# A CISO's Guide to Defender Alignment

A mature cybersecurity program is not necessarily an effective one. And while many companies conflate maturity with efficacy, the CISO knows that when it comes to information security, there is a significant difference between the two.

Most of the time, maturity means there are systematic processes in place that can be activated in a reliable and repeatable manner if a threat occurs. In other words, a mature security program has a well-established methodology that ticks all the proverbial boxes and can easily pass a compliance audit. In contrast, efficacy means having an agile, adaptable, and creative operation where teams possess the real-world knowledge and resources to detect and prevent threats on a practical level.

So, for many CISOs contemplating their roles and responsibilities within the organization — as well as the capabilities of their security operations center (SOC) and the complex cyberthreats that companies face — a few questions might come to mind.

## First: Are we informed?

- Does my SOC have a strong foundation?
- Have I equipped my team with the tools, processes, and capabilities to effectively deal with current threat actors and techniques targeting my industry?
- Does everyone on the team understand their roles in the event of an incident?

## Second: Are we ready?

- Does my team understand the unique inner workings of our business, and have the relationships with other teams, departments, and stakeholders, to the degree that they can mount a robust defense?
- Have my team and I defined what we own — and conversely, what we don't own — and are our colleagues sufficiently aware of this?
- Have we prioritized the data, systems, and users that need protection, and identified security and control factors that will deliver as required?
- Do we all understand the most critical use cases that could impact our business?

### Third: Can we respond?

- Have we implemented the right corporate policies and documented the appropriate actions to address incidents in a rapid and rigorous way?
- Do we have established communication and escalation paths across the business and the senior leadership team?
- Have best practices and processes been defined to remediate the weaknesses that allowed the threat in the first place, and is this tracked outside of IT?
- These questions underline why CISOs today must be fundamentally focused not just on adversary alignment, but also on defender alignment.

## Defining defender alignment

Anticipating adversary behavior is a tenet that most information security leaders adhere to. They are well accustomed to structuring their processes, protocols, and strategies based on the potential actions of an attacker. They also coordinate their security information and event management (SIEM) systems and security operations accordingly. Taken as a whole, this could be considered "adversary alignment".

**So what, then, is defender alignment?**

At its core, defender alignment involves looking at the behaviors and best practices that security analysts, engineers, and operators should be implementing in their daily work, then enabling them in a conducive and supportive way. It's about determining what defenders need to do and helping them do it as consistently, intuitively, and repeatedly as possible.

Defender alignment also involves the broader organization. Companies need defender-aligned processes and a culture of risk awareness where everyone does their part to reduce the attack surface.

In some ways, cyberdefense resembles self defense. It isn't enough to know the moves in a safe, supportive dojo if you don't know how to execute them in a potentially critical real-life situation. The right actions need to be committed to muscle memory, so that when faced with an attack, you know exactly what to do without having to think about it. But you also have to be flexible, agile, and adaptive enough to neutralize novel threats preemptively, because if you're only reacting, you're already too late. And, like self defense, this level of expertise can only come about with frequent training so that it becomes second nature.

Ultimately, being defender aligned means understanding the most useful and effective defender behaviors, removing obstacles in the organization that block these behaviors, and ensuring there are strategies and systems in place that set up defenders for success.

## Harnessing the power of TDIR

Organizations have to be able to identify, inspect, and circumvent potential security issues in order to consider themselves adversary and defender aligned. Collectively, these capabilities are often referred to as "threat detection, investigation, and response" (TDIR).

But just because security operations teams have implemented tools and rules related to TDIR, it doesn't necessarily mean their security strategy is mature or effective. Often, organizations neglect to define TDIR in a coherent, consistent, and contextually relevant way, and this can lead to processes that are disjointed or contingent on legacy technologies that don't support TDIR best practices. For instance, old alerts for adversary behavior may not map to new attack tactics, techniques, and procedures (TTPs).

When this is the case, aligning to best practices can be complicated for defenders. That's because the most effective defender behaviors require insight, intuition, and flexibility — but trying to be flexible within a rigid system can cause things to break and weaken the organization's overall security posture.

It's therefore important for the CISO to take stock of the capabilities, processes, and knowledge their security operation lacks, and then take action to close those gaps. A good SIEM platform can help achieve some of this, as the SIEM forms a foundation for sophisticated TDIR — though the CISO needs to select a solution that delivers the same intelligence, adaptability, and dynamism they expect from their security operations team. From there, they need to lead their team in embracing and embedding the principles of defender alignment.

Here are three strategies that can help the CISO introduce the principles of defender alignment to security operations and organizations.

### Stage 1: Enabling defenders with full awareness and context

To be defender aligned means that at the most fundamental level, defenders need to be able to articulate what their organization does and why it exists:

- If the organization is a business, how does it generate revenue?
- How does it fulfill its critical mission and objectives? Are these understood, agreed upon, and upheld by all stakeholders?
- What does sustained success in security look like?

Defenders struggle to answer such essential questions surprisingly often. Generally, that is because there is too wide a gap between their narrow, day-to-day tasks and the organization's broader goals. It is the CISO's job to ensure they can confidently answer those questions and close the gaps. After that, the teams can probe deeper:

- At the infrastructure level, what data, systems, and capabilities enable and support these business or organizational priorities?
- Where do these reside? How does the data flow? What are the potential vulnerabilities? And how can they be secured?
- Who are the most critical or at-risk users? What users, if compromised, present the greatest risk to the organization?

To that end, comprehensive visibility is a crucial baseline for a defender-aligned security team. That entails having legitimate on-premises and cloud topologies, schematics, and architecture diagrams that allow analysts to see how everything is laid out and how an attacker could infiltrate and take over. It also entails having clear escalation points across teams in the event of an occurrence. It is a simple but powerful principle: you can't defend what you can't see.

Here is a helpful question for CISOs and defenders to ask themselves: How much time do I waste trying to find the information I need to do my job or answer critical questions? If the current processes feel cumbersome, that could signal a need to improve visibility.

## Stage 2: Ensuring defenders have the right information and analytics

Once the first stage is complete, analysts will understand the context surrounding and supporting their role, which is key. It's not about training them to execute on their job description; it's about enabling them to see how that job connects to every aspect of the business.

It is also essential to foster an environment of continuous learning and growth. No one walks into a security operations position knowing as much about packet analysis, databases, cloud security, and directory authentication as an experienced member. Ongoing development of skills and knowledge lays the groundwork for true defender alignment.

Next, ensure that analysts collect and analyze the data relevant to this business complexity and business intelligence. When defenders understand what the critical data is, who their critical users are, and where they reside, they can onboard and analyze the correct use cases in their SIEM solution and better prepare to anticipate and intercept adversaries.

Collecting the right data for the right purposes in the right context can also help reduce the risk or impact of a cyberattack. Analysts can recognize adversary tactics and techniques most commonly associated with data breaches, such as compromised credentials and lateral movement within the environment. They can also maintain open lines of communication with development teams and provide crucial insight when new attacks, patches, or exploits become public.

Here is another important consideration for CISOs aiming to strengthen and streamline TDIR: It might be beneficial for them and the SOC to exercise a degree of oversight or ownership for certain assets traditionally controlled by the IT department and CIO. Certainly they shouldn't be overburdened with responsibilities, nor should they overstep their boundaries — especially when they should be able to obtain asset lists from a CFO or a summary of systems and architecture from a CIO easily enough — but having immediate decision-making authority over certain types of infrastructure can mean the difference between an attempted intrusion and a breach.

It's common in organizations for the core IT team, rather than security operations, to manage the log sources necessary for onboarding use cases into the SIEM, creating silos that impede TDIR. The CIO's sole oversight of system administration and network management may also create barriers to incident response. And change controls often do not include cybersecurity teams as informed participants. As a result, colleagues that should work together end up contending with each other over administrative processes rather than focusing on the adversary.

While it may be excessive for the CISO to share in infrastructure management above the software application layer, having an unobstructed view and unimpeded access to core systems and hardware can provide significant value to the organization's overall security posture. So too can having experts on the security operations team that can support IT in enhancing security and delivering threat intelligence — for instance, dedicated SOC engineers, and intrusion detection and automation content creators.

By rethinking the structure around IT and security operations teams, ensuring they "organize to operationalize", and encouraging evolution in the CIO and CISO roles, CISOs and defenders can move with agility. And they can focus their attention on the different aspects of the CIA triad — confidentiality, integrity, and availability — as needed.

### Stage 3: Empowering defenders to take a proactive — and corrective — approach

When the CISO has a defender-aligned SIEM and security operations function, they can expand the capabilities of their defense even further.

The possibilities are endless. Beyond the context of typical TDIR, there are log sources that can be monitored proactively to prevent and remediate problems before a threat actor can ever take advantage of them. Examples include misconfigurations, device vulnerabilities, and lapses in compliance. Monitoring can also extend to a wider range of use cases and identity and directory services context.

But arguably, it's even more important to have the ability, agility, and initiative to implement security improvements after a threat has exposed weaknesses. Too often, organizations address the short-term problem and then return to the status quo, rather than looking at strategies to prevent such issues long term. This could mean introducing new intrusion logic, configuration changes, security patches, and more robust processes. Remember — if the previous system came under threat, then it wasn't doing its job.

Superior visibility also supports the practice of threat hunting, where the SOC has the dedicated talent, automated SIEM capabilities, and intelligent alerts necessary to comprehensively search for anomalous behavior within the network. Here, defender alignment coincides with the related methodology of adversary alignment: if the best defense is a good offense, then a defender-aligned SOC will give teams the context, tools, skills, and strategies to attack before they are attacked.

By balancing all sides of the equation — detection, response, and prevention — and identifying issues as soon as possible, defenders can proactively reduce the cyberattack surface.

## Cultivating a collaborative defender ecosystem

In building more rigorous, robust, and defender-aligned security operations, CISOs can turn to their own internal and external collaborators for support. Here are some examples:

Cybersecurity peers and analysts: Talk to other IT security leaders to share knowledge and best practices around designing and aligning security operations and your SIEM to defender behavior.

Executive colleagues: Help other members of the C-suite understand what security operations can and cannot do with its current capabilities and communicate tool coverage or visibility gaps — along with how to remediate them.

A framework such as MITRE D3FEND™ is useful for this. At the very least, it can help to visualize the organization's security strengths and weaknesses for executive leadership.

Vendors and partners: Third-party tools allow the organization to optimize its TDIR processes and protect data with pre-built capabilities, rather than wasting developer resources.

It is invaluable to free up resources like this, so CISOs should treat these relationships seriously and recognize their trusted cybersecurity vendors as an extension of the team.

## Defender alignment in summary

In conclusion, here is a helpful line of investigation for considering defender alignment:

1. Does the cybersecurity team understand the organization and the major business drivers that support and define the overall team goals and mission?
2. Do they understand their industry and what common attacks look like — such as those seen in recent media coverage and intelligence reports?
3. Does security operations have the people, processes, and technologies necessary to address problems and anomalies without changing their behaviors?
4. Can the team prevent, detect, identify, investigate, and remediate issues in their environment without re-engineering how they work?

If so, then the pieces are in place for modern, proactive security operations, and the CISO can take pride in having created an organization that's defender aligned.



## About Exabeam

Exabeam is a global cybersecurity leader that created the New-Scale SIEM™ for advancing security operations. We Detect the Undetectable™ by understanding normal behavior, even as normal keeps changing – giving security operations teams a holistic view of incidents for faster, more complete response.

## Learn more about Exabeam today

Get a Demo Now →