

Using Splunk to Comply With NIST

Standards and Get Authorization to Operate

Antonio (Tony) Porras | Attorney/Security Architect

Date | Washington, DC

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

► Antonio (Tony) Porras

Agenda

- ▶ The ATO process
- ▶ Review NIST standard
- ▶ Splunk ES and NIST
- ▶ Living with NIST ATO system
- ▶ Next steps

What is Authorization to Operate (ATO)

- ▶ ATO is agency specific
 - Agency is accepting the risk that your organization will run information system securely
 - ATO must be given before your system becomes operational
 - There are periodic re-inspections to make sure the risk level of your system has not changed
- ▶ The agency uses the NIST standards to evaluate the information system's security posture
 - NIST FIPS 199 is used to determine the potential impact level of the data loss if the data in the system is compromised
 - NIST 800-53 identifies the necessary controls needed to protect the data in the system based on the impact level determined by the analysis done using the NIST FIPS 199
 - NIST 800-37 outlines the Risk Management Framework (RMF) and the continuous monitoring of the security controls selected in NIST 800-53

ATO For Our System

- ▶ The system is built for DHS/CBP
 - It was one of the first inspection after high profile breach of OPM in 2015
 - New inspection team
 - Requirements not clearly settled
- ▶ The system has the highest FISMA classification because of the type of data we process is very sensitive
 - Confidentiality: High
 - Integrity: High
 - Availability: Moderate
- ▶ ATO deliverables
 - Demonstrate that our controls protect the data being process
 - Independent Vendor Verification
 - Vulnerability Testing

Rubber Meets the Road

► We have a small implementation team (5 people)

- Over 600 remote users all over the country
- Re-inspection every 6 months
 - Had to automate as much as possible

► Nature of our data is high value target

- Real threat of data loss
- Many security tools, some overlap
 - IPS, antivirus, multiple factor authentication
- Data segmentation

► Compliance

- Have to prove that we are doing what we say we are doing
- Very burdensome inspections

Our Approach

► Establish clear system boundary

- Traceability of all that data goes in and out of the system boundary
- Account for all the software and hardware that is inside the system boundary
- Track all user access to the data inside the system boundary

► Be able to protect our system from attacks

- Implement control systems that will protect the data
- Be able to react in real time or as close to real time to issues
- Quickly determine positive from false positive issues

► Demonstrate that the data is protected

- Be able to provide the government agency reports and data to prove that the data is being protected
- Re-inspection every 6 months

NIST FIPS Publication 199

- ▶ Requires Federal agencies to assess their information systems for 3 objectives
 - Confidentiality – A loss of confidentiality is the unauthorized disclosure of information
 - Integrity – A loss of integrity is the unauthorized modification or destruction of information
 - Availability – A loss of availability is the disruption of access to or use of the information
- ▶ The impact is categorized as
 - Low – The loss could be expected to have a limited adverse effect
 - Moderate – The loss could be expected to have a serious adverse effect
 - High – The loss could be expected to have a severe or catastrophic adverse effect
- ▶ The security controls needed to comply are based on the impact level of each category

Potential Impact	Definitions
Low	<p>The potential impact is low if—The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.⁷</p> <p>A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.</p>
Moderate	<p>The potential impact is moderate if—The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p> <p>A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.</p>
High	<p>The potential impact is high if—The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p> <p>A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.</p>

NIST Special Publication 800-53

- ▶ NIST 800-53 defines the controls available to secure an information system based on the impact level of the data that is being protected
- ▶ It's a living document and its changing as needed
 - Our first implementation started with revision 3
 - When revision 4 came out it added data privacy controls
- ▶ Current version is revision 4
 - Revision 5 is in public draft
 - Major change is that it will shift focus from addressing Federal systems to all systems
- ▶ DoD is requiring its suppliers to adhere to NIST 800-171
 - It's an 800-53 lite
- ▶ Currently 18 Control Families

NIST 800-53 Control Families

Control Families 800-53

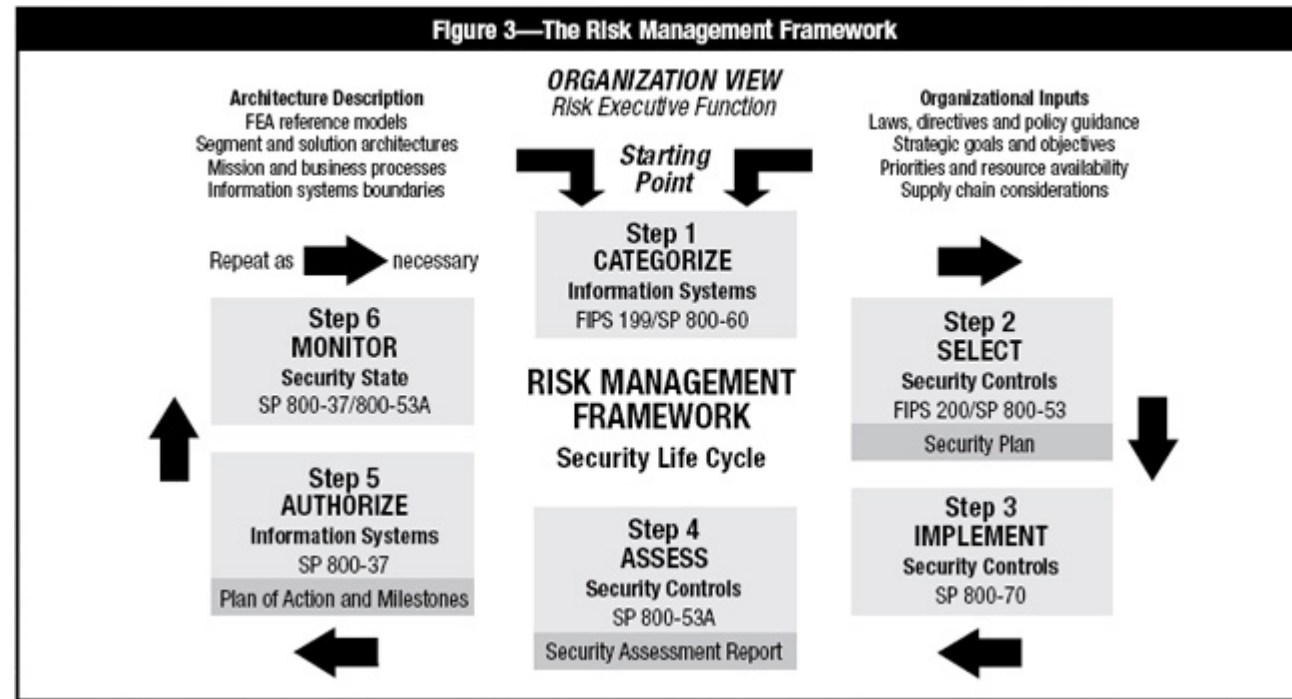
- ▶ AC - Access Control
- ▶ AU - Audit and Accountability
- ▶ AT - Awareness and Training
- ▶ CM - Configuration Management
- ▶ CP - Contingency Planning
- ▶ IA - Identification and Authentication
- ▶ IR - Incident Response
- ▶ MA - Maintenance
- ▶ MP - Media Protection
- ▶ RA - Risk Assessment
- ▶ CA - Security Assessment and Authorization
- ▶ SC - System and Communications Protection
- ▶ SI - System and Information Integrity
- ▶ SA - System and Services Acquisition
- ▶ PS - Personnel Security
- ▶ PE - Physical and Environmental Protection
- ▶ PL – Planning
- ▶ PM - Program Management

splunk>

.conf2017

NIST Special Publication 800-37

- NIST 800-37 outlines the Risk Management Framework (RMF) and the continuous monitoring of the security controls selected in NIST 800-53



Non-Government Agency NIST

- ▶ Federal Trade Commission (FTC) is becoming the cybersecurity police
 - Cybersecurity breaches are being seen as an “unfair or deceptive business practice in or affecting commerce”
 - In 2015, FTC brought an action against Wyndham Worldwide Corp. because it had been hacked 3 times and if failed to protect customer data
 - In 2016, FTC brought an action against ASUS for having critical security flaws in its routers and putting home networks at risk
 - In 2017, FTC brought an action against D-Link, alleging that inadequate security measures taken by the company left its wireless routes and internet cameras vulnerable to hackers
- ▶ FTC “Making sure companies keep their privacy promises to consumers”
 - Companies must have “Reasonable Security”
 - Reasonable security is what has been published by government agencies to protect systems
 - NIST Standards are the published and mandated government standards

Why NIST?

- ▶ National Institute of Standards and Technology (NIST) developed framework for approaching risk in information systems
- ▶ Biggest risk to information systems today?
- ▶ NIST has become the standard for cybersecurity frameworks
- ▶ NIST will become the de facto standard of care of Cybersecurity litigation
- ▶ Holistic approach for security

Splunk

► Evaluation

- Splunk Enterprise w/ FISMA App vs Splunk Enterprise Security

► Splunk ES

- Flexibility and adaptability to new and changing requirements
- Allowed us to start with a lot of controls that were covered with minor modifications and configuration (64 controls)
- Full SIEM capability to alert of possible threats
- Quick incident response investigations tracking
- Automate generation of reports to provide evidence of our implementation

► Government agencies are using Splunk

- Common language to communicate

Splunk ES and NIST 800-53

- ▶ Implemented ES as the top level reporting tool
 - Ability to change security tools without changing reporting
 - Many security tools: IPS, Antivirus, HIDS, 2 Factor, Firewalls
 - Able to meet the log requirements
- ▶ We are required to implement and monitor 507 controls
 - 64 are directly mapped to ES out of the box
 - Can probably increase in next re-inspection
- ▶ Ability to provide evidence of compliance
 - Provide reports based on the controls we monitor
 - Provide compound reports to show security metrics
 - Automate the creation of report

Selected Controls

- ▶ Our strategy is to have as many controls possible being monitored through Splunk
 - Easy to monitor
 - Automate the creation of inspection reports
- ▶ Example of easy ones:
 - Account Management: AC-2
 - Incident Monitoring: IR-5
 - Continuous Monitoring: CA-7
- ▶ Examples of interesting ones:
 - Information System Backup: CP-9
 - Information System Component Inventory: CM-8
 - System and Information Integrity Policy and Procedures: SI-1

Splunk ES and NIST 800-37

► Risk management framework NIST 800-37

- Monitoring the controls that were selected from NIST 800-53 as determined by NIST 199
- Able to automate the report creation for inspections

► Real Time Threat Intelligence

- Investigating as they pop up
- Trackability and resolution
- Resolve inside of ES

► Incident Response

- Tracking and resolving issues from the same interface
- Ability to document the investigations
- Able to prioritize the issues

Living with NIST ATO System

- ▶ Mitigate the risk

- Following the controls helps us protect our system
- ES gives us visibility into the system in real time
- Threat intelligence helps us look at external threats

- ▶ Able to manage with a small team

- Inspections every 6 months
- Ability to focused on problem areas
- Helps us with regular IT issues

► Getting better as we learn

- VPN Access, tracked location
 - We extended to alert on non US activity and multiple sessions
 - Get performance data to help operations

Going Forward

- ▶ Ability to manage risk in real time
- ▶ The standard is changing and we need to adapt quickly
- ▶ Threats are also changing
- ▶ We see that we can leverage User Behavior Analytics to further distinguish false positives
- ▶ Goal is automate more of the inspection reports
- ▶ Add more controls that can be covered by Splunk
 - Will help with inspection artifacts
 - Simplify inspection

► Leverage ES

- ## ► Monitoring

- Validate compliance

- 

Thank You

Don't forget to **rate this session** in the
.conf2017 mobile app

splunk> .conf2017