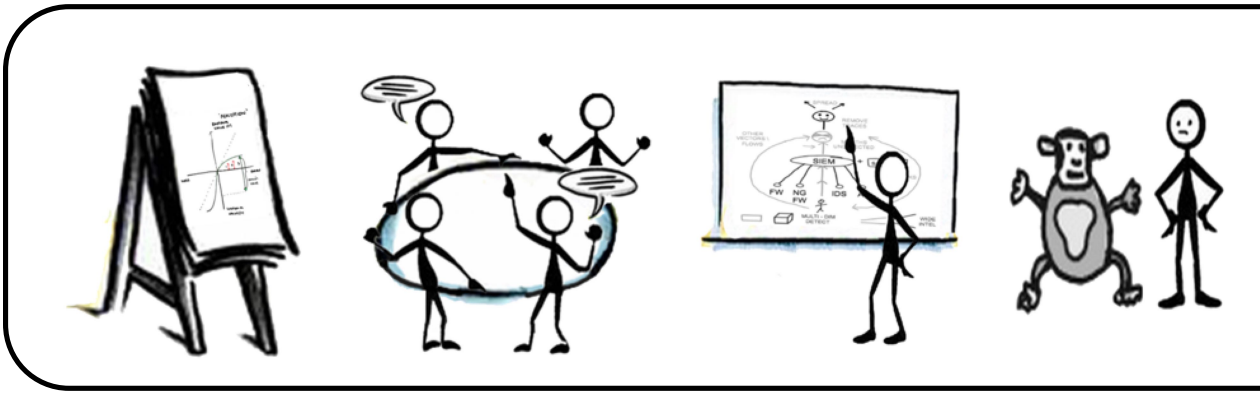
paloalto NETWORKS

Cause to Act Dialogue Guide

E.U. Version 4

Slingshot Guru Launch



SlingshotGuru
stories that sell

How to use this document

This guide provides instructions for delivering your Palo Alto Networks Cause to Act story.

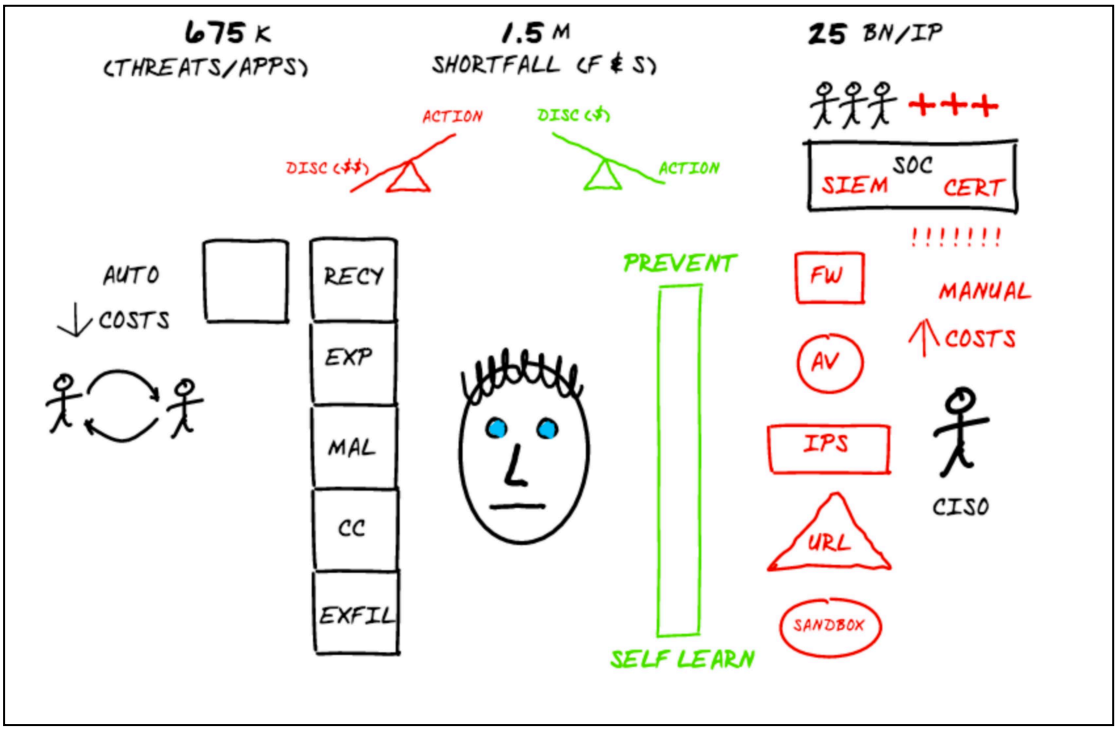
The information on each page of the guide is divided into two areas. The top half of the page shows a picture of your storyboard as you are drawing it and working your way through your Cause to Act story. Below this, in the bottom half of the page, the 'What you say' section contains your Cause to Act script.

The white numbers highlighted in blue within the script refer to their corresponding numbers displayed on the picture of your storyboard, and show you the order in which you should draw your story on the flipchart.

Words in the script that are highlighted in red have negative connotations, while words highlighted in green are positive. This is to help you summarise each story focusing on the points of contrast (the bad way compared to a better way).

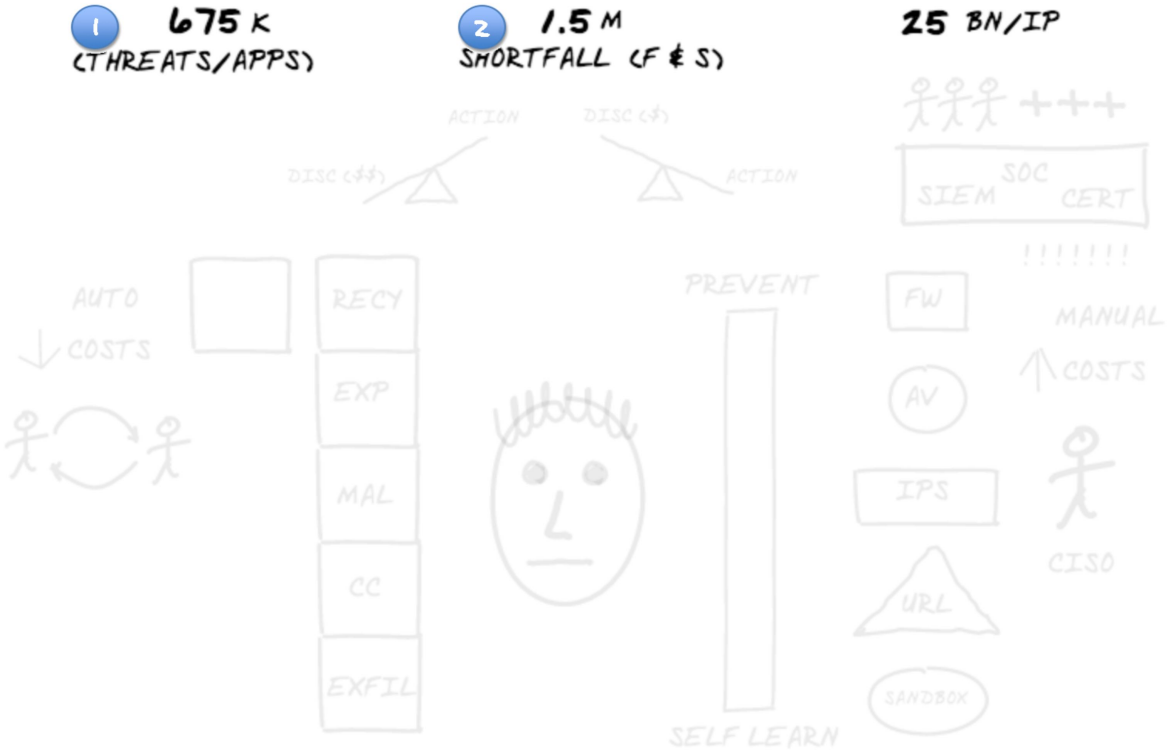
Each storyboard of your Cause to Act story builds into a big picture, which looks like this:

The Big Picture



1

Storyboard



1

What you say

These numbers (675, 1.5 and 25, already displayed) tell a story about your world. About the world of protecting your business from cyber attacks.

In 2015 the Application Usage Threat Report from Palo Alto Networks saw 675 k 1 distinct threats 2, across almost 3000 applications. I'm sure you've already heard such frightening statistics. But what does this actually mean in real terms to your business, to your team, or to you personally?

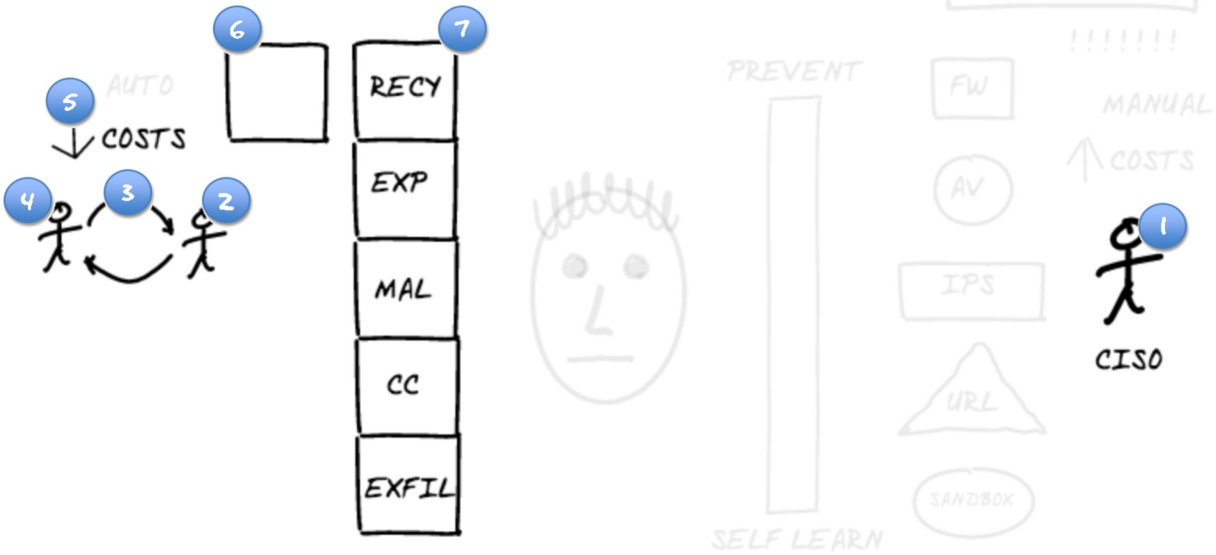
To get a feel for that kind of meaning you need more context that's relevant to your world.

This next number sets some context to this ever-increasing onslaught. 1.5 is actually 1.5 million 3. According analysts Frost and Sullivan, this is the shortfall 4 of cyber security professionals by 2020.

This demand outstripping supply is good news if you're a security professional looking for a job, but not so good news if you are trying to recruit cyber security professionals into your organization or retain your existing workforce.

In the next few minutes, you're going to see how many organizations have a model that is becoming harder and harder to sustain in this world of more threats and less availability of security staff. More importantly, you'll see how many security professionals are taking action to alter their defensive model to take advantage of the valuable assets they already have.

Storyboard



What you say

CISOs 1 of course defend their organization. Against what, though? Against an attacker 2. Today, though, it's not just an attacker; it's a market place 3 & 4: that means groups of people sharing best practices with each other—trading with each other.

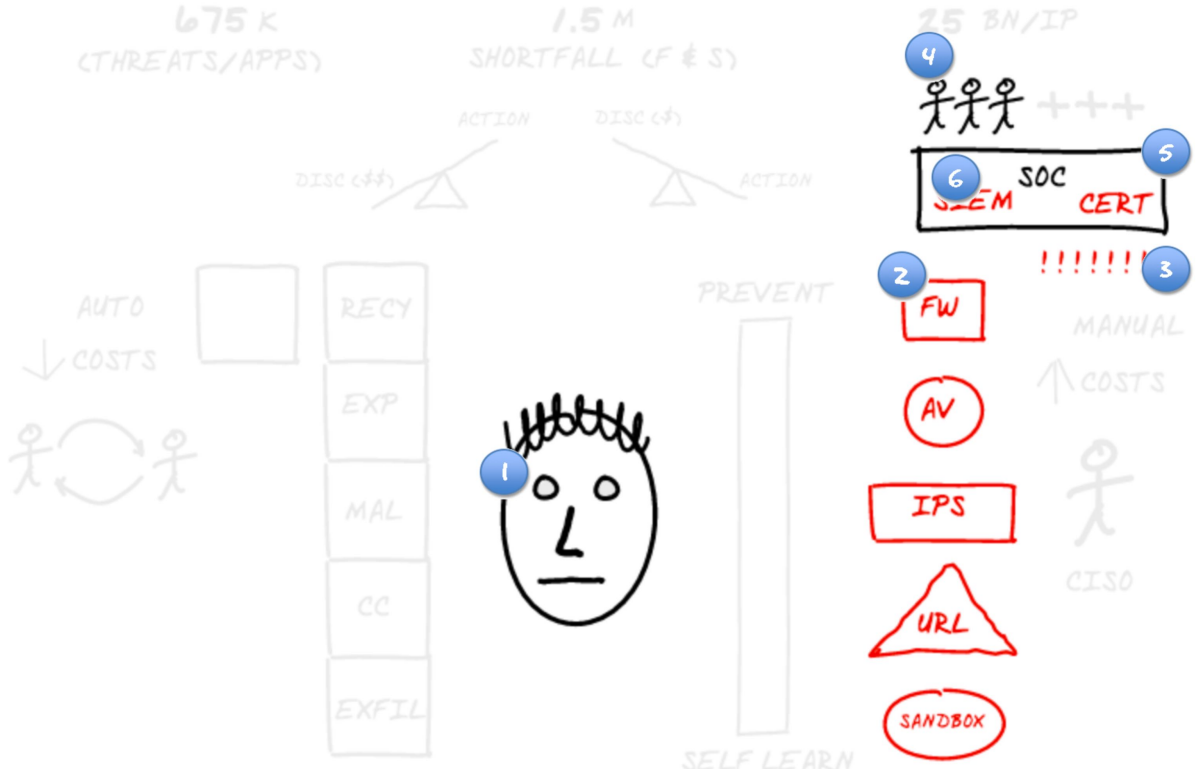
A few years ago some governments were investing huge amounts of resource to develop incredibly sophisticated attack approaches. Today anyone can purchase the same attack kit online for a few dollars, complete with instructions and how to get started video.

It's getting easier for attackers because of their **decreasing** costs 5 and the abundance of resources available to them. And they only have to be successful once to win—that's probably a tiny percentage of their attack attempts. Contrast that with the CISO who has to successfully defend 100% of the time. Attackers are **crowd sourcing** and CISOs are **on their own**.

Whilst in the past the make-up of an attack may have been made up of a **single object** 6 or component, the most significant change is that today's attacks are **multi-faceted** 7.

The first stage might be that they perform a reconnaissance of their target in order to try and look for weaknesses, to try and establish what you have of value. In the next stage, they'll choose the method of attack from a wide arsenal—the exploit itself. The exploit of a weakness. After they are in your network they'll use malware to discover your valuables and then establish command and control. A solid pathway from your organization back to their own before they exfiltrate your sensitive data.

Storyboard



3

What you say

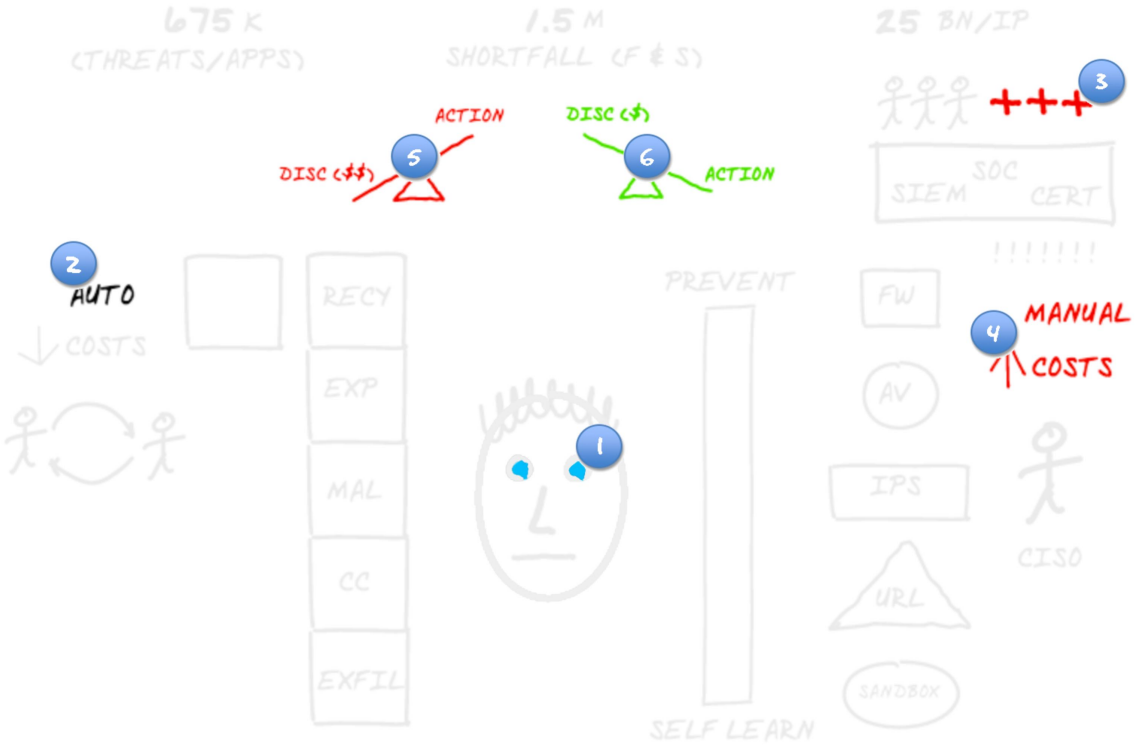
For each one of these stages, your attacker has many options to choose from. It's very hard to put a face to your attacker, but imagine the whole multistage attack is like a facial recognition system 1 with characteristics. Head shape, hair color, eye color, nose and mouth. Each characteristic corresponds to a different stage of the attack.

But in the same way as there are about 7Bn people on the planet, your attacker has a similar number of combinations to choose from in order to form their disguise. It's as if your attacker can disguise themselves as anyone on Planet Earth. And it's your job to spot them and minimize the damage they can cause.

What do may organizations do today? Well they have a number of different solutions 2 —FW, Antivirus, IPS and more. Each one of these is good at detecting a suspicious characteristic—they don't detect a criminal, just individual characteristics. Suspicious eyes. A suspicious nose. Suspicious hair color. Every time that happens, alerts 3 are generated.

And to manage these alerts, organizations are putting more and more people 4 inside a Security Operations Center 5, sometimes with a SIEM 6 and a CERT. All trying to separate the false positive alerts from what might be a real threat.

Storyboard



What you say

At one time this was effective, but not any more because there are just too many alerts. Let's say you detect a characteristic that is a known threat and you block it. The attacker just needs to change that one characteristic that you blocked, represented here by changing their eye color 1 and they are back in business. It's likely that they the attacker can do this very quickly using automation 2.

The more threats that appear, the more alerts that are generated and the more people that are needed 3. And as you've seen, the availability of such professionals is rapidly shrinking. Your security staff typically have skills that go way beyond the monotonous task of sifting through alerts searching for a threat. With the demand for security staff increasing, they have more choice of where to work, and they might consider moving to a place where they can really challenge and improve their skills.

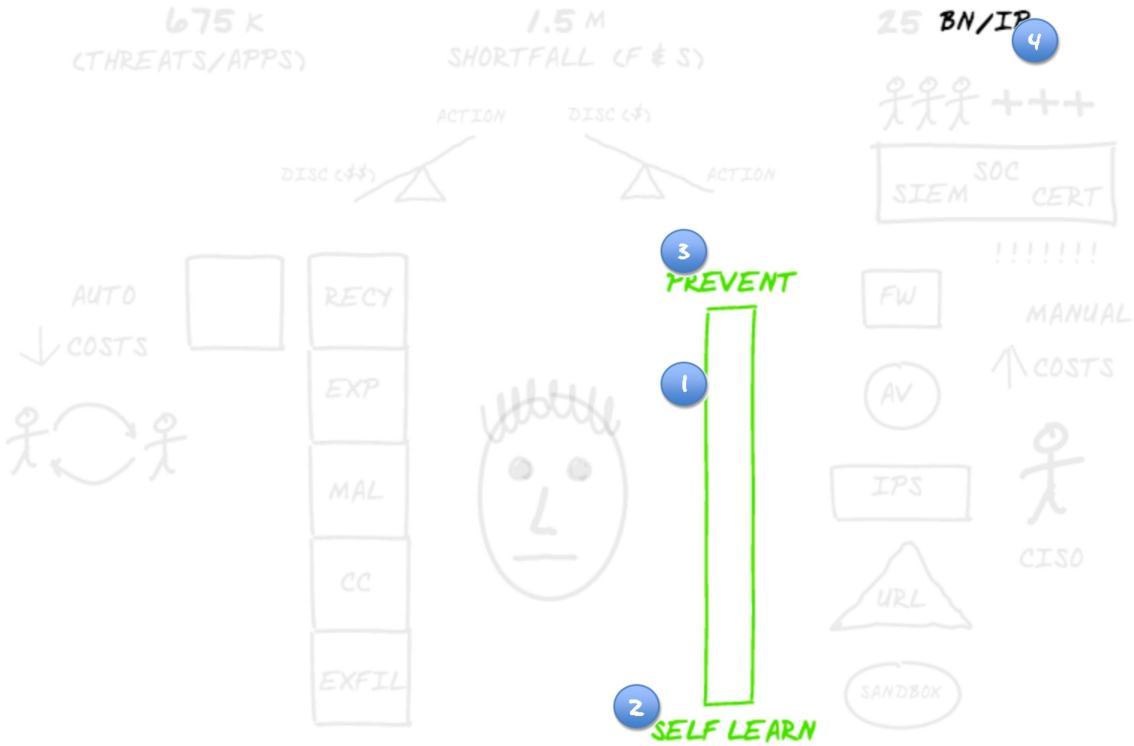
Organizations are faced with the situation where the attacker has **low costs** and **automation**. And the defender has **high costs** 4 and human beings performing **manual tasks**.

This is why leaders are looking for another way, because this model is hard to sustain. Perhaps unsustainable.

Imagine if you could change the balance 5. At the moment this precious resource—your people—is focused mostly on discovery. Taking productive business action is secondary. This model gives a poor return. What if your people only took productive business action 6 and the discovery part was automated? That model would give you a much higher return. Imagine if instead of your technology looking at **individual characteristics** of the photo-fit, it looked at the **whole picture**—all the characteristics—in a single pass.

5

Storyboard



5

What you say

Instead of detecting suspicious parts of a possible attack, you consider all 1 the characteristics and automatically detect a dangerous face. Even if your attacker changed one characteristic like they did before, for example if you can recognize the command and control protocols, even though another part might have been changed, you can block the whole attack. The overall face would be detected and blocked. And what if your automation was so extensive that it self-learned 2 in real time from hundreds of thousands of attacks that go on all the time in the world every day?

If you had that, then a new model could become a reality. Instead of **detecting** intruders and deciding how to respond, you could move to a model of **preventing** 3 them.

This brings us to the last number. It's actually 25Bn 4. According to Networking giant Cisco, by 2019 there will be 25Bn devices connected to the Internet. There are 16Bn today. That's a 55% increase in your attack surface to protect. The faster organizations consider a model that isn't dependent on hiring more and more people, the sooner they will have a defense model that they can sustain in our changing world

It would mean that they wouldn't have to keep on hiring new people. It would mean that the people they do have could use their skills to take active business action. They would be able then to keep their business secure and keep their best people engaged and employed in a model that is sustainable.

That's what I'd like to talk to you about today.