Security Capabilities Improvement

Professional Services - Security Management Framework

Contact Information

Corporate Headquarters:

Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054

About This Document

The Operational Enablement documents are designed to enable and inform customers on how to manage Palo Alto Networks technologies in a consistent and efficient manner. These documents assume that the reader is already familiar with Palo Alto Networks technology and they are meant to serve as sections within a runbook on how to manage the platform once deployed.

These documents do not replace other technical documentation published by Palo Alto Networks on their products and features. For more information about anything referenced in this document, see the technical documentation found at:

https://www.paloaltonetworks.com/documentation

Table of Contents

Overview

This document helps the customer identify where and what improvements can be made to prevent the same types of security incidents from occurring.

Background Information

Capabilities improvements prevent the same security incident from occurring as a result of a configuration setting. This provides the frame of thinking to examine your processes and procedures critically with an eye to constantly improve and refine, with an end goal to reduce the time it takes to mitigate a security incident.

Prerequisites

In order for the SOC to provide recommendations, it must have the visibility and knowledge of the tools and products that are in the environment. If the SOC does not have the visibility, they cannot provide specific recommendations on configuration changes. Without the knowledge and training on the tools that the company uses, the SOC cannot provide informed recommendations that can merge the security needs as well as the business needs.

Capabilities Improvement

The first thing that is necessary to improve on security capabilities is to know that an incident occurred. If the initial detection did not occur in a timely manner, either as a result of a lack of visibility or due to misconfiguration, we are unable to assess any further steps in the response process. We want to ensure that we are detecting incidents at the earliest possible phase of the attack lifecycle to ensure we are minimizing the impact.

Always validate that logging is in place. Regardless if the event was permitted or blocked, make sure that the action taken was logged and that log was sent to a SIEM or log repository that the SOC can utilize. Without a log of what occurred, it is impossible to determine what other potential mitigations or configuration changes are needed since we would not know what action was or was not initially taken.

If multiple layers of detection and/or prevention exist, did all layers detect the attack appropriately? If only a single layer detected, ensure that the configuration and visibility match across all layers. This is also a good practice to make sure all prevention mechanisms do not rely on a single point of failure.

The technologies and tools in place should prevent the same attack in the same way each and every time. Ensure that this consistency exists. This consistency allows for playbooks and automation to occur as the attack and vectors are known and documented, and the response is consistent, and the impact and risk of mitigation is quantified.

Evaluate how the tools and technology responded. Should they have alerted or mitigated differently or more quickly? Even if the tools do not yet possess the capability, perhaps the vendor can be engaged to add that capability or improve upon the existing capability. Do you have a technology or capability that is able to detect or mitigate the event, and if not, evaluate if an existing tool can be adapted to fit the need or if a new tool is needed? Also consider if the required capability exists on the market. The required capability may need to be custom-built for your specific security situation.

If the same style of attack occurs, but the indicators are slightly different, would the detection occur in the same manner and the mitigation be the same? You want to validate that the detections and protections are not so specific that they exclude similar types of events because the indicators were overly specific.

Questions to Ask of a Security Incident

There are a few high-level questions that should always be asked to validate that all that could have been done to prevent the incident.

- Did we detect the attack as early as possible, or could it have been detected earlier in the attack lifecycle?
- Did all applicable tools detect the attack, or only a subset of the appropriate tools?
- If this same attack happened would we respond the same way each time?
- If this same attack happened how should we respond versus how did we respond?
- If this same attack changed its IOCs (IP, Domain, URL, Hash) how would we respond?
- Do we have controls in place that could have prevented the threat (IPs, Antivirus, NGFW)?
  - If yes, how can we configure these controls to prevent the next threat without impacting existing network activity?
  - If no, does a technology exist that could have prevented the threat?
- Is there a way to reduce the time that it took to identify, investigate, or mitigate the security incident?
- Is the proper logging in place to validate the capabilities are working as intended?
- Can we replay the incident and ensure the same response each time?