The Essential Guide to **Foundational Security Procedures**

splunk>
turn data into doing

For years, security managers have faced a host of challenges — too many alerts, a security talent shortage and disparate security tools. Under-resourced security teams struggle to tackle the overwhelming abundance of security alerts coming in. The foundation for a strong, mature security operations center (SOC), built on standard security procedures that leverage automation and orchestration, has never been more critical.

Try Splunk SOAR for Free

Table of Contents

What Are Standard Operating Procedures?

Standard operating procedures are a set of written, step-by-step instructions that catalog how every employee or team member should perform routine operations. These procedures should be concise, easy-to-read and easy to revise.

Throughout this guide, standard operating procedures in the security industry will be referenced as standard security procedures (SSPs). SSPs are a critical component of any mature and adept security team. They act as a gold standard for experienced security analysts, but also as a training guidebook for new junior analysts joining the team. Let's explore some of the main benefits that security teams reap from having SSPs in place.

Benefits of standard security procedures

Reduce time for response

SSPs provide the security analyst with an established, repeatable set of steps that they can execute quickly and efficiently in response to a security incident. When a particular security incident occurs, the analyst can begin to execute the assigned SSP response actions almost immediately. No time is wasted figuring out how to respond to different types of incidents.

Reduce human error

Security analysts routinely operate under stressful, time-sensitive conditions. Unfortunately, this "pressure cooker" environment can catalyze errors by the analyst, which could spell the difference between a successful resolution and a costly breach. Analysts must respond to security incidents accurately and quickly in order to mitigate potential damage to the organization. With a clear list of procedures to follow, it's easier for the analyst to exercise increased focus, accuracy and speed under stressful conditions.

Measure team performance with predictable SLAs

SSPs help security managers understand and establish baseline performance metrics for their team against specific events with predictable turnaround times. This can help the team establish service level agreements (SLAs) and continually improve against them over time.

Quality control

It is exceedingly important for the SOC to maintain a consistent quality of detection, investigation and response across multiple types of security events. SSPs provide a mechanism to track the increase, decrease or consistency of the quality of those activities. Chief information security officers (CISOs) and SOC managers may need to report performance metrics back to business executives.

Compliance

Well-written procedures can meet certain compliance requirements from government regulations, and can act as a document checklist for auditors.

Historical records

Saving written or electronic records of what, when and how steps are taken during an investigation or remediation process allows anyone to understand what happened even if someone leaves the company. Unwritten "tribal" knowledge at an organization often disappears without proper documentation.

Training guidelines for new team members

It is important to provide accurate and concise documentation for new security analysts joining the team. Introducing SSPs to your new team members will guarantee faster onboarding.

Building the Foundation for Security Operations

Establishing a strong foundation for your security team is not an easy task. Many SOCs have between one and five personnel who are responsible for hundreds or even thousands of alerts coming in every day. In order to maximize efficiency, the team must be fully aligned on common protocols and implement a robust framework to carry them out.

Team alignment

One significant challenge that a SOC manager may face — particularly when taking an honest look at the team of people handling security incidents — is the difference in quality of work between an experienced analyst and a junior analyst. Without properly documented procedures, various SOC team members may execute different steps at different levels of rigor when investigating and remediating alerts. Additionally, various team members may not provide a rationale for why certain alerts are more deeply investigated and others are casually marked as completed. This can have a negative impact on the organization's overall security posture as some alerts may not be correctly or sufficiently investigated.

At the top of most security managers' wish list is a skillful team with mature, repeatable processes for handling incidents of various kinds. These processes will allow experienced analysts to innovate and iterate, while junior analysts can leverage them to grow their skillset. Consistent teams value iterative improvements, creative innovation, and well thought out processes to help bridge knowledge gaps for new or junior team members. By holding everyone to the same standard of expectations, security managers can ensure quality output by their team and provide clear performance metrics to executives as needed.

To aid in achieving team consistency, Splunk SOAR is a robust security orchestration, automation and response (SOAR) solution that provides a feature called "workbooks." This feature defines how a human should act (processes, procedures, output, etc.) when dealing with a case, and can be complemented or even supplanted with automation. Workbooks are essentially standard security operating procedures codified into the Splunk SOAR interface that provide effective streamlined workflows.

In the following section, we will guide you through how to draft SSPs, and translate those SSPs into workbooks in Splunk SOAR.

Drafting your standard security procedures

1. Process identification

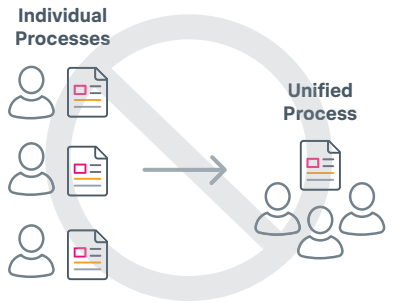
Start by identifying which security processes need to be operationalized and improved. The team should collectively decide which processes they would like to test first. Making a good choice for the team's first SSP to operationalize is crucial. A good result (an SSP that helps the team work faster and more effectively) can precipitate team buy-in around the concepts and benefits of SSPs, and team participation for implementing SSPs into an automation and orchestration tool.

Some guiding principles for choosing a security process to standardize:

1. Limit to processes that are performed today (i.e., already established work), that will produce quality feedback from the team.
2. Look for processes that are done relatively frequently and that are familiar to all members of the team.
3. Limit the options to processes where the penalty for inconsistency can be potentially high.
4. Look for processes where automation could be introduced in the future to reduce the number of manual tasks required by the analysts.
5. Look for processes that may have some compliance or regulatory requirement where consistency represents an audit improvement.

2. Process normalization

Now that you have a candidate process selected, you and your team can begin analyzing it objectively and then normalizing the work each of the team members do into a codified workbook — thus moving from individual processes to a unified process.



But before any normalization can be done, you must first understand how the team operates day-to-day. Here are some first steps to achieve a unified process:

- **Collect information** on how the team operates by interviewing the staff about their existing process against the process you chose. Independently observe how each of your team members handle this type of incident.
- **Synthesize all these individual processes** into notes.
- **Set up a team meeting** to consider the various tasks each member performed to remediate this incident. Understand the rationale behind what every team member did or didn't do, and why they performed them in that particular order and priority.
- **Encourage healthy discussion** and debate to work through everyone's perception on how to approach this security incident.
- **Agree on an optimized set of tasks in the process** that will be followed by everyone in the team going forward. This is the task list which will be used as a skeleton for drafting the workbook documentation, and codifying it into Splunk SOAR.

3. Workbook documentation

Once you have the list of actions that all analysts will perform going forward (discussed in your previous meeting), begin drafting a workbook (on paper).

Steps to drafting a workbook:

- **List the agreed set of actions on paper** from the previous team meeting and distribute it to the team.
- **Team members will review it independently** and note any thoughts.
- **Team members will review it collectively** and agree on a version.
- **Each analyst will use the paper-workbook version as a guide while handling live incidents.** During this time, analysts should have an adequate amount of time to test and ensure no critical piece was missed, to make sure nothing superfluous was added, and that everything can be accomplished within a reasonable amount of time.
- **Call another team meeting** after everyone has had time to review the task list and make notes. At this meeting, the list of tasks should become an ordered list of tasks with appropriate time-saving strategies built in.
- **Finalize the ordered list of tasks** — when codifying this workbook into Splunk SOAR, you will be asked to input the tasks and group them into "phases." Then the paper-workbook is finished!

With the paper-workbook created, the team should spend some time going through previous, real events to ensure that true-positives would have been caught with the new process. Remember that a cadence should be established for continuous improvement.

Finally, once everyone is satisfied with the newly documented procedure, it's time to move to the next step and codify what you have within Splunk SOAR. Please refer to the checklist at the end of the guide to ensure you've accomplished all the steps necessary to successfully create SSPs.

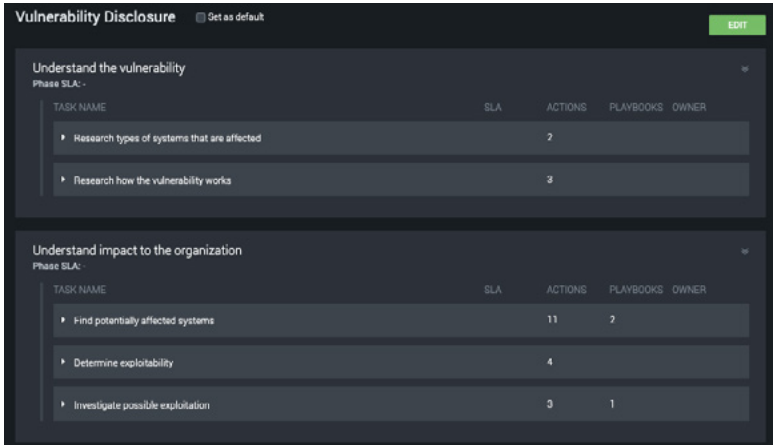
Setting Up Workbooks in Splunk SOAR

The foundation is now set for your team to implement your paper-workbook within Splunk SOAR, with an eye on future automation. Once this is done, you can be certain that all your analysts will apply the same steps each time an incident occurs — resulting in consistency of response, and a more integrated team.

Workbook components

A Splunk SOAR workbook is separated into phases. Each of these phases can have multiple tasks, service level agreements, actions and playbooks associated with it.

Ideally, when you and your team build workbooks, keep in mind phases represent conceptual steps that must be completed whereas tasks represent the concrete actions that must be performed. For example, if you were to create a workbook for a "vulnerability disclosure," it may look something like this:



Setting up a Splunk SOAR workbook

1. Splunk SOAR has built-in workbooks that can be found under **Administration** > **Product Settings** > **Workbooks**. You will also find a button to create new workbooks in this view.

2. Click the + WORKBOOK button where we'll be greeted with the workbook creation screen.

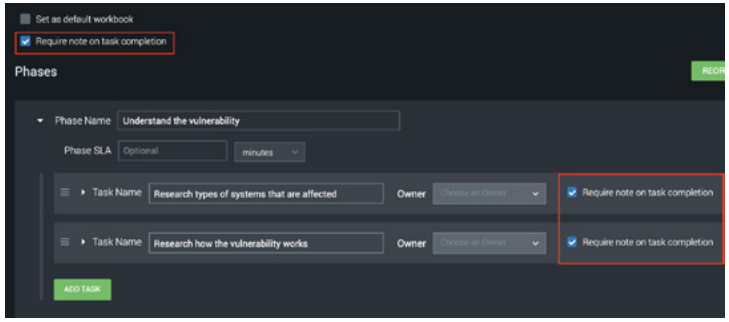
3. Enter the "Workbook Name" and "Workbook Description."

4. When creating or editing a workbook, there are two configurations that require you to make a decision and to click it if it applies.

"Set as default workbook" means that if you promote an event to a case without specifying a different workbook, or you create a new case manually without specifying a workbook, then this is the workbook that will be assigned.

"Require note on task completion" means that each task in each phase will have its own "require note on task completion" checked.

5. Next, you may start inputting what you have on your paper-workbook into phases and tasks in Splunk SOAR. You may also assign different owners to each task as an option. If there is an ordered structure for the analysts (e.g., tier one/tier two or junior/senior) that will be used for deciding who performs each task, then this should be captured in the configuration. As we will see in the next section, Splunk SOAR allows for assignment based on **user or role** and this concept will be important if the team is not flat.



If "require note on task completion" is enabled and if an analyst is working through a task, then they cannot mark the step as completed without putting in some notes. The setting of the same name on the workbook screen (screenshot above), if checked, simply means that every task in every phase will also have that setting checked. This is useful if the team desires a deep retroactive analysis of each event or case.

6. Go through each section and complete inputting your paper-workbook into Splunk SOAR. Once you are finished, save it in the system.

7. Once you have the workbook set up to your satisfaction, you might consider running through some test incidents and having the team do the same. This will give you the time to familiarize yourselves with the Splunk SOAR user interface related to workbooks.

Using Splunk SOAR Workbooks for Incident Events

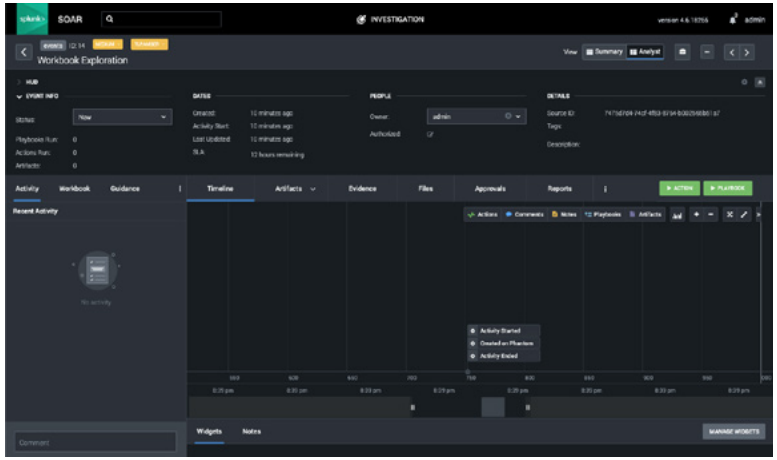
Once you have your workbook completed, you can start integrating it into your workflow when an event occurs.

Create an event

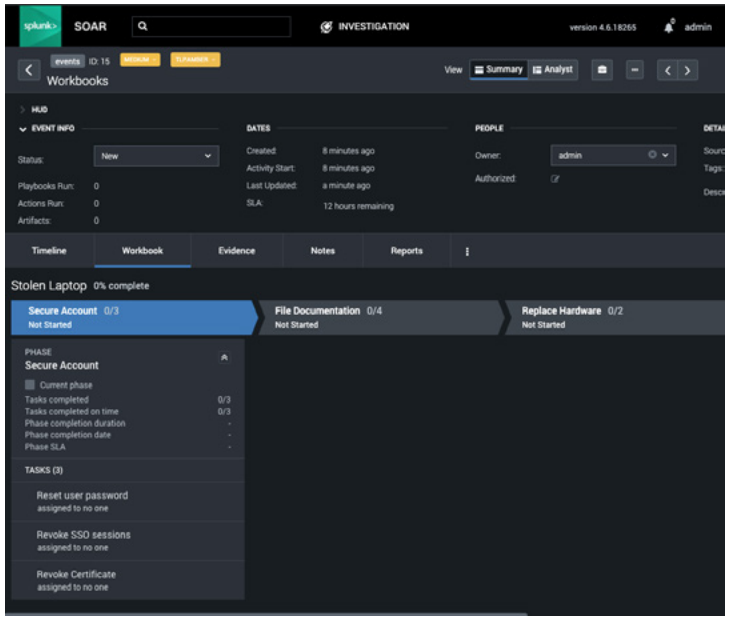
1. Navigate from **Administration** > **Sources**
2. Click + EVENT on the sources page
3. Fill out the “Add Event” window with:
   a. Event Name: Something short and obvious here (e.g., “Mary Smith”)
   b. Label: “Phishing Evaluation” (this label will be important later)
   c. Event Type: “Case” (this will allow you to use your workbook in the event)
   d. ...other values being left with their defaults
4. Click “Save” to create the new event.

Add workbook into event

1. Open the new event you just created.
2. You will see “Activity,” “Workbook” and “Guidance” on the bottom-left corner of the screen. When you click “Workbook” you can “Add Workbook” to activate the workbook that you have created. After that’s done, the workbook tab will include the phases and tasks you’ve defined. Make sure you are in “Analyst View.”



3. Now, you may step through the tasks of each phase, capturing notes and files as necessary. This is the framework that should help achieve consistency with regard to how every member of the team handles each defined incident type.



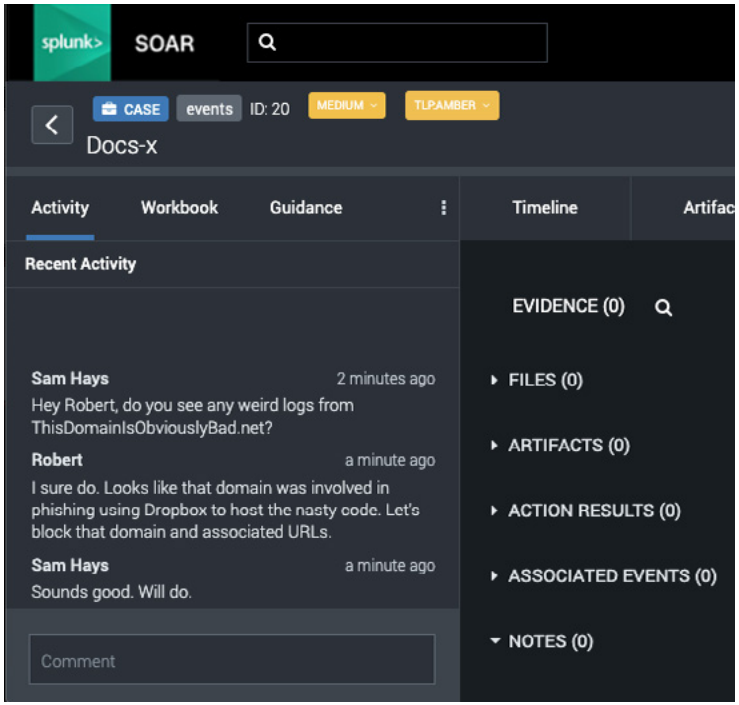
Collaborating with the team on an event

When handling an event, Splunk SOAR allows for direct interaction between team members within that Event. This is done primarily in three ways: activity, notes and evidence.

1. **Activity**

   You can see the "Activity" pane on the left hand side of the screen when viewing an event. Analysts can discuss remediation steps in real time within the Splunk SOAR environment. This alleviates the need to pivot to third-party chat environments during an investigation and contains the context of the incident within Splunk SOAR. This feature can be useful in bringing other team members up to speed on this specific incident when reviewing what was previously discussed.

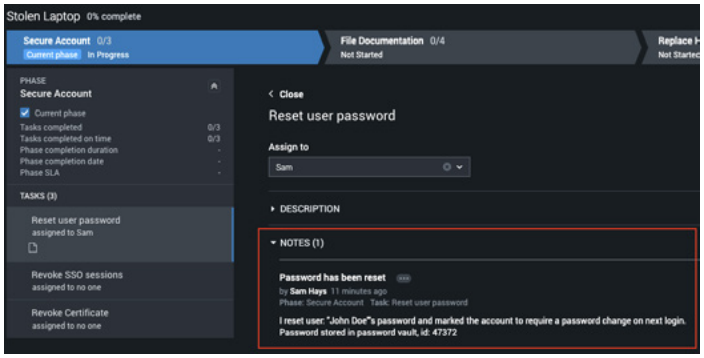
Having an internal platform to discuss sensitive information related to an incident helps the team to stay aligned with regulatory compliance. If a team is dealing with a security investigation and might be discussing a user or their associated attributes, then that may be classified as Personally Identifiable Information (PII). This type of data is protected by various laws and extreme care must be taken when handling it. To that end, keeping this data within Splunk SOAR alleviates the need to understand the Privacy Policies of those other chat systems.



2. Notes

While real-time communication is best suited for the activity pane, well-organized information should be written in notes as a means for easier reading and review. Splunk SOAR provides several classes of notes for this purpose.

- **Task notes:** As an analyst works through a workbook, they may wish to provide detailed descriptions for themselves or their team. These notes provide an intelligible story and the responding analyst would not have to dig through log/machine data to understand the details of the incident.
- **General notes:** General notes can be added to the case. These notes might be used to provide specific context for a specific event and are helpful for building the general story. This can also be a place for any disassociated pieces of information.

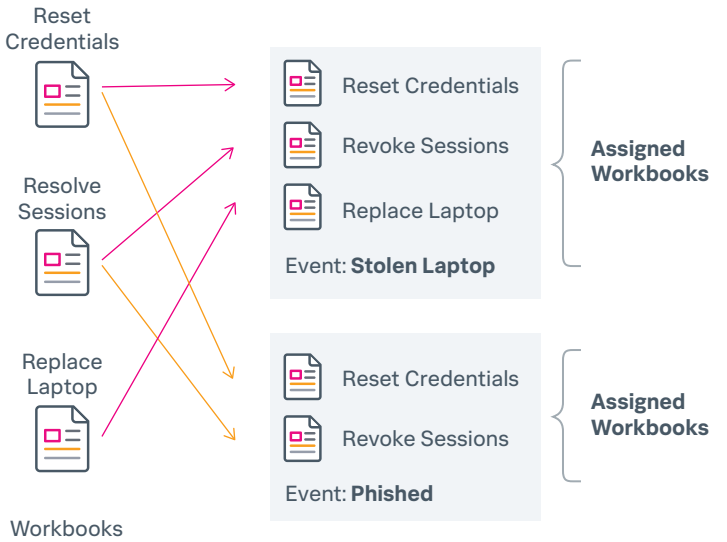


3. Evidence

As an analyst is tracking down all of the various leads during an investigation, many paths will be dead ends and some will provide meaningful results. It's likely that all paths taken will be documented, but that creates noise that must be sifted through to find details of interest. To eliminate this pain point, notes can be "marked as evidence." When this happens, the item will become available in the evidence pane. Once there, the more "interesting" findings of an investigation can quickly be reviewed. The evidence pane can include a number of items including files from the vault, artifacts, action results, associated events and notes.

Workbooks in multiple cases

Unlike many other competing SOAR products, Splunk SOAR allows the analyst to assign multiple workbooks to an incident or event. This provides a consistent, modular approach to workbook design.



In this way, as you create workbooks that represent a discrete set of actions, they can be reused in a myriad of use cases. Better still, when those actions change (e.g., the internal LDAP system changed from one type to another), updating one playbook will be reflected in all future incidents utilizing that workbook.

Case Study: The Phishing Decision

The Splunk SOAR team works with customers around the globe to help them optimize their security operations. The following example represents a real-world case of the initial work one company undertook on their journey to SOAR maturity with Splunk SOAR.

Context: This security team consists of a manager and five analysts with varying levels of skill who respond to security incidents. During the initial process-selection phase, the team decided that of all the various security tasks and responsibilities, phishing represented the best choice given the selection criteria in the guide earlier. Consequently, this is the process which they decided to tackle first.

The scenario: The organization had configured a mailbox called "The Pond" where all employees were trained to send any suspicious email (as an attachment). Users were also instructed to take no further action until they received an email response back from the security team directing them on whether or not they should interact with the original message.

At this point the team had completed the following steps:

1. Decided on a process to operationalize with Splunk SOAR (phishing).
2. Collect data on how this process is executed by each team member.
3. Synthesize the results from step two with the team to build a standard workflow.
4. Run through the newly defined workflow with example cases.
5. Implement the workbook in Splunk SOAR.

Example of a phishing workbook

Data collection phase:

1. Whoever is currently on-call (the responder) will actively monitor the mailbox during business hours. When a new email comes into the mailbox, the responder will create a new event in Splunk SOAR with the label "Phishing Evaluation."
2. The responder will download a copy of the entire message from the mailbox and attach it to the vault in the newly created event (for recordkeeping and future phases).
    a. The responder will open the email in text (or safe) editor for review.

Investigation phase:

3. The responder will evaluate the context of the body.
    a. If the language is obviously nefarious, then they will:
        i. Escalate to a case and set the priority to high
        ii. Create a note detailing the findings
        iii. Add note to evidence board
        iv. Finish investigation phase
    b. Otherwise:
        i. Move to step four
4. The responder will capture all hyperlinks in the body.

5. Every collected hyperlink will be evaluated in VirusTotal.

    a. If it's a positive score:

        i. Escalate to a case and set the priority to high
        ii. Add note with details
        iii. Mark note as evidence
        iv. Finish investigation phase

    b. Otherwise:

        i. Move to step six

6. Each collected hyperlink will be opened via sandbox cloud service and evaluated.

    a. If it's determined to be malicious:

        i. Escalate to a case and set the priority to high
        ii. Add note with details
        iii. Mark note as evidence
        iv. Finish investigation phase

    b. Otherwise:

        i. Move to step seven

7. The on-call person will check the age of the domain.

    a. If it's less than one year old, then:

        i. User will escalate to a case and set the priority to medium
        ii. Add note with details
        iii. Mark note as evidence

    b. Otherwise:

        i. Move to step eight

Decide and respond phase:

8. Responder will:

    a. Record their findings as a note

    b. Mark note as evidence

    c. Respond to the user via email with their findings

        i. If bad, the user will be directed to delete the email
        ii. If the domain is new (but no other indicators are found), then the analyst will provide guidance with their best judgement
        iii. If nothing bad is found, the user will be directed to use caution and proceed.

    d. Close the incident

After every task from our paper-workbook is represented within Splunk SOAR, we have a workbook that should considerably improve the consistency of response from our team. An established process is now in place. This gives us several benefits:

1. We know what to expect from the team.

2. We can evaluate the time it takes for each team member to complete similar tasks.

3. We can begin to track metrics for this incident type.

4. Steps should not be missed or skipped.

5. Ownership/accountability is established.

6. The foundation is set for automation, which will drastically decrease the time it takes to execute a phishing investigation.

In this guide, we've covered the importance of establishing a consistent security operations team by evaluating and streamlining repeatable SSPs. This way, you can ensure consistent quality output from your team every single time. Although building foundational security operation procedures is not an easy task, it is pivotal to a SOC's success by increasing the quality, speed and accuracy of response. Organizations that are looking to not only enhance their security operations with standard procedures but to also increase efficiency with automation and orchestration, should definitely begin to lay the groundwork by building foundational security operations with Splunk SOAR. Here are some key takeaways as you start your journey to implement robust standard security procedures with your security team.

Key Takeaways

Not all security operation teams are the same. Low maturity teams have ad-hoc processes and minimal automation or tool implementation. Medium maturity teams have some codified processes and policies in place but may lack consistent performance measurement and monitoring. High maturity teams have formalized procedures along with orchestration and automation implementation to allow for maximum efficiency and accuracy. Building a mature team requires preliminary work such as creating SSPs. Security teams looking to elevate their workflow and performance should follow this guide to start building a high-maturity team.

Gaining "buy-in" and participation from the team is very important early on because it is likely that staff will find ways to reduce time-to-respond, improve the investigative process, and innovate on other incident types going forward. If the team does not feel that the tool is ultimately going to make their work faster and easier, then trying to create standard security procedures and implementing them will be an uphill battle.

Committing to the tedious work around building standard security procedures will greatly improve the overall security posture of the organization. These processes will help reduce mean time to response, reduce human error, and ensure consistent control in quality and compliance.

Try Splunk SOAR for Free

Additional resources

- Create an account to join the Splunk SOAR Slack Community
- Splunk Answers
- Splunk SOAR Product Tour

Learn **More.**

Splunk SOAR provides security orchestration, automation and response capabilities that allow security analysts to work smarter by automating repetitive tasks; respond to security incidents faster with automated alert triage, investigation, and response; and strengthen defenses by connecting and coordinating complex workflows across their team and tools.

Splunk SOAR

splunk>

22-24068-Splunk-Essential Guide to Foundational Security Procedures-107