Security operations | 7 min read | Feb 28, 2018 | by Yanek Korff

How much does it cost to build a 24x7 SOC?

The phone rings. It's your boss.

"How much is it going to cost us to take our SOC to 24x7?!"

It sounds urgent. Turns out he's calling because he just saw someone tweet about a data breach at one of your competitors. You're tempted to throw out "a million dollars" as an estimate. It seems as good a place to start as anywhere. But is it? After all, the costs of building and operating a 24x7 security operations function can vary greatly.

One of the biggest factors impacting cost is how "good" you want to be. Do you need an excellent security operations center (SOC)? Or just one that's good enough? Or maybe something in-between? Turns out there's a "floor" cost that you're unlikely to go under if you're shooting for "competent." Beyond that, the sky's the limit. Let's take a look at how we get to a right-sized answer that fits your particular situation.

Night of the roundtable: adjectives matter when you build a SOC

It's tempting to whip out the calculator and start adding up the dollars … but not all SOCs are built alike. Are you building something basic? Advanced? What do these adjectives even mean?

A few years ago, our CEO was hosting a roundtable dinner with a room full of fellow CEOs. The topic was cybersecurity operations and the CEOs felt strongly that they needed to up their game. What they were doing just wasn't good enough. It was time to push the pendulum to "state of the art." What exactly does that look like, and what's the price tag? Let's look at the spectrum of what a SOC might do.

Security Operations Center (SOC) Capabilities

What it is...	What it looks like...
Basic detection	You're out of the alert quagmire and can determine which alerts matter by correlating network, endpoint and SIEM events (including, of course, in the cloud).
Investigation	Most security products aren't good storytellers. It's not (necessarily) their job. A well-rounded SOC can investigate critical alerts and "tell the story" about what happened. Investigation answers the what, when, where and how questions that inform your response.
Remediation	Once an investigation is done, it's important to have clear answers about what to do next. A SOC with remedation capabilities tells you how to fix the bad thing that just happened (and hopefully prevent it from happening again).
Hunting	When you plug in your security tech it'll generate alerts. But it won't find everything. By having analysts proactively drive your tech to find things that your products don't automatically alert on (aka "hunting") you improve your detection capability another notch.
Orchestration	If your security practitioners are doing security work (and not just pushing buttons and keeping the security tech running), then chances are they've got orchestration. It's a newish concept (and product category) in security operations. It basically boils down to streamlining investigation and remediation workflows.
Continuous improvement	This one kind of explains itself. But it's rare. If your SOC has gotten beyond treading water (aka processing alerts and fixing what's amiss) and is making steady improvement to your security posture then you're in the continuous improvement zone.
Periodic testing	How do you gauge if it's working? You need to test it. That usually means having a third party perform some outside-in testing from time to time to make sure your SOC is finding what it needs to and, ideally, getting better at it over time.

Whew. That's quite a lot of capability — and it begins to represent what a state-of-the-art SOC entails. Add all of that up and depending on how big your organization is, this could cost anywhere from a few million dollars to half a billion (or heck … even unlimited).

Now, back to that CEO roundtable. After the whole state-of-the-art discussion, one of the CEOs in the back of the room raised her hand, "Considering we're not a big bank … what's good enough and how much does that cost?"

Frankly, the foundational investments for "good enough" aren't any different than "state-of-the-art." You'll need people. While there are seemingly endless shift schedules to choose from, our experience building 24x7 security teams tells us that the minimum number of people you'll want operating in a SOC is 12. You could probably get by with eight, but vacations and illness will result in individuals being stranded alone on shift. Considering even entry-level security analysts command $75,000/year in salary alone, your cost to operate a SOC starts at roughly a million dollars.

Beyond people, the next largest impact on your SOC's efficacy will be your technology and how easy you can make it for your people to use. Any SOC that doesn't have the right technology to provide visibility, detection and investigative capabilities will end up being pretty useless, regardless of how many people you throw at it. While the technology bill at smaller organizations will only be a fraction of the staffing costs, as an organization grows, those tech costs can really skyrocket.

Now that we have a sense of our base costs, let's imagine four possible security operations centers. These examples map relatively well to examples we've seen in the field — both at customers and at service providers.

1. The basic SOC

This SOC focuses primarily on detection (but not so much on investigation). They've invested sparingly in technology and have an odd assortment of visibility, partially due to investments the last CISO made and partially due to limited current budget. Analysts work primarily in a SIEM that was deployed several years ago and it just hasn't been kept up to date. Overall, these technologies offer decent detection capability but there's not much flexibility to tune how they work with additional intelligence or use them for more advanced investigative use cases. Spending time doing investigations or engaging in "hunting" isn't really in the cards at all.

There hasn't been a major incident, but the current CISO worries: if there were, would his SOC find it?

2. The intermediate SOC

At this level, the SOC has mastered detection and the technology investments provide reasonably good visibility into the organization's nooks and crannies. Beyond the basic detection capability of a SIEM fed by event logs, the SOC has deployed a combination of EDR and network forensics technologies that provide advanced threat detection. Security analysts operate at multiple tiers — some of the more senior practitioners frequently leave the SIEM to take advantage of unique capabilities their advanced tech offers. The team really wants to spend more time being proactive, but "operational reality" makes that difficult.

SOC management oscillates on a day-by-day basis: some days they're confident about the capabilities of their SOC and other days they feel blind and they worry there's stuff on the network they don't know about.

3. The advanced SOC

SOCs that get to this level have made a tremendous investment in tooling to free up their analysts' time. Tier one and two analysts are working primarily in a SIEM. But that's only because they've taken the time (along with a good dose of help from outsiders) to tune their correlation rules and plug some of their more specialized products into the SIEM. They can even pull data from their network and endpoint security products without leaving the SIEM. This improves the quality (and speed) of their investigations. When they escalate incidents, tier three analysts pick them up and pivot directly to more sophisticated analysis tools and consoles.

While good things come in threes, advanced SOCs often add a fourth cadre of analysts called the "hunt" team. They're not part of the 24x7 rotation. They focus exclusively on finding things their tech missed. While they do a little work in the SIEM, they spend most of their time building and running custom scripts to find threats their security products aren't alerting on.

Lastly, there are a couple of groups helping to make all of the underlying tech runs. Intelligence analysts make sure that the intel feeding the technology is up to date, ensure it's not burying shift analysts in useless alerts and — when serious threats arise — add color and context so that management understands the risks they're facing. Finally, you'll see engineers whose job is to build software that makes their security products talk to each other. This helps streamline their processes and automate data gathering as best as they can. For lack of a better term at this organization, they call themselves SOC plumbers.

The CISO in the advanced SOC is comfortable with her security operation and periodically brings in third parties to run red team exercises to ensure the SOC is performing as she'd expect.

4. The learning SOC

Like the advanced SOC, this organization has invested an enormous amount of time and money in automation and analytics. They're focused on ensuring that humans are doing the security work that only humans can do. Everything else is handled by software.

To that end, they've tied their security technologies together with an orchestration framework and pulled in resources from IT to help automate investigation and remediation. As a metrics-driven organization, they watch closely what the ratios are between false positives and true positives, how long it takes to triage and investigate and how much value they're getting out of their security investments based on usage. These metrics drive a constant stream of change back into the infrastructure because the tuning is never done. A note of caution here: just because you have metrics doesn't mean you're operating at this level. They're a necessary but not sufficient condition.

Every time the CISO brings in a red team (he rotates between three vendors) he reviews the metrics to ensure time-to-detect, time-to-respond and the overall accuracy that's coming out of his SOC is improving. There's still no guarantee his organization's "secure," but he feels prepared to respond should anyone get in.

Picking the flavor that's right for you

What SOC is right for you? Perhaps it's one of the examples above. Or, maybe it's something in between. Only you can determine what's right for your organization … but maybe we can help. We've found that the best way to figure out how much "security" you need to put in place is by looking at things through the lens of risk. And specifically, through a framework. It probably doesn't matter which one, but starting with the end in mind is better than going YOLO.

I know. It sounds kinda boring. It would be a lot more fun to go buy and implement a bunch of whizz-bang security tech. We see this a lot. But we also see these organizations paying a price in the end. A few years down the road their whizz-bang security tools are gathering dust and their people are overwhelmed with useless alerts.

If you're willing to take this more step-by-step approach, we recommend NIST's Cybersecurity Framework. It's certainly not the only one you can use, but it breaks down security practices into five simple functions: identify, protect, detect, respond, and recover. It also encompasses a whole lot more than what goes into a SOC, which makes it even more useful. That said, if you're focused on SOC operations, you'll find your best guidance within detect and respond with a few relevant nuggets in identify.

We'll be providing a lot more guidance about this framework on the EXE blog soon, but for now, the important thing to know is that your level of "rigor and sophistication" doesn't need to be at level 4 across the board. It's more like building out your D&D character. You're essentially allocating a limited set of points across charisma, agility, and strength.

Adding it all up

After you've determined the kind of risks you want to manage and mitigate, you'll have a better notion of the kind of SOC you need to build. Below, we've outlined rough estimates for purchasing technology and staffing the team. Because technology[1] costs can vary significantly based on the size of the organization, we're imagining an organization with about 5,000 employees. Bear in mind that at larger organizations, the costs of technology can increase dramatically.

[1] We're focusing on SOC-specific tools, not the bread-and-butter security investments organizations make for things like basic firewalls, identity & access management, patch management, vulnerability management, and the like.

Sample costs for SOC-related tools, staffing and implementation

Based on an organization of 5,000 employees

	Basic SOC	Intermediate SOC	Advanced SOC	Learning SOC
General time estimate	months	months+	quarters	1 to 4 years
Annual cost of tools ($millions)				
Log mgmt/correlation	0.25	0.25	0.30	0.50
Detection	negligible	negligible	0.10	0.20
Investigation and response	-	0.10	0.40	0.50
Intel feeds	-	negligible	0.10	0.20
Workflow/orchestration	-	-	0.20	0.30
Intel management	-	-	-	0.20
Annual cost of personnel ($ millions fully loaded at 1.3x, Washington, DC metro area)				
Core 12-person 24x7 SOC	1.17	1.17	1.17	1.17
Senior/escalation support		0.86	0.86	0.86
Hunt team + manager			0.86	0.86
Intel analysts + manager			0.60	0.60
SOC plumbers			0.31	0.31
Dedicated engineering				0.55
Annual total ($M)	**1.42**	**2.38**	**4.90**	**6.25**
One-Time cost of implementation ($ million)				
Approximate costs ($M)	**0.10**	**0.25**	**0.40**	**0.75**

That's a wrap

Understanding the true costs of building and operating a SOC has more to do with the capability you'd like to field than the people you need to hire to run 24x7. Hopefully, this post has helped you estimate a little better what kind of SOC you'd like to build and how much that might cost. And look, if you're sitting here thinking "oh man, this isn't the kind of money I want to be spending … security's not a core part of my business, and there's no way we're going to become experts at it," well, a great many people end up at that same conclusion. In that case, it might be worth considering an as-a-service model for security operations.

I'll leave you with a parting thought. If you do decide that building your own SOC capability is a bridge too far … consider when you're outsourcing what exactly your provider is bringing to the table. Is it a basic SOC? An advanced one? Just the hunting use case? There are infinite ways in which these capabilities can be carved up, and the better you understand what capabilities you need, the better equipped you'll be to build them or buy them.

Visit the EXE blog for more articles like this.

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