CD R&T
Cyber Defense Research & Technology

PV&S
Project Vision & Scope

CASA

Whom do you trust?

The **Certificate Authority Situational Awareness** (CASA) application offers insights into the Certificate Authorities (CAs) currently trusted on a network. CASA is an analytics dashboard that leverages the Splunk framework to gather data from the Microsoft certificate store on network workstations and servers, synthesizes the data, and provides analytics and visualizations for cyber defenders and system administrators to easily identify unexpected or prohibited CAs across their networks.

Scope

The CASA project used data science and applied research to explore the x.509 standard certificate data fields, including ver 2/3 extended fields, to provide basic statistics, charts, visualizations, and search capabilities.

What's the gap?

There currently exists no effective method to collect and analyze certificate authority information across a network. This is currently a time-consuming process often requiring users to manually gather data from hosts individually.

Who cares?

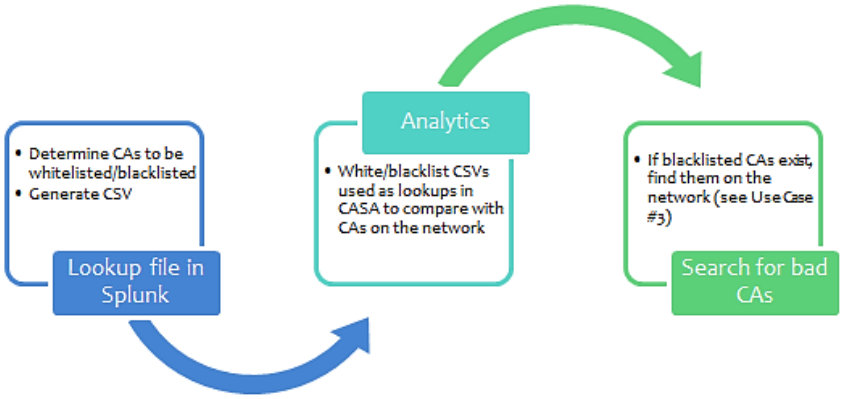
- *System Administrators can more effectively examine and manage CAs trusted on their networks.*
- *Cyber Defenders can easily check for CAs using outdated algorithms/key sizes, compare CAs against white/blacklists and more.*

So what?

CASA provides new insights and actionable intelligence about CAs on a network; an easy way to manage the collection of CA data as well as a central dashboard for visualizing the data, and easily identifying and physically locating CAs of interest.

Use Case #1

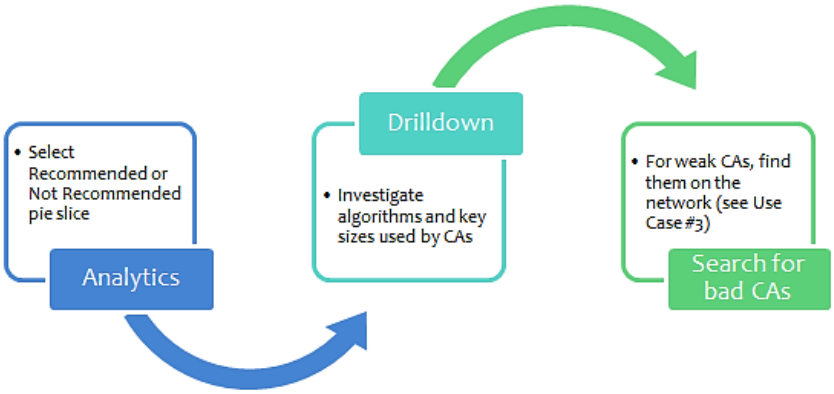
Compare network CAs to known white/black lists.



- By updating CASA's white/black lists regularly Cyber Defenders can easily identify unknown CAs on local machines
- Visiting the Analytics Dashboard and viewing the 'Status of Trusted CAs' Panel, a Cyber Defender effectively evaluate the networks Certificates Authorities against the white/black lists

Use Case #2

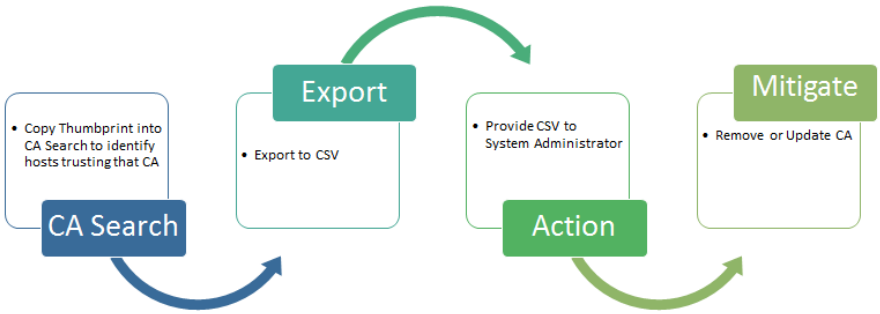
Finding CAs Vulnerable to Cryptographic Attacks.



- Algorithms and key sizes from NIST Special Publication 800-57 Part 3, Table 2-2 are used in CASA to identify the CAs that are not using the recommendations.
- Visiting the Analytics page and clicking the 'Not Recommended' pie chart slice of the 'CAs Using Recommended Algorithms/Key Sizes enables cyber defenders to identify non-compliant trusted CAs.

Use Case #3

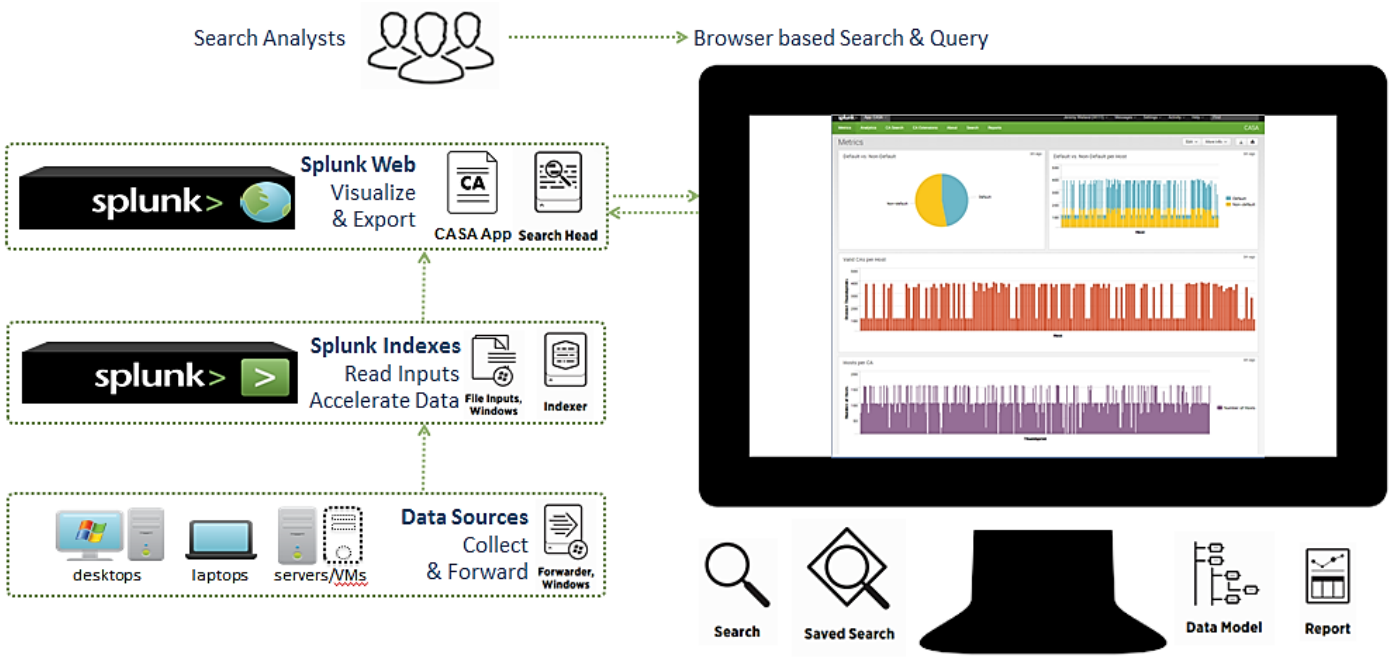
Find compromised CAs on the network.



- SUPERFISH used a self-signed root CA which made computers with it vulnerable to attack. Using the 'CA Search' panel enables the cyber defender to search for all hosts that trust the CA. A report can be generated to guide mitigation actions.

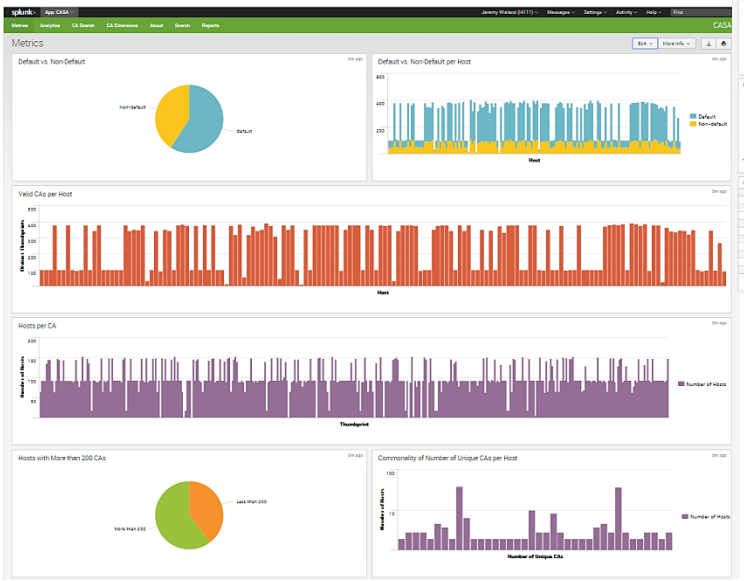
Splunk Implementation

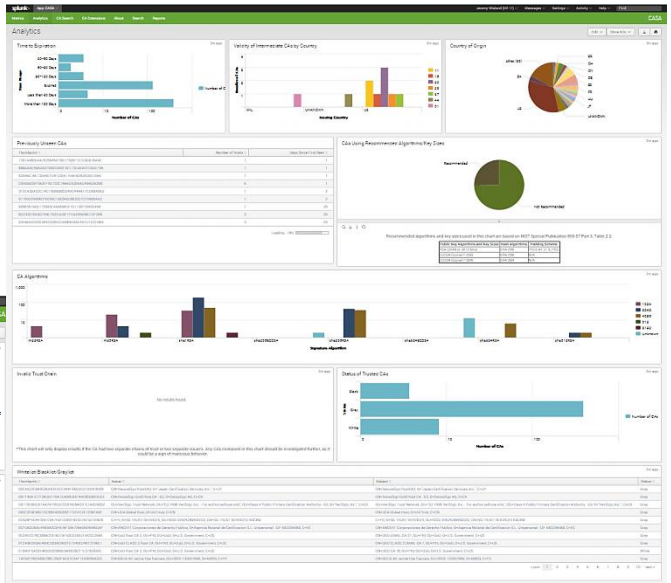
The CASA project is divided into two pieces, a Splunk app and a Splunk deployment app. The deployment app includes the configuration files for each endpoint to collect the certificate attributes from the Windows file system send the data to the Splunk indexer. The Splunk app contains the lookups, searches, and dashboards for the user.



Functional Dashboards:

Metrics Dashboard - The metrics dashboard contains numerous visualizations to assist the user in garnering some general information about the CAs across the network including: Number of CAs Per Host, Commonality of Number of Unique CAs per Host, Hosts with More than 200 CAs, Default vs. Non-Default, Default vs. Non-Default per Host, and Number of Hosts per CA.





Analytics Dashboard - The analytics dashboard contains nine panels geared towards analytics: Time to Expiration, Validity of Intermediate CAs by Country, Country of Origin, Previously Unseen CAs, CA Algorithms, CAs Using Recommended Algorithms/Key Sizes, Invalid Trust Chain, Status of Trusted CAs, and Whitelist/Blacklist/Graylist.