Splunk Inc., Information Technology Solutions (ITS) PMO

Project Management, Project Communications, and Process Improvement

I was embedded in Splunk's ITS PMO and drove project communications for the Endpoint Security Protection (ESP) program, distilling complex, technical information into crisp, clear language with as little jargon as possible in support of the program director and five project managers across 10 workstreams. Our internal clients were technology and engineering teams, the ITS leadership team, and the Splunk Global Security (SGS) leadership team. (Endpoints—desktops, laptops, smartphones, tablets, servers, and workstations—are key points of vulnerability and provide attack paths into corporate networks by cybercriminals.)

I came aboard the ESP program two months in and served seven months, to the end of the program. I created and led a hands-on communications framework to strengthen Splunk's ESP transformation journey:

My primary task was to nurture productive, collaborative relationships with technology and engineering teams, which called attention to serious inefficiencies in the content creation and distribution process. To address the issue, I introduced a light-touch, repeatable process that increased predictability, consistency, and accountability, creating fewer pauses and roadblocks that were slowing content distribution timelines. That light-touch process was built on the commitment of my technology and engineering colleagues to meet in biweekly Slack forums to discuss project roadmaps to gain a solid footing and common understanding among ITS and SGS leaders and SMEs regarding communications support, which was especially important because most projects required a series of communications.

The most interesting example thereof was the initiative for bringing Linux endpoints into compliance, a critical element of the ESP program, as mandated by SpAARC, Splunk's audit committee. The Linux initiative was kicked off on June 10 and completed on August 18, the day HIP (Host Identity Protocol) checks were enforced, which meant that users who delayed in acting were locked out of the network. To get the cooperation of our Linux community, which was a tough task, we employed a simultaneously white-glove and threatening approach because Linux users are the Splunk's application developers and therefore Splunk's moneymakers, a great many of whom had been around since the company's inception and are used to working in what had been dubbed "a wild west environment."

Managing Linux Endpoints

Communications Plan and Calendar

June 10

Medium: Slack

Audience: Between five and 10 Linux power users

Poster: Tanya

Objectives:

- Give power users a heads up of the June 11 communication
- Explain the specifics of the go-forward plan

June 14

Medium: Slack

Audience: Fewer than 200 Linux users

Poster: Tanya

Objectives:

- Initial notification of set-in-stone Linux endpoint management criteria
- Five-actions are required for compliance

Support contact: Tanya

June 14

Medium: Slack (V#it-linux-champions)

Audience: Fewer than 200 Linux users

Leaders: Tanya, Jose, Ashley, Simran

Objectives:

- Address concerns to the satisfaction of Linux questioners
- Short circuit any pushback or resistance
- Increase employee engagement and improve internal communications
- Reminder of their deadline for compliance

July 1

Medium: Broadcast email

Audience: Linux user population, minus Edge Puck IoT team members

Sender: Alex

Objectives:

- Attachment: Detailed instructions for bringing Linux device into compliance
- Reminder that their deadline is mid-August

Support: GSD

Note: The Puck team was carved out of this communication as work on a new, custom Linux gateway solution continues.

System Compliance Checks **Enabled**

July 15

Medium: Targeted email

Audience: Non-IoT Linux user population

Sender: Jose

Objectives:

- Notification that system compliance checks have been enabled
- Noncompliant devices will receive notification with a link to an FAQ

Support: GSD

Same Day, July 15

Media: Targeted emails

Audiences:

- Edge Puck IoT team members
- Technology Enablement/Education team

Senders: Mohit/Praveen

Objectives:

- Notification that system compliance checks have been enabled
- Announcement of a new Linux OpenVPN gateway solution, which includes additional restrictions designed expressly for the Edge Puck team, based on different criteria, including such things as source group, destination, etc.

Support: Mohit/Praveen

July 28

Medium: Targeted email

Audience: Fewer than 200 Linux users

Sender: Jose

Objectives:

- Reminder that system compliance checks are in place
- Reminder that the deadline for compliance is only two weeks away

Support: GSD

System Compliance Checks **Enforced**

August 18

Medium: Targeted email

Audience: Fewer than 200 Linux users

Sendeer: Jose

Objectives:

- Notification that system compliance checks will now be enforced for noncompliant Linux endpoints
- Notification that noncompliant endpoints lose access to applications behind VPN

Support: GSD

Your Devices

From the Desk of
Alexander Fridman, CIO

Linux community colleagues,

A few months ago, we launched an enterprise-wide initiative called ESP (Endpoint security program) and in support of that your action is required.

Splunk-owned Linux devices are not managed and compliant until the following five compliance actions have been taken:

1. Ensure you are running Ubuntu 20.04 LTS, kernel <= 5.8
2. Enable full-disk encryption via LUKS
3. Install Puppet Agent and register
4. Install GlobalProtect VPN
5. Install CrowdStrike and register

Here are the dates you need to be aware of:

- **On July 15**, the following actions will take place:

  ➔ The Linux legacy VPN gateway will be deprecated, and you will therefore no longer be able to access internal apps behind GlobalProtect VPN (e.g., Jira, Confluence). **From now on, you will be required to connect via our new portal, not the gateway. Here is how to reach the new portal:**

  After installing GlobalProtect, enter the following command into the Linux command line:

  ```
  globalprotect connect -p gp-linux.splunk.com -u <Okta username>
  ```

  ➔ System compliance checks will be **enabled**, which triggers a notification if your device is not compliant, as described immediately below.

- **From July 15 through August 17**, please use the GlobalProtect app to run “globalprotect show --notification,” **which will pop up a browser window and a CLI message** that informs you of the system compliance checks that failed on your workstation. The notification will also include a link to an FAQ that lays out the corrective actions you need to take to bring your Linux device into compliance. Please take these corrective actions before reaching out to GSD.

- **August 18** is your deadline for action. HIP checks will now be **enforced**, which means that the **five compliance actions** called out earlier must have been taken or you will lose access to apps behind VPN.

Please refer to our Splunk Linux Deployment instructions that detail how to perform the five actions required to bring your Linux endpoint into compliance.

Please do not hesitate to reach out to GSD for help if you are still having issues after trying the options provided.

Thank you, and best regards,

Alex Fridman

High-Risk Travel Policy: Overview

The HRC policy states requirements for travel to High-Risk Countries to manage and reduce cybersecurity risks.

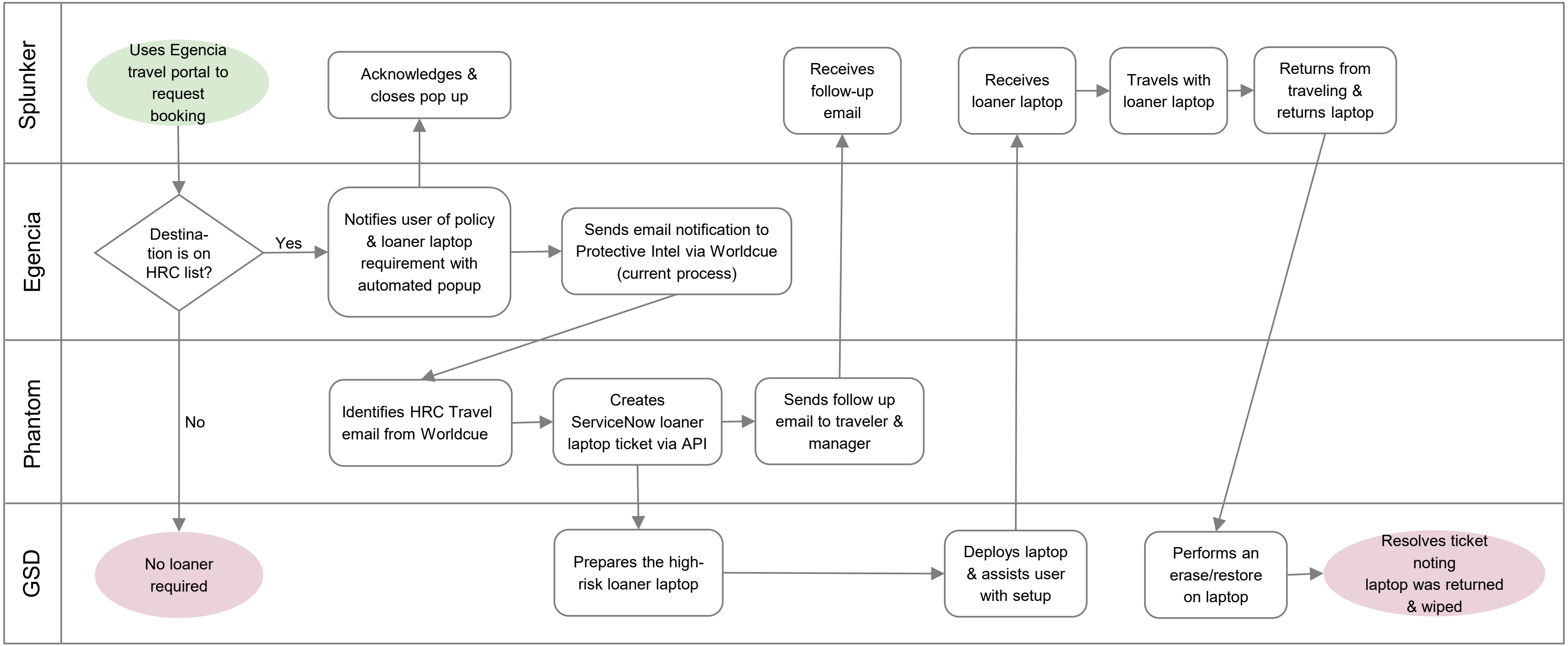
- When traveling to a country defined as high risk, Splunkers must obtain a loaner laptop from Splunk IT and use that laptop in lieu of their standard Splunk-issued laptops.
- Policy also restricts traveling with or accessing source code when traveling to any country designated as a Technology Export Restricted Country (TERC).
- Personal devices, with Advanced MDM installed prior to Splunker travel, will be addressed in a future phase.

The process below explains how a Splunker traveling to a high-risk country would request, receive, and return an IT-provisioned loaner laptop.

1. Splunker books travel using Egencia as usual
2. If destination is in a high risk country, Egencia will:
   a. Pop up a notice regarding the policy
   b. Include a link to the SNOW form for requesting loaner laptop
3. User completes loaner request form
4. GSD prepares and deploys the loaner and supports the user with setup
5. Splunker travels with loaner, leaving standard Splunk-issued laptop at home
6. Splunker returns loaner after returning from the trip

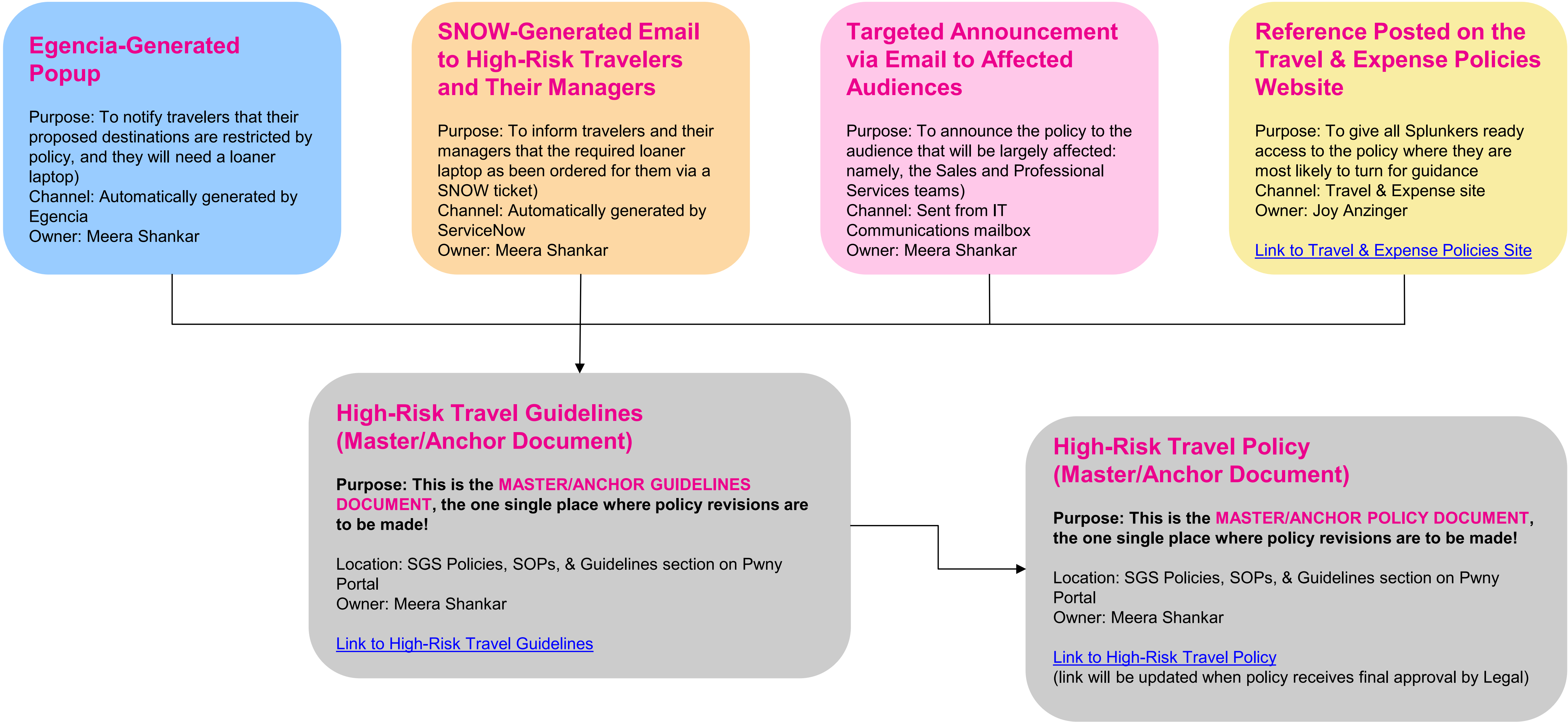
High-Risk Travel Policy: Loaner Process

The process below illustrates how a Splunker traveling to a high-risk country would request, receive, and return an IT-provisioned loaner laptop.


Splunker
Egencia
Phantom
GSD
Uses Egencia travel portal to request booking
Destination is on HRC list?
Yes
No
No loaner required
Notifies user of policy & loaner laptop requirement with automated popup
Acknowledges & closes pop up
Sends email notification to Protective Intel via Worldcue (current process)
Identifies HRC Travel email from Worldcue
Creates ServiceNow loaner laptop ticket via API
Sends follow up email to traveler & manager
Receives follow-up email
Prepares the high-risk loaner laptop
Deploys laptop & assists user with setup
Receives loaner laptop
Travels with loaner laptop
Returns from traveling & returns laptop
Performs an erase/restore on laptop
Resolves ticket noting laptop was returned & wiped

High-Risk Travel Policy: Project Closure

Launch and Assistance Channels



Egencia-Generated Popup

Purpose: To notify travelers that their proposed destinations are restricted by policy, and they will need a loaner laptop)
Channel: Automatically generated by Egencia
Owner: Meera Shankar

SNOW-Generated Email to High-Risk Travelers and Their Managers

Purpose: To inform travelers and their managers that the required loaner laptop as been ordered for them via a SNOW ticket)
Channel: Automatically generated by ServiceNow
Owner: Meera Shankar

Targeted Announcement via Email to Affected Audiences

Purpose: To announce the policy to the audience that will be largely affected: namely, the Sales and Professional Services teams)
Channel: Sent from IT Communications mailbox
Owner: Meera Shankar

Reference Posted on the Travel & Expense Policies Website

Purpose: To give all Splunkers ready access to the policy where they are most likely to turn for guidance
Channel: Travel & Expense site
Owner: Joy Anzinger

Link to Travel & Expense Policies Site

High-Risk Travel Guidelines (Master/Anchor Document)

Purpose: This is the MASTER/ANCHOR GUIDELINES DOCUMENT, the one single place where policy revisions are to be made!

Location: SGS Policies, SOPs, & Guidelines section on Pwny Portal
Owner: Meera Shankar

Link to High-Risk Travel Guidelines

High-Risk Travel Policy (Master/Anchor Document)

Purpose: This is the MASTER/ANCHOR POLICY DOCUMENT, the one single place where policy revisions are to be made!

Location: SGS Policies, SOPs, & Guidelines section on Pwny Portal
Owner: Meera Shankar

Link to High-Risk Travel Policy
(link will be updated when policy receives final approval by Legal)

Your Devices

From the Desk of
Yassir Abousselham, CISO

Guidance for High-Risk Travel

Travel involves many inherent risks. For the safety and security of our employees, we ask you to plan your trips accordingly and to exercise commonsense caution when on the road.

Travel to high-risk regions is more complex than general travel due to the possible threats posed to Splunk's network infrastructure and therefore requires an even more heightened level of preparation and vigilance.

Splunk defines "high-risk countries" (HRCs) based on guidelines from the United States Department of Homeland Security and the United States Department of State.

Whenever You Travel, Wherever You Travel, Travel with Safety in Mind

While this guide calls out specifics related to high-risk travel, all travel (domestic and international) requires caution. Staying safe requires that you exercise common sense and situational awareness.

We have broken this guide into three sections to call out recommendations and reminders for safe and productive travel:

Section 1: What You Need to Know about Travel to High-Risk Regions

Section 2: Exercising Heightened Awareness Wherever You Travel

Section 3: Frequently Asked Questions

Section 1: What You Need to Know about Travel to High-Risk Regions

EXERCISE CAUTION WHEN TRAVELING TO HIGH-RISK REGIONS

- Employees who travel to countries listed in the High-Risk Travel Policy must adhere to the directives found within the policy. Therefore, travel to high-risk countries requires special consideration and preparation. The aforementioned policy also includes a list of those regions identified as high risk.

- Splunk will issue loaner laptops to employees to perform duties while in high-risk areas. Those devices will have enhanced or additional security measures, as outlined in the policy.

- To provide our travelers with trouble-free support, we require travelers to use our centralized online booking system, **Egencia** or their local **Egencia partner**. Using Egencia ensures access to all of Splunk's travel-related services.

- If you want to access Splunk systems from your personal phone while traveling to a high-risk region, you must have IT install Advanced Mobile Device Management software on your mobile device. You can submit the request through ServiceNow.

BOOKING YOUR TRIP TO A HIGH-RISK REGION

Because travel to high-risk regions is evaluated more aggressively than regular international travel, we recommend that you book your trip and request your loaner laptop **at least 10 business days** in advance of your travel date to ensure your trip goes smoothly. Here are the specifics you need to know:

1. Travel requests to high-risk regions are automatically flagged by Egencia.

   Note that travel requests to non-high-risk countries pass through the system uninterrupted.

2. The requestor will receive a popup during the booking process with information about the policy and notification that a loaner laptop has been requested for her or him. A follow-up email will be sent to the traveler and his or her manager with the ServiceNow ticket number and support options.

WHAT ADDITIONAL HELP IS AVAILABLE TO ME?

We encourage you to download **WorldCue Mobile**, which is a **multilingual** smartphone app (iOS and Android). Here is what you need to know about WorldCue Mobile:

- **WorldCue Mobile automatically syncs with Egencia**, providing you with multilingual security alerts and immediate access to travel intelligence and assistance.

- With WorldCue Mobile and Egencia, you get 365/24/7 assistance, including:

  - Medical assistance, if needed
  - Evacuation alerts, if necessary
  - Pre-trip briefings, to include health information, political stability, and travel information
  - Alerts and updates on any changes affecting ALL legs of your trip

- Here is how to download the app:

  - Go to the **iOS App Store** to download the app on your Apple smartphone
  - Go to the **Google Play Store** to download the app to your Android smartphone

Section 2: Exercising Heightened Awareness Wherever You Travel

PREPARING FOR YOUR TRIP

- Confirm your ServiceNow (SNOW) request for a loaner laptop if you are traveling to a designated high-risk region. (As noted above, Egencia will automatically generate a SNOW ticket and follow up with an email confirmation. Refer to that email for additional instructions and contact the Service Desk if you do not receive the confirmation email.)

- Re-review the Splunk Acceptable Use Policy to re-familiarize yourself with Splunk's cybersecurity expectations.

THINGS TO REMEMBER WHILE TRAVELING

- Immediately file an incident report with the **Global Security Coordination Center (Slack #GSCC) or call +1-571-421-6783** if your laptop has been lost, stolen, confiscated, or compromised. Other reportable security incidents include malware, keylogging, ransomware, compromised user account, or denial of service.

- Here are additional recommendations for safer, more secure travel:

  - ★ Be mindful of public Wi-Fi hotspots and connect only when necessary. **Mac users** can set Wi-Fi to "do not automatically connect" by clicking the Wi-Fi icon in the upper righthand corner and clicking the slider. **Windows users** can turn off automatic connections by selecting the Start Menu, then following this navigation: Settings / Network & Internet Settings / Wi-Fi.

  - ★ Do not update software on your computer while connected to a public or hotel wireless network, even if prompted to update.

  - ★ Be mindful of your device and screen at all times, especially in public areas and when logging in or inputting data into your devices. Use the provided privacy screen when on your laptop, and never leave your laptop or mobile device unattended.

  - ★ For passwords, do not use the "remember me" feature; instead, manually retype your password when prompted.

  - ★ Do not post about your travel plans to social media before or during your travel, and do not post from a country designated as a high cybersecurity risk.

  - ★ Avoid transporting devices in checked baggage.

  - ★ Do not open unsolicited emails or attachments, and do not click on links before verifying the source is legitimate. If you have questions about verifying emails, refer to the Phishing Attacks - Security Advisory. When in doubt, please forward the email in its entirety to phishing-pond@splunk.com.

  - ★ Shut down the laptop when it is not in use.

WHEN YOU RETURN

- Immediately change any passwords you may have used during your travels to prevent future attacks on your account.

- Do not use the laptop you traveled with to reconnect to the Splunk network. Ensure that the laptop is wiped and reimaged by the Global Service Desk with trusted software versions.

Section 3: Frequently Asked Questions (FAQs)

What countries are covered under our High-Risk Travel Policy?

Splunk defines “high-risk countries” (HRCs) based on guidelines from the U.S. Department of Homeland Security and the U.S. Department of State, and we will update our list accordingly. To see the most current list of high-risk countries and regions, as identified by Splunk, please go to the **High-Risk Travel Policy**, which will always be kept up to date.

What happens if my manager has an issue with possibly limited productivity while I am away?

Although loaner laptops will be restricted, they will still provide access to standard corporate applications and systems. However, some features will be disabled, such as remote login (SSH), remote management, and the ability to install additional applications. Contact the Service Desk at #help-servicedesk for a complete list of restrictions. Please discuss this issue with your manager well in advance of your travel plans to determine if your productivity will be impacted and how you can mitigate any impact to your work.

What if I forget to add advanced mobile device management (MDM) to my mobile device before I leave?

Please contact the Service Desk at #help-servicedesk ASAP to be added to the advanced MDM group.

What happens if I accidentally bring my work laptop instead of or in addition to the loaner?

Please contact the Service Desk at #help-servicedesk immediately, and they will advise you on next steps, depending on your specific situation.

What do I do if my device is breached, confiscated, or if there is unauthorized access to the network?

In the event of a security incident, immediately file a report with the **Global Security Coordination Center (Slack #GSCC) or call 1-571-421-6783.** Reportable security incidents include lost, confiscated, or stolen laptops, malware, keylogging, ransomware, compromised user accounts, or denial of service.

Will loaner phones or tablets be available for travelers to high-risk regions?

At this time, Splunk will not be issuing loaner phones or tablets.

Document Title	Guidance for High-Risk Travel	
Document Owner	Yassir Abousselham, CISO	
Policy Stakeholders	Splunk IT Data Protection – Legal Splunk Travel Splunk Physical Security	
Launch Date	03/22/2021	
Document Objective	Develop easily digestible, easy-to-understand guidelines for overseas travel overall and high-risk travel in particular, the latter of which will include security guidelines, including the loaner laptop requirement	
Audience	Splunkers who book their travel through Egencia	
Delivery Methods	1. For Splunkers seeking guidance before booking travel: Document will be hosted on SGS's Google Drive folder and posted to the SGS landing page on Pwny Portal. 2. For Splunkers requesting travel to high-risk regions on Egencia: An automated popup from Egencia will direct the Spunker through the process for travel to high-risk regions, including the loaner laptop requirement	
Document Approval Process	Creation	Peter Speliopoulos Consultant, IT PMO, Endpoint Security Protection (ESP)
	Review	Joy Anzinger Director, Corporate Travel & Expense
	Review	Tanya Pfeffer Senior Manager, Client Platform Engineering, Splunk IT
	Review	Tony Iacobelli Senior Security Incident Handler, SGS
	Review	Meera Shankar Senior Risk Analyst, SGS
	Approval	Yassir Abousselham, CISO

Message for Slack (Must Be Splunkified for the Pwny Portal

Hello, Splunk people manager! Did you know that Splunk IT has deployed more than 1,000 laptops to our new starters over the last two quarters? Although growth is exciting, managing the employee lifecycle can sometimes pose challenges. As part of a recent effort to ensure that we are quickly shipping systems to users, it is equally important that we receive those devices when employees separate. As part of your offboarding conversations, **we ask that you remind exiting employees of their responsibility for returning their Splunk-owned assets**. Please take a minute to review this Manager's FAQ, which shares recent advancements made to streamline the asset reclaims process.

Manager's FAQ

Manager's FAQ: Recovering Laptops from Employees Who Leave Splunk

Employee turnover is a fact of life, and asset retrieval is the responsibility of every Splunk manager. It is therefore important for you to be ready for this eventuality.

Here is what you need to know to ensure that separating employees (Splunk alumni) return their Splunk-issued laptops:

What does the employee separation process look like?

Employee separation is a five-step process:

1. The process begins with the employee's decision to separate or the manager's decision to terminate.
2. Next, the employee's profile is updated, as follows:
   a. For fulltime, permanent employees (FTEs), the Splunk People Operations Team (SPOT/HR) will process the termination in Workday.
   b. For alternative workforce resources (e.g., contractors), managers are responsible for processing the offboarding in the Wand/AWF portal.
3. An offboarding ticket is created in ServiceNow, alerting the Service Desk to:
   a. Revoke systems access to account(s)
   b. Track the return of Splunk equipment
4. The separating employee is sent instructions or packaging for prepaid shipping with FedEx (or a local shipping vendor, depending on the Splunk alumni's region).
5. Finally, the Service Desk will track the return of the package, from dropoff at FedEx to delivery at Splunk.

What specifically is expected of managers?

The requirements are limited:

1. **Voluntary separations (i.e., the employee gives notice or resigns):** Managers are expected to initiate a separation request in Workday (or work with SPOT/HRBP to do so) when an employee submits his or her resignation.
2. **Involuntary separations (i.e., termination for cause, performance, etc.):** SPOT or your HR business partner will initiate the termination process in Workday for all involuntary terminations.
3. Next, we ask that managers communicate directly with the departing employee, clearly laying out the expectation that Splunk-owned equipment must be **returned within seven days** of the employee's last day of work.
4. SPOT/HR, the Service Desk, and Global Security coordinate the details of equipment return and will send an email to separating employees with specific instructions or packaging for prepaid shipping with FedEx.

How long does a separating employee have to return his or her laptop?

Splunk equipment is expected to be dropped off at a FedEx location for return delivery within **seven (7) days** of the employee's last day worked.

We request that our managers lay the groundwork for separating employees with strong, but sympathetic, guidance by asking departing employees to start preparing for the return of their Splunk laptops during the week leading up to their last day of work. This includes reminding departing employees to:

1. Download their personal data to an external drive
2. Transfer ownership of their work files and drives to their direct manager and teammates

What should managers do if a departing employee reports that the shipping material has not been received?

In situations where the separating employee has not received her or his Splunk hardware instructions or packaging, we ask that managers reach out to the Splunk Service Desk for assistance in completing the asset reclamation. When a manager reaches out to the Service Desk, the situation will be investigated, and the Service Desk will follow up with the separated employee. No further action is required of the manager.

What if I need additional help in recovering Splunk-owned assets or if I have questions about the asset reclamation process?

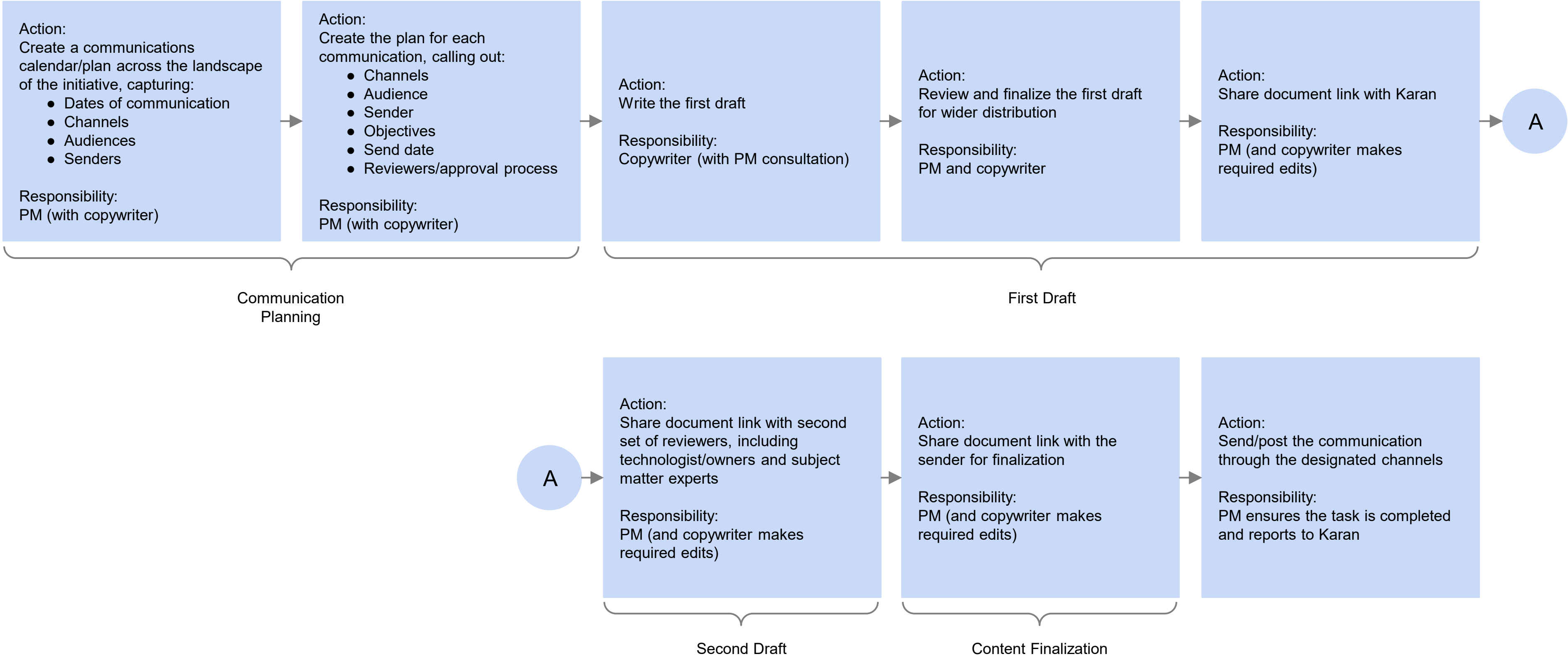
If you run into roadblocks, have questions, or want to know the status of an asset reclamation, please select one of the following resources:

1. Inquire in the Slack channel #help-service desk
2. Call 1-877-371-8267 for 24/7 support
3. Email help@splunk.com and a ServiceNow ticket will automatically be created for you

Thank you for supporting the asset reclamation process!

Document Title	Recovering Laptops from Employees Who Leave Splunk	
Document Owner	Ashley Sprague, Senior Director, IT Operations	
Policy Stakeholders	IT Operations Legal	
Launch Date	04/08/2021	
Document Objectives	1. Remind managers of their responsibility to notify separating employees of the need to return their laptops 2. Notify managers that the separation process is now fully articulated and addresses the lack of information that has been available to managers 3. Provide managers with overview of the separation process, including communications that will be sent by SPOT	
Audience	Splunk people managers	
Delivery Methods	1. Managing@Splunk on the Pwny Portal 2. #people-managers on Slack	
Document Approval Process	Creation	Peter Speliopoulos Consultant, IT PMO, ESP
	Review	Earlvin Rivera, IT Business Systems Analyst, Corporate Finance
	Review	Jeff Johnson, Project Manager, IT PMO, ESP
	Review	Karan Bajaj, Director, IT PMO, ESP
	Review	Agim Kraja, Senior Manager, Global IT Services and Support
	Approval	Ashley Sprague, Senior Director, IT Operations

Content Creation and Approval Process



Action:
Create a communications calendar/plan across the landscape of the initiative, capturing:

- Dates of communication
- Channels
- Audiences
- Senders

Responsibility:
PM (with copywriter)

Action:
Create the plan for each communication, calling out:

- Channels
- Audience
- Sender
- Objectives
- Send date
- Reviewers/approval process

Responsibility:
PM (with copywriter)

Communication Planning

Action:
Write the first draft

Responsibility:
Copywriter (with PM consultation)

Action:
Review and finalize the first draft for wider distribution

Responsibility:
PM and copywriter

Action:
Share document link with Karan

Responsibility:
PM (and copywriter makes required edits)

First Draft

Action:
Share document link with second set of reviewers, including technologist/owners and subject matter experts

Responsibility:
PM (and copywriter makes required edits)

Second Draft

Action:
Share document link with the sender for finalization

Responsibility:
PM (and copywriter makes required edits)

Action:
Send/post the communication through the designated channels

Responsibility:
PM ensures the task is completed and reports to Karan

Content Finalization

splunk> turn data into doing

ESP Weekly Digest

Deliverables Over the Week of March 1, 2021

Overall Program Health 🟩

Network & Device Access

Accomplishments

- NEST and CPE team has built the networks and VDI to support U.S. East and Singapore regions. User testing began March 1 and is on track to complete on March 5.
- Systems Compliance (HIP) Checks are in place and activated. The informational email message was sent on February 22, and the pop-up message for users failing the check started on February 26.
- GSD has started the white glove outreach to the 619 individual users who were identified as failing HIP checks and needing remediation.
- Okta device trust for Windows has completed functional and browser testing and is in the process of high-availability testing.

Risks

No risks

Health 🟩 **Complete** 85%

Vulnerability Management

Accomplishments

- Patch Management: Phase 1 - Setup Systems Manager (SSM) complete, except for the final communication.
- Linux Endpoints: CPE working with IT PMO/CMO to create a plan to communicate updated policies to ensure systems are managed by March 12.
- Designed and implemented a process to resolve the identified open vulnerabilities.
- The Threat and Vulnerability Management Program Service Level Agreement Standard has been built out as of February 22 and was communicated to IT and SGS on March 3.

Risks

No risks

Health 🟩 **Complete** 40%

IT Asset Lifecycle Management

Accomplishments

- GSD implemented the new asset reclaim process for unrecovered laptops.
- GSD implemented biweekly (every two weeks) computer inventory asset scans of computers located in the office, updating computer records in ServiceNow for all records scanned.

Risks

No risks

Health 🟩 **Complete** 70%

Security Configuration Management

Accomplishments

- Password Policies on Macs: The change has been approved and just needs to be executed against. The CPE team will complete this by March 5.
- JAMF Connect: Certification configuration is in place but is not being distributed yet. CPE is working with NEST, targeting March 10 to test.
- CIS benchmarks for the CPE team have been created, as well as the implementation. The last step to close this out is to create the evidence documentation for SpAARC.

Risks

No risks

Health 🟩 **Complete** 60%

Other Observations

Accomplishments

The standards document to support the high-risk country travel policy has been completed.

Risks

This project is yellow to highlight the change in completion date from 3/31 to 5/31 to implement the loaner laptop program for high-risk travel:

- Before implementation, the policy will be updated to remove the regional exclusions and to add new capabilities, such as support for mobile devices and the use of Chromebooks for the loaners.
- Per the updated plan, the team will (1) revise the policy in March, (2) socialize the changes and prepare processes and communications in April, and (3) roll out the loaner laptops in May 2021.

Health 🟨 **Complete** 40%

Unenforced Multifactor Authentication (MFA)

Accomplishments

- Reached out to owners of all high-risk service accounts via Slack and sent an official email through IT Communications.
- The team has created a tracking sheet for capturing owner information, login details, etc. for all of the service accounts in our environment.
- Process Document: Documented the initial process flow for service account remediation.
- Azure/Office 365 is now federated with Okta, as of February 12.

Risks

No risks

Health 🟩 **Complete** 75%

Credential & Authorization Management

Accomplishments

- Completed review, revoke, and rotation of all compromised credentials in JIRA tickets and Confluence pages.
- Completed the implementation of the credential scanning program to detect future secrets in plain text violations on collaboration tools.
- Completed the creation and communicate of a credential management standard.

Risks

This project was yellow because due dates needed to be reassessed. Since then, the team has performed the following tasks and is now green: (1) decided to merge discovery efforts for both projects, as they tie to the same server farm, (2) estimated the scope and end dates, and (3) socialized with SpAARC, IT, and SGS.

Health 🟩 **Complete** 60%

Network Segmentation

Accomplishments

- The team received track logs and started analysis on the traffic flow to identify what traffic is accessing the overly permissive firewall rules.
- The team will use the analysis from the logs to determine more granular firewall rules to implement the new rules above the overly permissive rules.
- On track to begin pushing the new granular rules on March 9.

Risks

No risks

Health 🟩 **Complete** 80%

ESP Status Summary

Program & Management Action Plan (MAP) Status Summary: Presented to SpAARC

ESP Program Status 🟢

The overall ESP program status remains green. Out of the 10 ESP projects, 1 project (Network Segmentation) was completed by the end of April. All of the other projects are on track.

The project team is working with SAARC to invite Bishop Fox for next round of audit by end of June. By then, a total of 5 out of the 10 projects would be completed.

Recent Accomplishments & Highlights

1. Developed and published the Threat and Vulnerability Management Procedure, the SOP, and the service level agreement
2. Remediated of of the 27 high-risk service accounts
3. Disabled the use of SSH for remote administrative access by default on Macs
4. Removed overly permissive firewall rules
5. Patching completed for all in scope AWS Non-Prod instances
6. Completed the Software install & automation setup for Linux CVDI solution

Upcoming

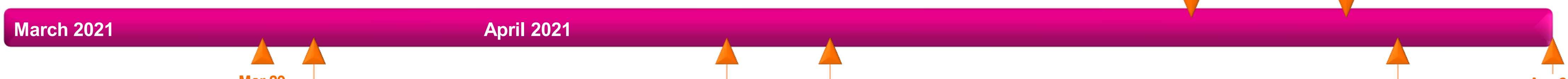
1. Patching of AWS Prod Instances scheduled for 05/18
2. Publish High Risk Travel Policy
3. Complete planning for next phase of account remediations (“IT-Linked”)

Management Action Plan Roll Up

The summary table below represents overall MAP status. ***Please note!*** MAPs vary significantly in implementation and level of effort. MAP’s may have dependencies on others, may overlap scope with others, or be updated as teams deem necessary. Updates and changes will be communicated.

Project Swimlanes	Total Project Deliverables	Percent Completed
Acceptable Use Applications (MAP 5)	5	0%
Vulnerability Management (MAP 2)	8	38%
Credential & Authorization Management (MAP 9)	16	81%
Unenforced Multifactor Authentication (MAP 8)	9	56%
Network & Device Access (MAP 1)	13	85%
Other Observations (MAP 7)	6	33%
IT Asset Lifecycle Management (MAP 3)	8	50%
Security Configuration Management (MAP 4)	7	71%
Network Segmentation (MAP 10)	3	100%

Project Communications Calendar (March and April 2021)



Mar 29
PM: Lynette Shelton
Project: Network & Device Access
Audience: All Windows users
Purpose: Communication to Windows users to determine if their PCs are Splunk-issued; if not, they will be required to authenticate through Okta every time they choose to use a Splunk application
Deliverable: Email through IT Communications mailbox

Mar 30
PM: Srikanth Polapragada
Project: Credential & Authentication Management
Audience: 201 service account owners
Purpose: Lock inactive service accounts (i.e., those not accessed in the past 90 days)
Deliverable: Email

Mar 30
PM: Srikanth Polapragada
Project: Credential & Authentication Management
Audience: Targeted distribution lists
Purpose: Identify owners for "Active" service accounts in Phase 2
Deliverable: Google Forms survey

Apr 7
PM: Joel Braddock
Project: Vulnerability Management
Audience: Server, service owners
Purpose: Confirm AWS account owners
Deliverable: Email, Slack, with guidance from IT leadership

Apr 9
PM: Joel Braddock
Project: Vulnerability Management
Audience: ~200 Linux users
Purpose: Announce the newly agreed-upon two-phase approach to managing vulnerability on Linux endpoints, including a timeline specifying actions required of Linux users
Deliverable: Email, other avenues TBD

Apr 9
PM: Jeff Johnson
Project: IT Asset Lifecycle Management
Audience: Splunk managers
Purpose: Inform managers of updated processes for securing Splunk-owned laptops from separating employees
Deliverable: FAQ posted to Confluence, Slack

Apr 16
PM: Joel Braddock
Project: Security Configuration Management
Audience: Mac users
Purpose: Announce enhanced application patching for Macs via JAMF
Deliverable: Pwny Portal

Apr 19
PM: Srikanth Polapragada
Project: Credential & Authentication Management
Audience: 148 service account owners
Purpose: Lock stale service accounts (i.e., those created in the past 90 days, but never logged in)
Deliverable: Email

Apr 20
PM: Srikanth Polapragada
Project: Multi-Factor Authentication
Audience: ~15 application owners
Purpose: Work with app owners to initiate migration of SAML/SWA-capable applications
Deliverable: Email, Slack

Apr 20
PM: Jeff Johnson
Project: Other Observations
Audience: Splunkers who book travel through Egencia
Purpose: Security guidelines for travel to high-risk regions, including the loaner laptop requirement
Deliverable: Targeted email, Pwny Portal

Apr 23
PM: Srikanth Polapragada
Project: Credential & Authentication Management
Audience: 142 service account owners, managers
Purpose: Actions and deadline for remediation of active service accounts
Deliverable: Email

Monthly Retrospective

Key Learnings: March 2021 (page 1 of 4)

Key Learnings

Learning 1 (AE, N&DA)

During the HIP banner change, we had to roll back the change because the date was postponed. This happened after CAB approval and the CHG went through. Rollback occurred two hours after the change. Stakeholder representation during CAB to an IC (individual contributor) needs to be cascaded downward and not through a single channel (like a manager). Have redundancy in communication to the individual contributors implementing the change.

Learning 2 (PB, N&DA)

Some Linux users (~10) were blocked after the change and we communicated there was another option (using OpenConnect) but looks like not all Linux users are part of the AD group which required adding them later. GSD and NEST quickly unblocked them to get them working again. Also, thanks for CPE team for responding/providing support to the users.

Learning 3 (AE, N&DA)

Would recommend a requirement where a deliverable has a Splunk(ed) data representation (or data points be shared to multiple team members). This allows us the opportunity for stakeholders to review data and question why. For SCC banner, if NEST did not review data in a regular cadence, we would have missed two scenarios: (1) Deloitte/SAP Ariba being able to access the network and (2) users that do not have VDI but are failing HIP. These use cases would not have been brought to other teams' attention and decisions made for them (Deloitte/Ariba was added to the exclude list, users were reached out).

Learning 4 (AE, N&DA)

I commend the escalation procedure of the individual contributors (in GSD, in CPE, and in NEST) when issues occur. During one of the troubleshooting sessions that GSD and CPE reported, we found that there was an unexpected behavior that pertains to HIP banner (occurring at the short delay of processing HIP vs. the connectivity time of VPN). We were quickly able to create a solution that acknowledges that delay time and were able to prevent a small number of people from being misinformed. (issue fixed)

Network & Device Access	🟩	Vulnerability Management	🟩	IT Asset Lifecycle Management	🟩
Security Configuration Management	🟩	Other Observations	🟩	Unenforced Multifactor Authentication	🟩
Credential & Authorization Management	🟩	Network Segmentation	🟩		

Monthly Retrospective

Key Learnings: March 2021 (page 2 of 4)

Key Learnings

Learning 5 (AE, N&DA)

During our data analysis, we found that the Windows 10 standard has updated (to version 2009 from 2004). This was unaccounted for in the acceptable OS version (N-1). While this is a non-impacting HIP check (not part of enforcement), this gave a wrong impression that they were failing the OS check (N-1 version) (again, non-impacting). We were not informed that a new build version was out. NEST added a new HIP profile that accounts for version 2009. (issue fixed)

Learning 6 (AE, N&DA)

During HIP enforcement, tickets were wrongly assigned to endpoint security group in ServiceNow to park/track users added to the exception group. This did not follow the process flow chart documented here https://docs.google.com/presentation/d/1sN0KILVbo7FIBKT46dKEEYJJSFcUMt8F7U9wdgTme_c/edit?userstoinvite=mbenabbas@splunk.com&ts=60256adf#slide=id.p1 that any escalations after adding to the exception group should be assigned to the relevant party capable of resolving it (CPE or NEST). There is a work in progress to add a new subcategory in ServiceNow called “HIP exception” for endpoint security to track (and ServiceNow is also in RZ-Splunk). NEST has updated their internal process that when troubleshooting a user that is exempted from VPN to use Subcategory: “HIP exception” (after it is added to ServiceNow) to the ticket.

Learning 7 (Tanya, Network & Device Access)

The limitations of VDI for non-Windows users was not fully appreciated and accounted for in advance of HIP blocking. The success of moving Sykes and Blue Ocean from Citrix to Amazon Workspaces was not a good enough predictor of how successfully that VDI would be in the wider community.

Learning 8 (Tanya, Network & Device Access)

Our initial investigation about Linux compatibility with our toolset fell short of fully grasping the nuances of the kernel variation within Linux flavors and versions. We didn’t anticipate needing to restrict kernels within our chosen supported version and the impact this would have on Linux using Splunkers.

Network & Device Access	🟩	**Vulnerability Management**	🟩	**IT Asset Lifecycle Management**	🟩
Security Configuration Management	🟩	**Other Observations**	🟩	**Unenforced Multifactor Authentication**	🟩
Credential & Authorization Management	🟩	**Network Segmentation**	🟩		

splunk> turn data into doing

Monthly Retrospective

Key Learnings: March 2021 (page 3 of 4)

Key Learnings

Learning 9 (Tanya, Credential & Auth Mgmt)

Initial communication for rolling out LastPass was combined with AD requirement changes, necessitating a truncated communication. This led to critical information being omitted and confusion in the community about appropriate use of the tool.

Learning 10 (Tanya, Credential & Auth Mgmt)

The precarious nature of our MS PKI infrastructure caused a delay in transitioning away from Enterprise Connect in favor of Jamf Connect for local Mac password syncing. We should have prioritized rebuilding our cert workflow at the onset of this project.

Learning 11 (Craig, Network & Device Access)

Technical limitations of GlobalProtect were not fully realized by the project team. This resulted in requirements not being able to be met and workarounds needing to be completed.

Learning 12 (Craig, Network & Device Access)

Gathering data and presenting it in shared Splunk dashboards is something that should be set up in the beginning of each subproject so the definition of “done” can be seen (by % completed).

Learning 13 (Craig, Network & Device Access)

MAPs should have been revalidated (weekly, if necessary) to ensure everyone was on the “same page” on the plan as well as “who had to do what.” Granular review of every project and project plan needed to be completed to ensure we didn’t “deviate.”

Learning 14 (Craig, ESP as a whole)

MAPs are good, but a definition of “done” needs to be completed before start of work. If the definition changes, that is OK, but a central doc for the project needs to be updated so everyone knows what changed.

Network & Device Access	🟩	**Vulnerability Management**	🟩	**IT Asset Lifecycle Management**	🟩
Security Configuration Management	🟩	**Other Observations**	🟩	**Unenforced Multifactor Authentication**	🟩
Credential & Authorization Management	🟩	**Network Segmentation**	🟩		

Monthly Retrospective

Key Learnings: March 2021 (page 4 of 4)

Key Learnings

Learning 15 (Craig)

High-level decisions and discussions need to be documented. With everyone working on multiple projects, not everyone is aware of major changes when they happen. This results in lots of miscommunication.

Learning 16 (Pradeep/CorpIAM, Credential & Auth Mgmt)

Even after working with the service account (SA) owners, after completing a standard password rotation, there were unknown dependencies that resulted in system outages. SA owners need to manage SA account to limit its scope of use or clearly can identify where it is in use to anticipate impacts of password rotation/disablement.

Learning 17 (Pradeep/CorpIAM, Credential & Auth Mgmt)

The ability for service account owners to reset/rotate passwords is suboptimal and requires manual coordination and can be error prone. Need to accelerate Hashi Corp Vault <>AD integration to mitigate this.

Learning 18 (Pradeep/CorpIAM, Credential & Auth Mgmt)

New service account requesters may not know of “modern” alternatives, which then increases/encourages more service accounts. Help educate requesters that there could be other options available and publish a guide/standard.

Learning 19 (Pradeep/CorpIAM, Credential & Auth Mgmt)

Completing discovery of service account (SA) owners and their usage is difficult if not properly documented (SNOW ticket, AD account description, Confluence pages, tribal knowledge, staff turnover). To add another useful datapoint for discovery, the LDAP/AD VIP configuration needs to be updated to easily track source IP addresses.

Learning 20 (Meera, Credential & Auth Mgmt)

Updates to the credentials doc were pretty simple, but the process to align various stakeholders on content took many cycles. Would have been nice to align SpAARC asks with, Splunk capabilities/realities of Splunkers, with senior leadership, ahead of revisions.

Network & Device Access	🟩	**Vulnerability Management**	🟩	**IT Asset Lifecycle Management**	🟩
Security Configuration Management	🟩	**Other Observations**	🟩	**Unenforced Multifactor Authentication**	🟩
Credential & Authorization Management	🟩	**Network Segmentation**	🟩		