA Fields
3. Extracting Fields from W3C Format
4. Using Reports and Dashboards for Web Traffic
5. Configuring and Modifying Lookup Values

The reports and dashboards included in this app rely on eventtype="ironport_proxy" and all relevant fields in order to report on the Cisco IronPort Web Security Appliance data. By default, there is an ironport_proxy event type with: search = sourcetype=cisco_wsa*

If you already have IronPort web data in your Splunk index and are extracting the fields you can simply save an event type with the name ironport_proxy. You will still need to configure the lookups for your proxy logs. Instructions on how to do this can be found below under: Configuring and Modifying Lookup Values

If you already have IronPort web data in your Splunk index but do not have the fields extracted, you will find instructions on how to set up field extractions below under: Extracting Relevant IronPort Web Fields

Quick Start: If you have not indexed any IronPort web data and the logs are already accessible to your Splunk server in the squid format, you can simply create a data input that monitors the directory containing the squid formatted logs and set the sourcetype to cisco_wsa_squid

Procedure 1 Getting WSA Data into Splunk

Configure your Cisco IronPort WSA to schedule an export of the access logs to a directory accessible by the Splunk Server in either the squid or w3c format. The recommended interval for this is 15 minutes. Please note that the squid logging option provides a fixed format and the app includes field extractions for this. For the w3c format you will need to supply the field header in order for the app to function – this simple step is explained later on this document.

After the data is in a directory accessible by the Splunk server, you will need to configure a data input to monitor that directory instructions on how to configure a data input can be found here: http://www.splunk.com/base/Documentation/latest/Admin/WhatSplunkCanMonitor

When configuring the data input, you will need to select manual and set cisco_wsa_squid or cisco_wsa_w3c as the sourcetype value.

Tech Tip

If you exported the Cisco WSA access logs in the squid format and set the sourcetype to cisco_wsa_squid there is nothing more to configure at this point.

If you require an alternative name for the sourcetype due to naming conventions within your agency you will need to follow the steps below for configuring eventtypes and field extractions for already indexed IronPort web data.

Procedure 2 Extracting Relevant WSA Fields

The Splunk for Cisco IronPort WSA app contains field extractions for the squid formatted access logs. If you have already indexed the squid access logs under a different sourcetype, you will need to create sourcetype alias for the existing sourcetype, or map the field extractions and event type to your existing sourcetype. To create a sourcetype alias simply add the following entry to props.conf under the local directory of this app ($SPLUNK_HOME/etc/apps/SplunkforIronPortWeb/local):

```
[put_ironport_web_squid_sourcetype_here]
rename = cisco_wsa_squid
```

If you prefer to map your existing sourcetype to the field extractions and eventtype, add the following entry to props.conf under the local directory of this app ($SPLUNK_HOME/etc/apps/SplunkforIronPortWeb/local):

```
[put_ironport_web_squid_sourcetype_here]
KV_MODE = none
MAX_TIMESTAMP_LOOKAHEAD=19

REPORT-extract = squid
lookup_table = cat_lookup x_webcat_code_abbr
```

Add the following entry to eventtypes.conf under the local directory of this app ($SPLUNK_HOME/etc/apps/SplunkforIronPortWeb/local):

```
[ironport_proxy]
search = sourcetype=put_ironport_web_squid_sourcetype_here
```

Procedure 3 Extracting Fields from W3C Format

If your Cisco WSA access logs are in a W3C format you will need to create a DELIMS based extraction for this log format since this data is space delimited. The fields value for this extraction will be set to the header of your W3C logs. This is the order in which the fields were selected in the management interface. Alternatively the field values can be seen at the top of the W3C formatted log file.

To create the field extraction add the following entry to props.conf under the local directory of this app

($SPLUNK_HOME/etc/apps/SplunkforIronPortWeb/local):

[ironport-w3c] DELIMS = " " FIELDS = "time", "c_ip",field3",….,"field30" *be sure to list all of the fields included in the log.

Required fields: (The reports require the following fields to function properly)

- cs_username
- c_ip
- x_webcat_code_abbr
- x_webroot_threat_name
- x_wbrs_score
- sc_bytes
- cs_url

Procedure 4 Using Reports and Dashboards

Reports and dashboards are included to provide visibility into Acceptable Use/Compliance, Web Security Threats and Network Utilization. There are also form based reports for client profiling and analysis. Creating your own reports and dashboards is quick and easy in Splunk. Details on how to do this can be found here: http://www.splunk.com/base/Documentation/latest/User/AboutReportsAndCharts

The reports rely on the search eventtype=ironport_proxy and all of the required fields listed below. The Acceptable Use dashboards require lookups on usage against the x_webcat_code_abbr field.

The following is a list of the usage fields used by the Acceptable Use dashboards and reports:

- Business Usage (usage="Business")
- Productivity Loss (usage="Personal")
- Legal Liability (usage="Violation")
- Internet Tools (usage="Borderline")

Instructions on how to modify lookup values can be found below.

There are three scheduled searches included in this app which create a cache for the dashboards. They will run every 3 hours with a Splunk enterprise license. To change the schedule you can edit the following searches under the manager:

- Cisco WSA – Acceptable Use – DataCube
- Cisco WSA – Security – DataCube
- Cisco WSA – Network Resources – DataCube

Procedure 5 Configuring and Modifying Lookup Values

You can modify the usage and severity value for a particular category by editing the following file in the lookups directory of this app:

`$SPLUNK_HOME/etc/apps/SplunkforIronPortWeb/lookups/category_map.csv`

Process

Receiving Raw Events from Cisco Security MARS

To install this add-on, unpack this file into $SPLUNK_HOME/etc/apps and restart.

Step 1: Configure your MARS instance schedule an export of the raw message archive logs into a directory accessible by the Splunk Server.

Step 2: Once the data is in a directory accessible by the Splunk server, you will need to configure a data input to monitor that directory containing the MARS archive files. instructions on how to configure a data input can be found here: http://www.splunk.com/base/Documentation/latest/Admin/WhatSplunkCanMonitor

Step 3: When configuring the data input you will need to select manual and set cisco_mars_rm.

Step 4: There is one scheduled search included in this add-on which creates an cache for the dashboard every 3 hours with a Splunk enterprise license. To change the schedule you can edit the following search under the manager: Cisco MARS Archive – IPS – DataCube

Process

Receiving Logs from a Cisco IronPort Email Security Appliance

To install this add-on, unpack this file into $SPLUNK_HOME/etc/apps and restart. Next configure a data input to monitor your IronPort Mail logs setting the sourcetype to cisco_esa.

If you already have the IronPort Mail logs indexed under a different sourcetype you will need to update the props.conf and eventtypes.conf files in the local directory of this app.

Step 1: In props.conf create the following entry, replacing the stanza name with your own name for the sourcetype for your IronPort Mail logs:

[enter_sourcetype_here] REPORT-ironport = get_mid, get_to, get_from,

get_icid, get_dcid, get_attach_name, get_attach_size, get_subject1,

get_subject2, get_subject3

Step 2: In eventtypes.conf create the following entry, replacing the search terms with the sourcetype for your IronPort Mail logs:

[cisco_esa] search = sourcetype=your_usa_sourcetype tags = cisco e-mail security

The sample reports in this add-on rely on the search: eventtype=cisco_esa in order to report on IronPort mail data. There is one scheduled search included in this add-on which creates an cache for the dashboard every 6 hours with a Splunk enterprise license. To change the schedule you can edit the following search under the manager: Cisco IronPort E-mail – DataCube

Notes

Understanding Additional Splunk for Cisco Security Content: Landing Page

The landing page of the app provides an overall view of your Cisco security events in real time. While each add-on provides a real time dashboard where applicable the landing page is looking across all Cisco add-ons, plotting the events in real time as they happen, as well as providing an overview of the source and destination IP addresses involved.

There are two geo views available on the landing page: a real-time view and a cached view of the last 24 hours updated hourly. You may modify this view to include only the events or environments that are of interest to you. In order to modify the schedule or content of the event mapping search you will need to go into the Manager and edit: Event map

If you would like to create additional map content for use in Splunk dashboards please download the Splunk for amMap flash maps add-on and documentation located here: http://www.splunkbase.com/apps/All/4.x/Add-On/app:Splunk+for+use+with+amMap+Flash+Maps

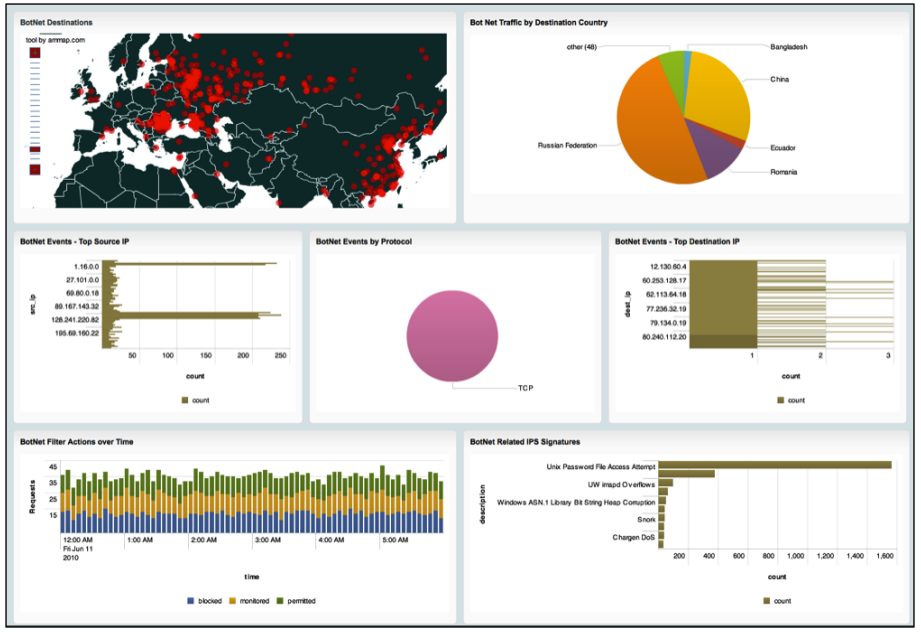
BotNet Overview

The BotNet Overview dashboard utilizes Cisco Firewall's BotNet filter, providing a view into the latest BotNet activity in your environment. This dashboard is driven off of a saved search that creates a cache for the dashboard every 3 hours with a Splunk enterprise license.

To change the schedule or the time frame reported on you can edit the following search under the manager: Cisco BotNet Filter – DataCube

The BotNet map included with this view is mapping the geo info from the destination IP of the BotNet request. This map is driven off of the results of Cisco BotNet Filter – DataCube. To make changes to the search schedule or that time frame simply edit the search.

Figure 10. BotNet Dashboard



Global Threat Correlation Overview

The Global Threat Correlation Overview dashboard is comprised of IPS alerts that surpass defined thresholds for a Global Threat Correlation Score. By default this is set to 0. This dashboard is driven off of a saved search that creates a cache for the dashboard every 3 hours with a Splunk enterprise license.

To change the schedule, the time frame reported on, or the GTS thresh-hold you can edit the following search under the manager: Cisco IPS Global Threat Correlation – DataCube.

Maintaining and Updating Splunk for Cisco Apps and Add-ons

Copies of all the Cisco Apps and add-ons can be found at www.splunkbase.com free of charge. For notifications of updates to the Cisco apps-and add-ons posted to Splunkbase, it is recommended that the user monitor the Splunkbase page via RSS. The RSS icon is located in the upper right part of the Splunkbase webpage.

Due to the modular nature of the apps and add-ons, updating and implementing new versions of Splunk over time does not adversely affect the installed adds or add-ons.

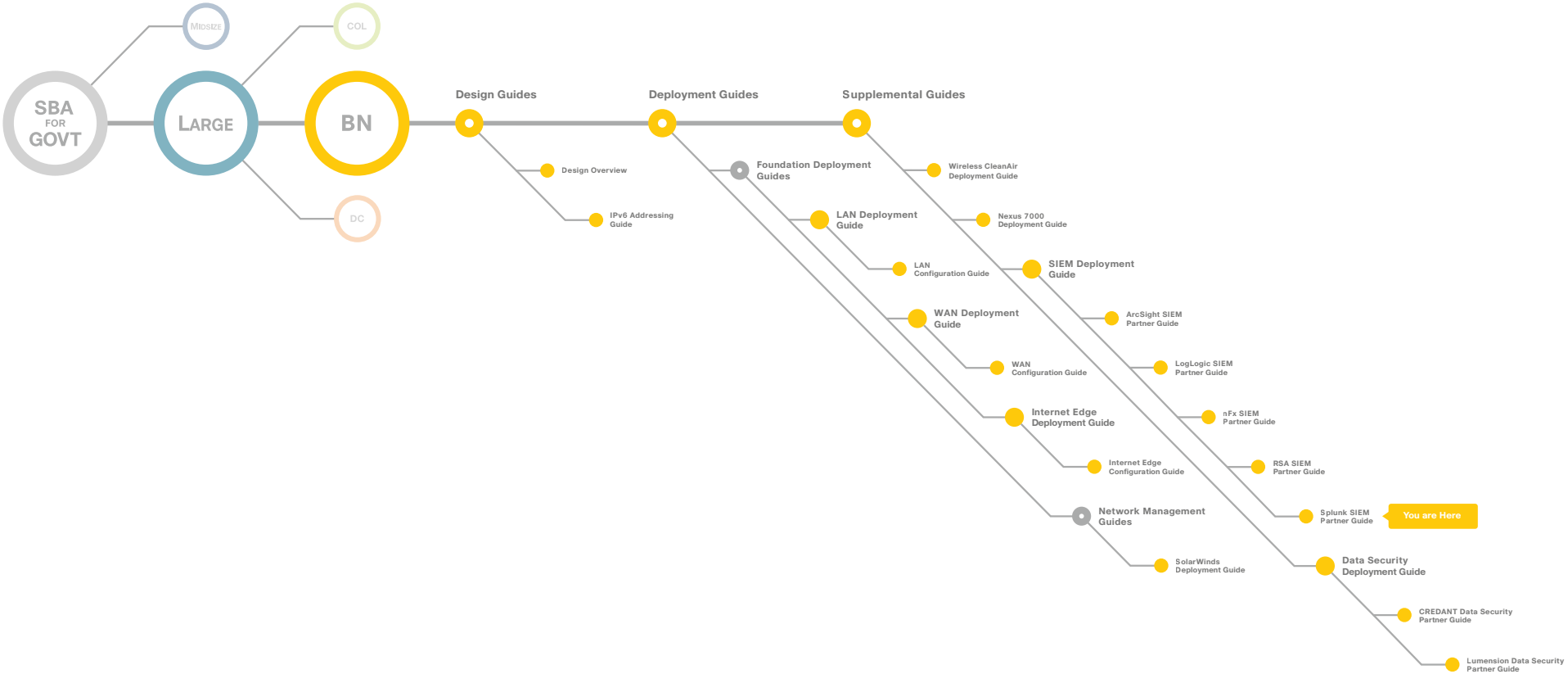
Products Verified with Cisco SBA

The Splunk for Cisco Security app version 4.1 has been verified with Cisco Cisco SBA using the following software versions:

- Cisco ASA 5500 Series 8.2(1)
- Cisco IOS Software Release 15.0(1)M2
- Cisco IOS XE Release 2.6.1
- Cisco Intrusion Prevention System 7.0.(2)E3
- Cisco IronPort AsyncOS Version 7.1 for Email
- Cisco IronPort AsyncOS Version 6.3 for Web
- Cisco Security MARS 6.0.5 .

Notes

Appendix A: SBA for Large Agencies Document System



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

C07-641104-00 02/11