expel™

How to get started with the NIST Cybersecurity Framework (CSF)

By Bruce Potter

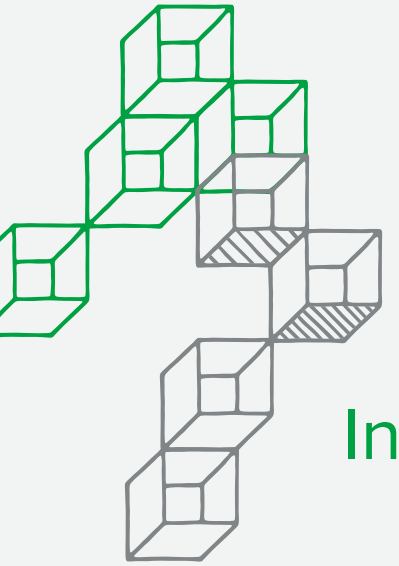
www.expel.io

Contents

About this doc

Alright, let's address the elephant in the room. Frameworks aren't known for being page turners — even when they're shortened into seven characters like the NIST CSF. But there are some things you do because they're "good" for you — like going to the doctor, eating well and exercising. The NIST CSF is like that.

While we can't turn the NIST CSF into the latest best seller (sorry!), we can give you a quick tour and show you exactly how Expel can positively affect your NIST CSF ratings — both now … and over the long term.



Introduction

Newsflash! The NIST Cybersecurity Framework was never intended to be something you could *"do."* It's supposed to be something you can *"use."*

But that's often easier said than done. The CSF can be a confusing and intimidating process to go through. So, if you're at a loss about how to implement it, you're not alone.

But rest assured, since the CSF was released back in 2013, lots of organizations have done it, including Expel. Like others, we've found it to be a useful tool to help us understand where we are and where we're going as we grow our broader cyber risk management program.

Here at Expel, we are our own customer. That means we use our own service as part of our internal IT security efforts. I've honestly been shocked at the impact using the Expel service had on our CSF scores and wanted to share what I've learned about how Expel can help you on the road to CSF nirvana.

A three-minute tour of the NIST CSF

Let's start with a "CliffsNotes" overview.

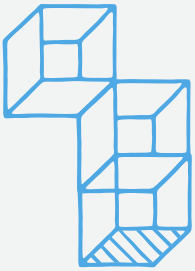
Like an apple, at the core of the CSF is, unsurprisingly, the Core. The Core is meant to capture the entirety of cybersecurity. Yup, pick anything related to cybersecurity and it should be in the Core. If you're thinking "that sounds ambitious" you're right. To capture everything, the Core is broken down into buckets (and even more buckets inside those buckets).

Or, if you're more outdoorsy, you can think of the Core as a big tree with big branches (aka functional areas), which have smaller branches (aka categories), which have leaves on them (aka sub-categories). Whatever metaphor you choose, the sub-categories have the specific types of things you should probably be doing.

The Core has functional areas: identify, protect, detect, respond, and recover. These are basically the lifecycle of cybersecurity without actually being a loop.

Under each functional area, there are categories. For instance, under Identify, there's asset management, business environment, governance, risk assessment, and risk management area. Under each category, there are (unsurprisingly) sub-categories. For instance, under asset management, there are six sub-categories including things like "Physical devices and systems within the organization are inventoried" and "Software platforms and applications within the organization are inventoried."

The Core is nothing if not comprehensive. It's a big tree, but it's a tree that can really help you mature your cyber risk management posture … which is pretty unique for a tree.



Find your baseline (in two hours or less)

Whew! Now that we've got that out of the way, what can you do with the Core?

At Expel, we've found the CSF Core can be super helpful to describe where we are and where we want to be with respect to cyber risk management. The first step is getting a baseline of where we're at today.

Here's how we suggest figuring out the "as is" state for your organization.

Start by looking at the sub-categories. You'll see lots of very specific things that you should be doing. For example, under **Anomalies and Events** (AE) in the **Detect** (DE) functional area, there are five sub-categories:

- **DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed
- **DE.AE-2:** Detected events are analyzed to understand attack targets and methods
- **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors
- **DE.AE-4:** Impact of events is determined
- **DE.AE-5:** Incident alert thresholds are established

You'll probably look at these sub-categories and think "yeah, I'm kinda doing those things," which is good. But how *well* are you doing them? At Expel we use a six-point scale to rate ourselves on each subcategory (we're computer scientists, so our scale starts at 0). Here's what the scale looks like:

0 Nope, we're not doing this at all

1 It's ad hoc, we only do it in cases where we have to

2 We do it … but it's not consistent or structured

3 We do it consistently … but it's not best practice and it could be better aligned with the business

4 We do it well and I wouldn't be ashamed to show this to my peers

5 We're world class (as in, we're one of the best in the world)

By applying this scale to the (gulp!) 98 sub-categories you'll get a good measure of where your organization stands. Just don't forget that there are *98* sub-categories. So, don't overthink it. You don't need to spend a bunch of time debating the finer points of each score.

For instance, resist the urge to add significant digits to the scale. Try to stick with integer ratings. If you must, allow yourself ½ increments (for example, you can score a 2, 2.5, 3, 3.5, etc). If you're incrementing by tenths you're in the danger zone … and under *no* circumstance should you go to the hundredths place. Not ever. That's far too much specificity for what's meant to be a quick assessment of where you stand.

At a leisurely pace of two sub-categories per minute you'll be done in an hour and even have time for a break.

Once you're done with the self-assessment, take that break and then do it again. But this time, instead of documenting where you *are*, document where you *want to be*. When building your "to-be," be aware that (with the rare exception) you don't need to be a five. Being "world class" in anything takes a lot of effort and resources. Organizations that require world class security controls generally know it and are prepared to shell out megabucks (or megaBitcoin) to achieve it. In most cases you should probably be shooting for a four — sometimes a bit higher, sometimes a bit lower.

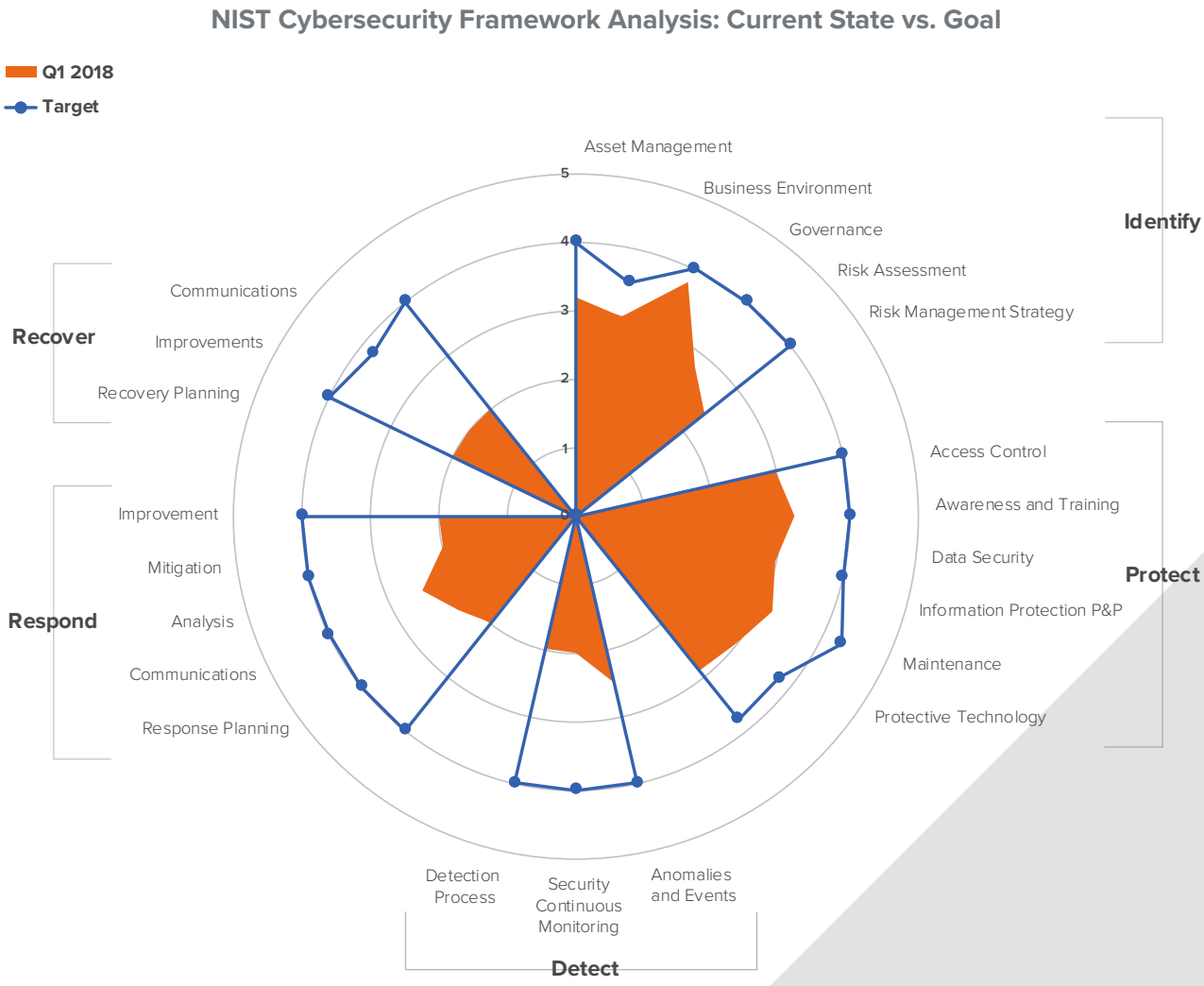
Charting your course ... literally

OK. So now you've got a lot of data and you're thinking "how the heck do I analyze and interpret all of this data" and "how are my execs (who only understand simple shapes and primary colors) going to understand this?" You're in luck. With this "how to", we're releasing the Expel self-scoring tool for NIST CSF. It's an excel spreadsheet that'll track all of your info and (bonus!) it'll autogenerate fancy shmancy radar charts for you.

The spreadsheet rolls up all of your scores for each subcategory into an average for the category that you can use to see exactly where you stand and where you want to be. You can see an example of the type of graph the spreadsheet can create on the next page.

These graphs do a good job of highlighting the areas where you're doing really well (in this case, Identity: Governance) and areas where you need to focus your efforts (Detect, Respond and Recover). Every organization is different, so don't let the gaps freak you out. Remember that the CSF is an attempt to cover *everything* in cyber risk management. So even in large, mature organizations there are going to be areas that haven't been a priority and large gaps between where you're at and where you want to be.

Now what? Well, it's time to prioritize and plan. Unfortunately, we don't have a spreadsheet to autogenerate that. Based on your business needs and the types of risks you're most concerned about, you'll need to figure out what gaps you want to work on and how you're going to close them. It's important to set expectations (with yourself and up the chain). Closing gaps isn't a short-term program. What usually emerges is a strategic plan with lots of little pieces that fall into place along the way.



ProTip

Re-evaluate yourself quarterly. It's a good way to check your progress, keep yourself honest and tweak the plan if need be.

Using Expel to color in your CSF

As I mentioned before, we've gone through the exercise I outlined above here at Expel. And we also *use* Expel to *protect* Expel. As a result, we've got an idea of how Expel can impact CSF scores.

To understand the answer, first you need to understand a bit of what Expel does. In short, our transparent managed security service monitors your network 24x7, investigates bad activity and helps you get the answers you need so you can respond to attackers and keep them out. We do that by using your existing security technologies and ingesting the alerts they create into our Workbench to keep tabs on what's happening in your network. No new endpoints to deploy, no complex integration.

Expel's first-year impact

For this example, let's assume you've got a reasonable set of existing security controls: you have antivirus on the desktop, a next-gen firewall of some sort and maybe even some other intrusion detection product. But you don't have anyone whose job it is to look at those systems. You're hoping they're defending your network and that they'll sound a siren or blast a red light when something is wrong. In that case, your CSF graph may look a lot like the one above. Now, let's say you decide you want to move to Expel and want to know what your scores would look like. Take a look at the chart on the next page.

Quite the change. Now, let's look at each functional area.

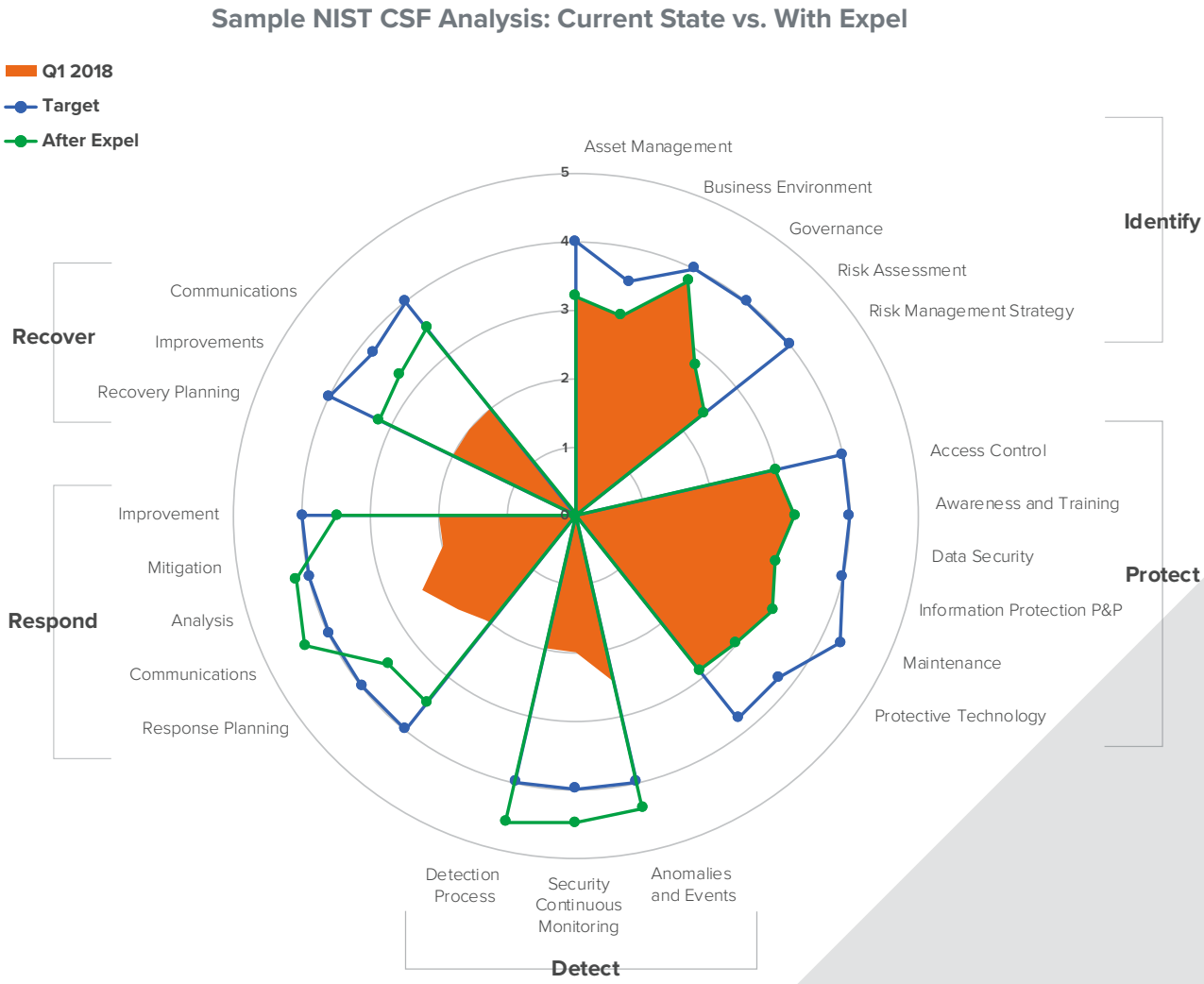
Detect

Since Expel is a 24x7 service that detects bad and anomalous activities on your network, it lifts all of the Detect scores across the board. Our detection and correlation capabilities, which our analysts and engineers are constantly refining, detect threats in your enterprise and present them to our analysts in a structured and consistent way, 24-hours a day, seven days a week. So, it kinda makes sense that outsourcing your security operations leads to better scores in the Detect function.

Respond

In the Respond functional area, Expel also has a dramatic impact on each category. Our remediation actions are the reason we can move the needle so much. When we detect a potentially bad activity, we kick off an investigation. Our analysts look at the alerts, gather related data and if we find there's something legit bad going on, we declare it a security incident.

But we don't stop there. We also give you remediation actions for each incident. These actions are concrete steps that you can take to address the threat,



accompanied with our analysis and other supporting material. This process adds consistency and technical completeness to your incident response, so you can quickly address the attack and get back to running your business.

Our remediation actions allow you to stand on the shoulders of our world-class platform and analysts, so you get a world-class response capability. It's a huge lift in an area where many organizations struggle to even get to a "three" despite years of trying.

Recover

Expel impacts the Recover functional area a bit less than Detect and Respond. Recover is focused on longer-term incident response issues like corporate lessons learned, updating plans, and reputation management. That said, Expel still impacts your Recover score since you're more informed about the incidents you've experienced and the remediation steps you've taken. The net result is that your Recover activities are better informed and more mature.

Expel down the road

Now, fast forward 12 months and let's look at what things look like after you've been an Expel customer for a year. Unsurprisingly, you'll continue to make incremental improvements to Detect, Respond and Recover as you continue to refine those functional areas. But now there are also big jumps in Identify and Protect because over time Expel provides more and more impact in the early lifecycle functional areas.

As we get to know you as a customer, we learn more about your systems and networks — including what's normal and what's not. Over time, we'll uncover actions we think you should take to make your enterprise more resilient to attack. These resilience actions might be configuration changes on your firewall or data protection systems, user training to help with phishing or removal of accounts with shared roles so you can audit more easily. Our analysts know a lot about security, and

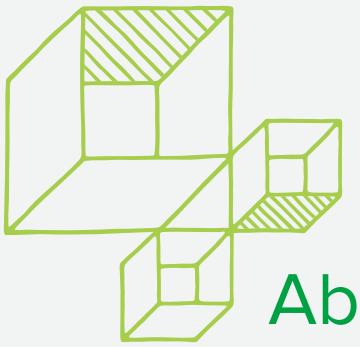
Sample NIST CSF Analysis: Expel on day 1 vs. Expel on day 365

we feel you should be able to learn from their expertise. We'll send you resilience actions whenever we uncover these deeper concerns. Sometimes these "ah-ha" moments will come in the middle of an incident. Other times, we might be out getting a cup of coffee when inspiration strikes. Whenever we have an idea that'll help make your organization more secure, we'll pass that along.

Really?

I know it sounds too good to be true. And I confess I'm a skeptical curmudgeon so even I was surprised. But … yes … really, Expel can help you rapidly close the gaps between where you are and where you want to be from a security risk management perspective.

Heck, that's why I work at Expel. I feel strongly about helping businesses of all sizes be more secure — not just big companies with huge security and risk programs. I think Expel is unique in this regard and can provide a nearly instantaneous lift for your security posture for relatively little expense and time.



About Expel

Expel provides transparent managed security. It's the antidote for companies trapped in failed relationships with their managed security service provider (MSSP) and those looking to avoid the frustration of working with one in the first place.

Transparency is the unique bit. You get 24x7 access to our security analysts so you can watch investigations as they're unfolding and take action immediately — all within a shared interface. Our analysts monitor your environment and investigate suspicious activity using the security products you already own. When we find a problem, we tell you exactly what to do about it including how to fix the root cause of problems that happen over and over. To learn more, check us out at www.expel.io

(this is the last page)

expel™

Expel provides transparent managed security. It's the antidote for companies trapped in failed relationships with their managed security service provider (MSSP) and those looking to avoid the frustration of working with one in the first place. To learn more, check us out at www.expel.io.