Operationalizing the CIS “Top 20” Critical Security Controls with Splunk Enterprise

Anthony Perez – Security Architect, Splunk
Roadmap for Today’s Session

- Framing our discussion
- The legacy challenge
- An approach for operationalization
- Impacts on security maturity
- Live Demonstration
Framing our Discussion
Organizational security should be viewed as a continuum versus an end-state

- Viewing security as a continuum positions organizations to focus on continuous improvement
  - “We can always improve something.”

- The security continuum concept can also drive introspection for organizations
  - “What is our security maturity today?”

- Introspection on an organization’s security maturity often feeds strategic thinking
  - “Let’s map out steps to raise our overall security maturity.”
Regardless of where an organization exists on the security continuum, their foundation should be built upon best-practices

- Accepting that foundational security is built upon best practices – We still need to identify what best practices actually are
- Organizations also need to establish policies and procedures aimed at keeping their best-practices relevant as the threat landscape changes
- Beyond policies and procedures, organizations need to establish a plan for operationalization of these best practices as well
The best-practices selected for that foundation should be rooted in the defense against current real-world threat activity

- The origins of the CIS controls map to a 2008 request from the Office of the Secretary of Defense to the NSA regarding help prioritizing the various controls available
  - This drove an “offense must inform defense” approach
- This approach persists in the CIS CSC
  - The CIS Controls are developed, refined, and validated by a community of leading experts from around the world

**Key Insight:**

“The National Governors Association recommends that states turn to the Critical Security Controls for a baseline of effective cybersecurity practices…”

National Governors Association
*Act and Adjust: A Call to Action for Governors for Cybersecurity*
September 2013
The best-practices selected for that foundation should be rooted in the defense against *current* real-world threat activity

- The origins of the CIS controls map to a 2008 request from the Office of the Secretary of Defense to the NSA regarding help prioritizing the various controls available
  - This drove an “offense must inform defense” approach

- This approach persists in the CIS CSC
  - The CIS Controls are developed, refined, and validated by a community of leading experts from around the world

**Key Insights:**
- The CIS controls are analogous to components of multiple US Federal information security frameworks such as FISMA, DFARS, and RMF
- The Controls also map closely to Australian Signals Directorate “Top 4” and ISO/IEC 27001
The Legacy Challenge
Best practices security recommendations have been around for some time, but operationalization remains fractured

- Googling for ideas on where to begin with operationalization returns uniformly unhelpful results

“Use these 10 solutions to gain visibility”

“Hire us to build you something from scratch”

“Run this scanner when you want to generate a report”

“Leverage your legacy SIEM to get some of the way there”
Best practices security recommendations have been around for some time, but operationalization remains fractured

- Googling for ideas on where to begin with operationalization returns uniformly unhelpful results

- Common comments/questions on operationalization include:
  - “This is such a big project, I have no idea where I should even start...”
  - “Why can’t I use my legacy SIEM?”
    - Rigid (data source-specific) and conventional security data only
  - “What about ES?”
    - Flexible, capable, but some organizations aren’t sized or structured to *need* ES for operations
An Approach for Operationalization
Three key ingredients are needed to effectively operationalize the CIS controls in your environment

- Data relevant to the controls
  - Device inventory
  - Software inventory
  - HW/SW configurations
  - Vulnerability scan results
  - Administrator activity

**Key Insight:**

*CIS states:*

- “Organizations that apply just the first five CIS Controls can reduce their risk of cyberattack by around 85 percent.”
- “Implementing all 20 CIS Controls increases the risk reduction to around 94 percent”

[https://www.cisecurity.org/critical-controls.cfm](https://www.cisecurity.org/critical-controls.cfm)
Three key ingredients are needed to effectively operationalize the CIS controls in your environment

- Data relevant to the controls
  - Device inventory
  - Software inventory
  - HW/SW configurations
  - Vulnerability scan results
  - Administrator activity

- Domain knowledge about your organization
  - System owners
  - Approved devices & software
Three key ingredients are needed to effectively operationalize the CIS controls in your environment

- Data relevant to the controls
  - Device inventory
  - Software inventory
  - HW/SW configurations
  - Vulnerability scan results
  - Administrator activity

- Domain knowledge about your organization
  - System owners
  - Approved devices & software

- Splunk Enterprise
Combining these ingredients can drive “quick win” visibility into security posture relevant to the CIS controls

- Basic steps for operationalization include:
  1. Ingest data relevant to the control categories into Splunk Enterprise
  2. Ensure that data is compliant with Splunk’s Common Information Model (CIM)
  3. Install the *CIS Critical Security Controls* app for Splunk
  4. Update lookup files within the app based on domain knowledge about your organization
What’s really making this possible on the backend?

- The Splunk Common Information Model (CIM)
  - The “Rosetta Stone” that provides data normalization

- CIM-compliant searches
  - Provide flexibility and vendor/data-agnostic visibility into the environment

- Splunk lookup files
  - Provide data enrichment – *specifically relevant to your organization*

- Open source Threat / IOC lists
Impact on Security Maturity
What impacts should organizations anticipate for their security maturity?

- **Visibility:**
  - *Holistic* visibility into your organization’s security posture with respect to best practices in near-time

- **Flexibility:**
  - Vendor / sourcetype-agnostic architecture (via CIM) builds in flexibility as your infrastructure and organization changes

- **Efficiency:**
  - Increased efficiencies from an operational perspective, freeing time for more value-add security activity

- **Federal Relevance:** The controls are analogous to components of multiple Federal security mandates such as FISMA, DFARS, and RMF
What should I expect based on my organization’s current security-maturity level?

- Organizations will gain utility regardless of where they exist on the security maturity continuum

- For nascent security programs
  - Quick time-to-value on best-practices tied to current real-world threats

- For mid-maturity security programs
  - + automation that creates efficiencies for smaller teams, enabling time for more value-add activities such as proactive analysis

- For high-maturity security programs
  - + consolidated reports and visualizations that are easily integrated into existing workflows
Live Demonstration
.conf2017 is coming to Washington, D.C.!

September 25-28, 2017
Walter E. Washington Convention Center

Reserve your seat for .conf2017 now through November 30th to get the super saver discount!

Reserve your spot today, pay later!


After registration opens, you will have 60 days to complete your registration to secure the super saver rate.

Visit the Information Kiosk in the Solution Pavilion!
Support Operation Homefront!

Collect 6 Sponsor Badges!

Earn Your 6 Sponsor Badges!

Splunk will donate $10 Dollars to Operation Homefront’s Holiday Meals for Military Families Program for every attendee that completes their mission of earning 6 sponsor badges. The program will provide meals to our local military families this holiday season.

Plus a bonus if we hit 350 number of completed missions. Splunk will double the $3,500 donation to $7,000!
Workshops: Get Splunk Hands-on Experience

Attend a Splunk Workshop

Upcoming Schedule

- December 1: Introduction to Splunk Enterprise
- December 14: Introduction to Splunk IT Troubleshooting
- January 11: Introduction to Splunk Enterprise Security
- January 11: NEW! Database Performance Tuning and Capacity Planning Workshop
- January 25: Introduction to Splunk IT Service Intelligence
- January 25: NEW! Splunk App Development Workshop

Location

- Splunk Office McLean, VA

Visit http://www.doyouknowsplunk.com/workshops

Visit the Information Kiosk in the Solution Pavilion!
Splunk User Groups - Connect with Local Splunkers

Northern Virginia
Meets the last 3rd Thursday of every month
https://usergroups.splunk.com/group/northern-virginia-splunk-user-group.html

DC
Meets the last Wednesday of every month
https://usergroups.splunk.com/group/washington-dc-splunk-user-group.html

Baltimore
Meets the 3rd Monday of every month
https://usergroups.splunk.com/group/baltimore-splunk-user-group.html

Visit the Information Kiosk in the Solution Pavilion!
Take the GovSummit Post Event Survey!

We value your feedback!

Take the post event survey on the iPads in the foyer starting at 2:30pm!