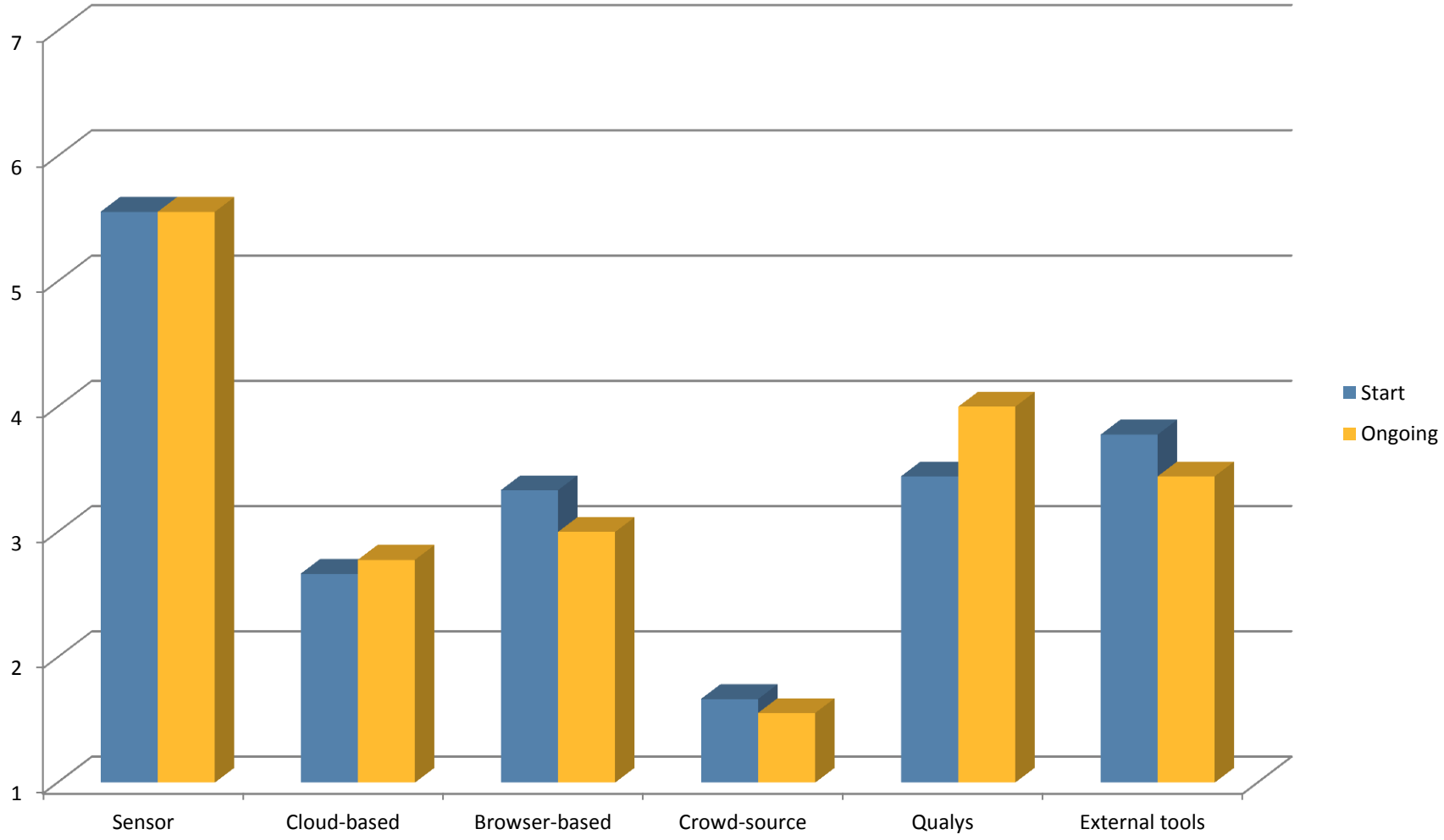
CIC Survey – July 2015
Alternatives for Certificate Discovery

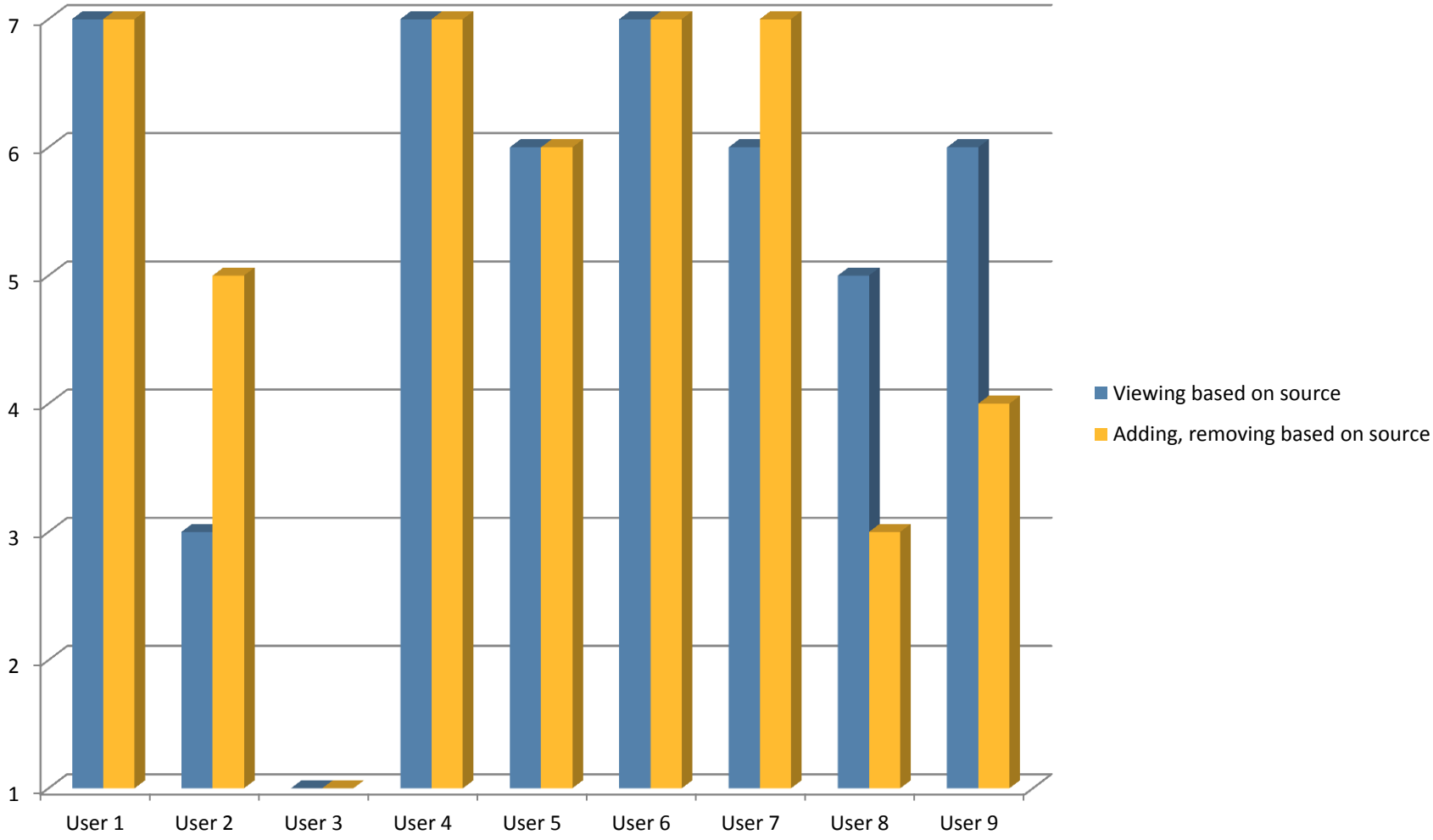
Lisa Kelly

CIC User Research

Alternatives for certificate discovery - Summary scores



Managing data based on source



Participants

User number	Participant	Company
User 1	Michael B.	CSG International
User 2	Kevin B.	FedEx
User 3	Incomplete	Unknown
User 4	Tim P.	The Capital Group Companies
User 5	Mark M.	Firemans Fund Insurance
User 6	Dominic B.	Marriot Vacations Worldwide
User 7	Yahia C.	Orange (Telecom)
User 8	Dennis J.	Liberty Mutual
User 9	Russel M.	State of Texas

Appendix 1 – Data by user

	User 1		User 2		User 3	User 4		User 5		User 6		User 7		User 8		User 9	
	Start	Ongoing	Start	Ongoing		Start	Ongoing	Start	Ongoing	Start	Ongoing	Start	Ongoing	Start	Ongoing	Start	Ongoing
Sensor	7	7	6	6	0	6	6	7	7	6	6	7	6	5	6	6	6
Cloud-based	1	1	6	6	0	7	7	1	1	1	1	2	4	2	2	4	3
Browser-based	3	2	4	4	0	7	7	3	2	3	4	3	3	1	1	6	4
Crowd source	3	2	4	4	0	2	2	1	1	1	1	2	2	1	1	1	1
Qualys	5	3	7	7	0	4	6	2	2	2	2	2	4	3	6	6	6
External tools	4	3	5	5	0	7	7	3	3	4	4	5	2	5	6	1	1

Appendix 2 – Questions asked

- Q1: What is your status with certificate discovery (CIC)?
  - We have discovered certificates using CIC sensors installed on our servers.
  - We plan to use certificate discovery, but have not installed CIC sensors, yet.
  - We haven't activated certificate discovery in our Managed PKI for SSL account.
- Q2: Please tell us why you haven't activated certificate discovery (Certificate Intelligence Center) in your Managed PKI for SSL account.
  - I just purchased it.
  - I am waiting for deployment approval.
  - I don't have the resources to support it.
  - I'm having trouble getting access.
  - Other (please specify).

Appendix 2 – Questions asked, cont.

- Q3: Please rate your level of interest in the following 6 methods, as an **initial process** to gather certificate data from your network.
  Ranking = 1 (not interested) to 7 = (very interested)

  - Cloud-based scanner
  - Qualys integration
  - Browser-based scanning
  - Crowd sourcing
  - Integration with external tools
  - Sensor-based scanning

Appendix 2 – Questions asked, cont.

- Q3: Please rate your level of interest in these same methods, as a **long-term permanent process** to gather certificate data from your network.
  Ranking = 1 (not interested) to 7 = (very interested)

  – Cloud-based scanner
  – Qualys integration
  – Browser-based scanning
  – Crowd sourcing
  – Integration with external tools
  – Sensor-based scanning

Appendix 2 – Questions asked, cont.

- Q4: If we gather and display certificate data from multiple sources, how important will the following features be? Ranking = 1 (not important) to 7 = (very important)
  - Viewing or filtering certificate data based on the source
  - Adding, suspending or removing data from some of the sources

Appendix 2 – Discovery definitions

Cloud-based scanner

This would be a scan by sensors hosted in the Symantec cloud. Symantec would manage how many of your public sites are scanned and how often the scans occur (based on the domains you have vetted in Managed PKI for SSL).

Features

- No software installation required
- May require configuration
- The data would be available immediately

Potential Drawbacks

- Only discovers certificates on your public sites

Appendix 2 – Discovery definitions, cont.

Qualys integration

Qualys is a third party tool used to scan your network. If you have Qualys installed, Symantec would use their API to leverage information from Qualys and pull it into CIC.

Features

- Leverages existing software installed on your network
- Can discover internal and external certificates

Potential Drawbacks

- Relies on a third party for data collection
- If issues arise, support would be more complex

Appendix – Discovery definitions, cont.

Browser-based scanning

A browser-based tool that you configure to scan sites on your network. The scan only works for network sites (public and private) that you can reach from your browser

Features

- Easy to install
- Can discover internal and external certificates
- Requires initial configuration and setup

Potential Drawbacks

- Slower performance
- Must manually initiate certificate discovery scans
- Can’t schedule recurring scans

Appendix 2 – Discovery definitions, cont.

Crowd sourcing

A browser-based tool that would analyze browsing history and scan for certificates on sites that you and other members of your company have accessed. Instead of manually configuring sites to scan, the list of sites would grow automatically based on browser history.

Features

- You don't have to specify which sites to scan.
- Works for any sites where you or other members of your company have access.
- Would discover internal and external certs

Potential Drawbacks

- Would mine all data accessed through browser
- Could have a lot of extraneous data
- Would require installing Symantec software in many browsers to get enough coverage of external and internal sites

Appendix 2 – Discovery definitions, cont.

Integration with external tools

There are tools you may have installed (for example, Symantec Control Compliance Suite, Symantec Endpoint Protection) that scan sites on your network. Symantec would leverage configuration options in these tools and create an API to discover certificates and display them in CIC. As an alternative to an API, we would bundle the sensor / browser tools as a part of the other products so you wouldn't have to install something separately for certificate discovery.

Features

- Leverages existing implementation
- May require time to customize
- Should be able to discover internal and external certs

Potential Drawbacks

- May not include as much data (for example, certificate details) in discovery results

Appendix 2 – Discovery definitions, cont.

Sensor-based scanning

This is the model we currently use for certificate discovery. Sensor software is installed on a host machine in your network and you use the CIC console to configure which network sites to scan.

Features

- Can discover internal and external certificates
- Fully integrated with CIC
- Provides full control over which sites are scanned and when they are scanned

Potential Drawbacks

- Requires installation and configuration
- May require changes to company firewalls and network permissions to communicate with the cloud