THE ULTIMATE GUIDE TO PLAYBOOKS:

Everything You Need to Know About Building Customized Cybersecurity Playbooks

Cybersecurity playbooks are a critical part of every deliberate security plan. Strategically developing a plan for what to do during a cyber event ensures proper action in a potentially stressful situations. Playbooks help reduce response times, costs and overall impact of a security incident.

Playbooks are often a mark of an organization with a mature security posture, as the initial development and documentation can be daunting. In this guide, Brite provides a suggested process to create and implement playbooks successfully, increasing your organization's effectiveness and efficiency.

This guide covers:

- The Basics of Cybersecurity Playbooks: What they are and why they're needed
- Building Cybersecurity Playbooks: Planning, creating and best practices
- How to Implement Cybersecurity Playbooks: Ensuring adaptation across the organization

It is not a matter of "if" but "when" an organization will need a cybersecurity playbook.

Brite
Brite.com
800.333.0498
SalesInfo@brite.com

THE BASICS OF CYBERSECURITY PLAYBOOKS

What is a Cybersecurity Playbook?

A cybersecurity playbook is a collection of proven procedures that determine if an event has occurred and how to properly respond to that event. They are an essential manual of repeatable and predictable methods for all security teams to identify, analyze and respond to security events.

Examples of security events include:

- Data theft
- Phishing attacks
- Unauthorized domain admin access
- Ransomware attacks
- Malware infections
- Simultaneous logins
- Distributed Denial of Service (DDoS)
- Escalation of privileges

Why are Playbooks Needed?

Albert Einstein said, “Life is a preparation for the future”. Proactively preparing for when an incident occurs will greatly reduce the potential disruption. The development of comprehensive playbooks benefits the organization in three key ways:

Consistency

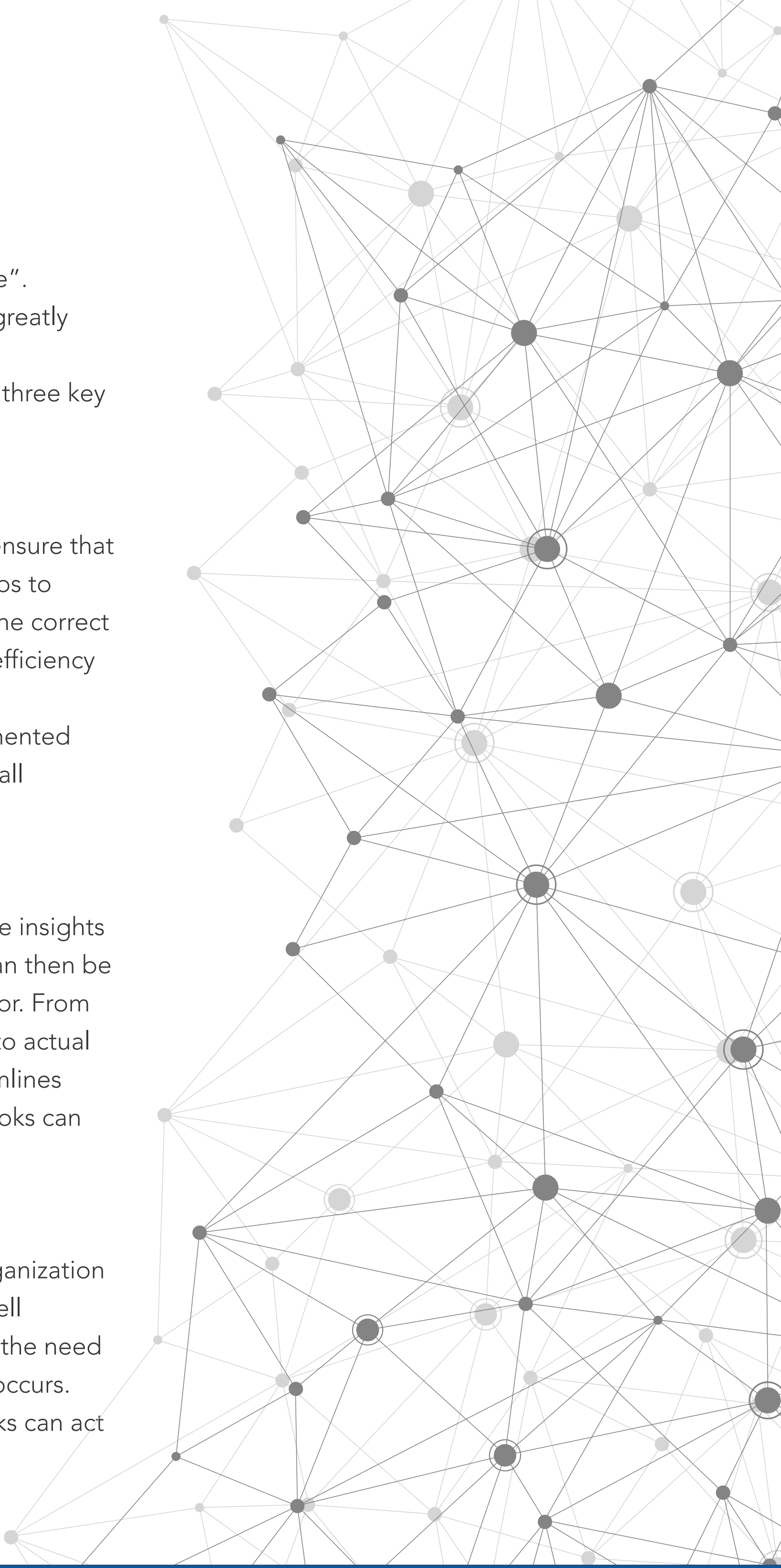
Playbooks provide a repeatable process to ensure that any trained analyst is following the same steps to identify, analyze and respond. This ensures the correct pre-mediated actions are taken to improve efficiency and minimize impact. Additionally, strategic modifications can be made based on documented outcomes and observations to improve overall processes.

Efficiency Through Automation

Consistent and centralized processes provide insights into common repetitive tasks. Those tasks can then be automated to reduce fatigue and human error. From tuning the threshold of when to investigate to actual steps of the investigation, automation streamlines operations. With new AI capabilities, playbooks can fully be enacted without human interaction.

Emergency Preparedness

Cybersecurity playbooks also prepare an organization for a worst-case scenario. A thorough and well thought out playbook will reduce stress and the need for rapid decisions, if and when an incident occurs. Additionally, a developed library of playbooks can act as a starting point when new scenarios arise.



> Playbooks are the great equalizer in our SOC. Everyone is following the same script. This has enabled us to empower even our co-ops to successfully function as Security Analysts within our team. Everyone - a new team member, myself, or even our President - can follow a playbook with a high level of success.
>
> - Jon-Michael Lacek | CTO, Brite

Building Cybersecurity Playbooks

There are two phases to creating cybersecurity playbooks. The first is planning, which includes determining how playbooks will be stored, the efficient format for practical use and which events will be included. The second stage entails the actual creation of individual playbooks.

SELECT A PLATFORM

Are you looking for a simple collection for the playbooks or the most efficient?

A good entry point into playbooks is to utilize documents stored in a centralized file share like SharePoint or Box. By simply documenting the steps using a common platform like Word or Excel, you encourage the internal resources to follow a process. By using a standard medium, the playbook details can be accessed easily and leverage existing backup and collaboration methods. Playbooks will become an integral part of a cybersecurity team's daily operations and inability to access will be problematic. This type of platform is simple, but it leaves the work for the analysts to do manually.

The next option is to use an incident response (IR) platform. The benefit of an IR platform is that it walks the analyst through the process. This helps the new and veteran analysts follow the same process in an interactive manner. In many of the platforms, the user is forced to interact with the system to go to the next stage, moving through a wizard type interface as the investigate, analyze and respond.

Furthermore, an organization may choose to invest in a SOAR (security orchestration, automation and response) platform. A SOAR uses data from alerts to trigger playbooks. A response workflow is then deployed based on the event template that has been built within the platform. Additionally, a combination of human inputs and machine learning are utilized to optimize automated response for efficient handling. Though SOAR platforms provide a tremendous amount of power and ability to automate, it also adds a cost for the organization.

Pro Tip:

A playbook doesn't have to be complex. It can be as simple as a collection of documents. What counts is that the information is there and the continuous updates to keep it current. An organization can always upgrade to an Incident Response Platform or SOAR as the operations mature.

DETERMINE WHICH PLAYBOOKS ARE NEEDED

Start by brainstorming alerts leading to incidents that have actually taken place at the organization. Next, consider additional common security alerts and incidents that the organization is susceptible to. This could be a sizable list. Prioritize the events on that list to select an initial group of playbooks to create and then subsequent groups. The key to embarking on this program is to break it down into manageable pieces.

SET A TIMELINE

Create a concrete timeline utilizing the prioritization list previously created. Teams are more likely to accomplish the project in a timely manner when taken in reasonable sections and tangible due dates are set.

BUILD A CADENCE

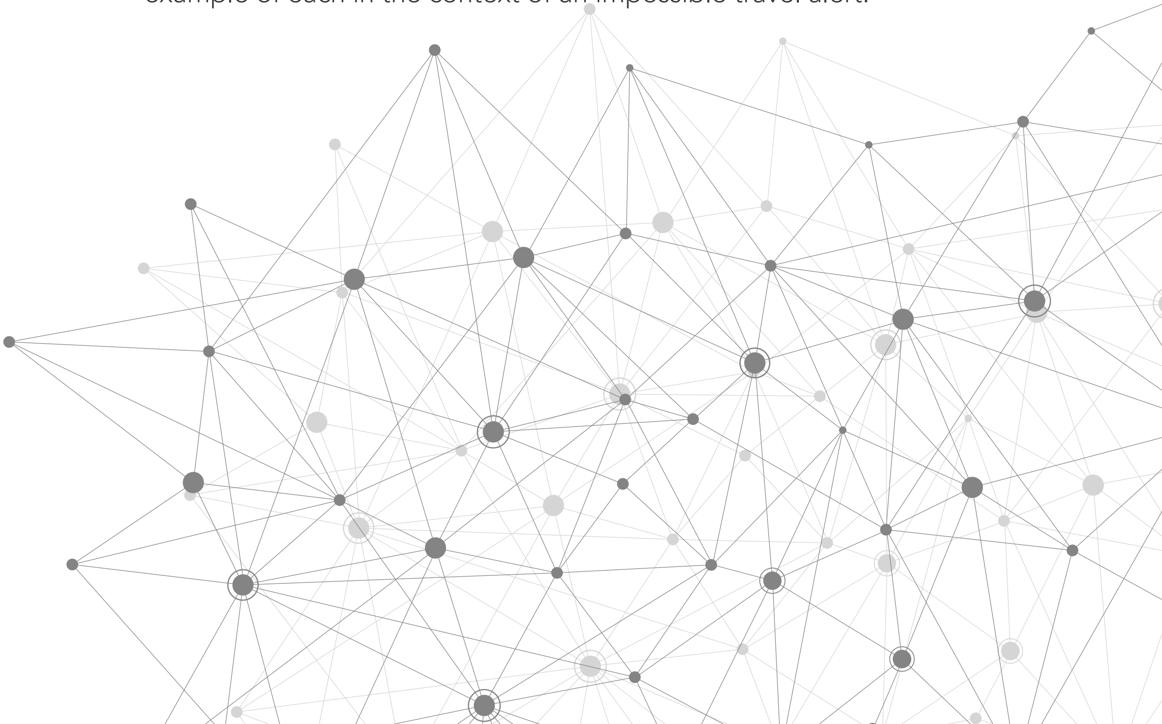
Work with the team on a frequent basis (weekly or monthly) to review the common incidents and further develop the playbook. Don't let it become stale.

DOCUMENT INDIVIDUAL PLAYBOOKS

A cybersecurity playbook's foundation remains the same from organization to organization. These key elements include:

- Identify: What is being investigated?
- Analyze: Is it a true or false positive?
- Respond: Appropriate action based on analysis and playbook guidelines

Below the definition, we will provide an example of what this looks like. We will now explore each of these three steps and share an example of each in the context of an impossible travel alert.



Pro Tip:

Good news - A security team doesn't have to reinvent the wheel when it comes to playbooks. Simply start with a template and tailor it to the organization's needs if a team is using a collection of documents. There are plenty of credible resources available to utilize a generic form and tweak it as necessary like the SANS Security Policy Templates.

1. IDENTIFY

Identify the overall goal of the investigation. Think of this as the main topic of the playbook or the criteria of the analysis. It can be helpful to frame the identification as a question formatted as follows: 'Does the alert from X tool verify that Y has happened?'.

Next, determine what logs need to be collected for analysis if the occasion in question did or did not happen. Outlining what information is needed and available will help guide the process later. For example, if a phishing attack is suspected, logs from email filtering tools, endpoints, firewall, etc. may all be relevant.

Finally, pinpoint the threshold of concern. This is the point where an alert becomes an incident to be investigated. Decide what is noise versus what has potential to be an incident. Additionally, determine how you are going to gauge that threshold. A SOAR platform can be beneficial to automate the triggering of a playbook based on pre-determined thresholds to expedite response time and increase efficiency.

EXAMPLE: Impossible Travel

Low Severity to Medium Severity

DESCRIPTION: A user logged in from locations that are impossible to travel between in the time frame.

IDENTIFY | INVESTIGATE ANOMALY

- What are the locations in the alert?
- Do any of the source IPs or source locations correspond to the tenant's known physical location?
- What was the login type?
- Was the login attempt successful?
- What user is associated with the alert?

Pro Tip:

Playbooks should be comprehensive with the necessary details. Document the threats and response actions taken in detail from this point forward. This will ensure that threats and attacks and general incidents are handled as expected.

2. ANALYZE

It is finally time to analyze. To do so effectively, organizations need to outline what needs to be analyzed. The goal of playbooks is to have any analyst follow the proper process. To ensure this happens, a detailed guide of key points that determine the difference between true positive or false positive are outlined.

A well-thought guide however does not replace the need for talented analyst, ideally 24/7/365. The quicker an alert is investigated accurately, the better the opportunity to reduce the impact.

Additionally, the most common alerts and analysis should be evaluated to see if automation is possible. Replacing manual steps with appropriate automation reduces strain on limited human resources and focuses attention toward the most critical tasks.

Pro Tip:

Data sources from different tools provides insights from different perspectives for the analysis. This is simplified when on open XDR platform with data normalization features is used.

EXAMPLE: Impossible Travel

Low Severity to Medium Severity

DESCRIPTION: A user logged in from locations that are impossible to travel between in the time frame.

ANALYZE

- Does user/source IP regularly trigger this alert?
- Is user/source IP linked to any other suspicious activity?
- Would user have any reason for logging in from either location?

3. RESPOND

Both true positives and false positives require action. Many of the determined actions are centered around proper documentation. A premeditated response including proper documentation will satisfy even the most scrupulous auditor. Now, let us explore the difference in action for a true positive or false positive outcome.

If it is a true positive alert:
Ensure each step of the investigation process has been properly documented. If it is a True positive with impact, move to an incident response plan with documented steps on proper response. Depending on the severity, a response team may need to be engaged.

If it is a false positive:
Document the steps taken to conclude it is a false positive. Use it as a learning opportunity, and determine why the alert was flagged initially. The threshold may need to be adjusted or systems tuned to reduce the noise.

Pro Tip:

Every false positive can be approached as an opportunity to tune your system. Data surrounding why an alert was flagged and its reason for being a false positive is invaluable for improving operations.

EXAMPLE: Impossible Travel

Low Severity to Medium Severity

DESCRIPTION: A user logged in from locations that are impossible to travel between in the time frame.

RESPOND | ESCALATION

If activity is determined malicious (or to help verify malicious activity), reach out to the tenant with details of the alert.

> “To be a SOC II compliant security operations center, a high level of importance is put on processing integrity. As a business owner, I am confident in our ability to consistently and appropriately process and respond to alerts because of the importance put on playbooks.
>
> - Justin Smith | President and COO, Brite

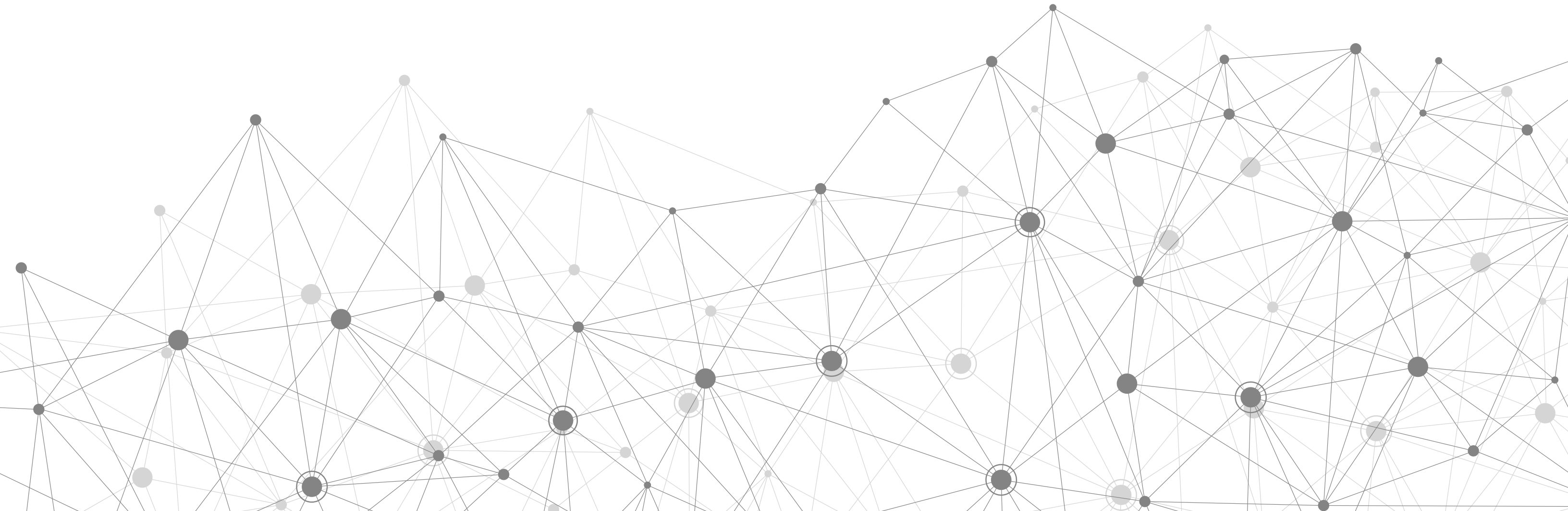
How to Implement Playbooks

“Build it and they will come” does not necessarily apply to playbook utilization. No matter what platform is leveraged, a well thought out implementation plan is key. Below are the key factors to ensure adaptation of playbooks.

Leadership Participation: The entire IT organization must be on board when it comes to playbooks. Keep in mind getting full buy-in won’t happen overnight. Start with the endorsement of key leadership to assist with the adaptation throughout the organization.

Easy Access: Verify employees have appropriate access to both playbooks and the systems required for analysis. It is critical that access is not a barrier to easy use.

Training: With a new process comes a need for training. Allocate time to educate those executing the playbooks on how to properly utilize them, access required information for analysis and document correctly.



BEST PRACTICES

It may feel overwhelming because there are many things to remember when creating cybersecurity playbooks. Here are the top takeaways to remember:

1. Use a Template

Don't start from scratch. Find a generic template based on the security event and develop a playbook and edit it for the unique environment. If an incident response platform or SOAR is being used, templates are often built into these platforms.

2. Automate

Analyze known repetitive tasks within the analysis of alerts to discover which are worth automating. Streamlining resolutions with automation will reduce human error and alert fatigue. Certainly, not every action is worth automating and some cannot be done so appropriately. Strategically automation of tasks balances efficiency and cost-effectiveness.

3. Document Everything

Starting with documentation of current alerts through the outcome of each investigation, the more documentation the better. Any organization will be thankful for detailed documentation when an audit or incident arises.

4. Keep Updating

The cybersecurity landscape is constantly evolving, stagnate playbooks create a risk in themselves. Create a cadence to review and update playbooks. Make data-driven decisions based on industry changes and playbook response data to ensure long-term relevancy.

Pro Tip:

Keep it simple, especially when starting. It is most important to begin with a simple process that can actually be followed. A culture of continuous improvement will help grow the program.

Alternatives to Building and Executing Your Own Playbook

Playbooks are powerful tools; however, it is an effort to develop, maintain and utilize properly. Specialized skill sets from coding to alert tuning and well-training analysts are required. Additionally, 24/7 staffing of analysts for rapid assessment.

For playbooks customized to your organization with ease, opt to partner with Brite and utilize its world-class MSSP service. BriteProtect is powered by an innovative open XDR platform, optimized through an intelligent SOAR platform, and acted on by Brite's talented team.

ABOUT BRITEPROTECT

BriteProtect expertly collects, investigates and responds to alerts across the entire environment. Brite is able to realize additional value of existing tools through innovative data normalization and correlation. Brite's 24/7 SOC 2 compliant service utilizes industry-leading technologies and expertly optimized playbooks, each managed by a team of experts.

The benefit of being prepared for an emergency is inestimable. Let BriteProtect launch your journey with cybersecurity alert response preparedness today.

Brite

Brite.com
800.333.0498
SalesInfo@brite.com