Your First 90 Days as CISO -

9 Steps to Success

Cynet

Congratulations!

You're the Chief Information Security Officer for your organization. What you do in the first 90 days will lay the foundation of your success, or failure. It is easy to choose wrongly from the list of competing priorities and regardless of the organization, there will be emergencies that you will need to handle.

Having clearly defined steps laid out for you can help you seize the opportunity and put into place a cyber security capability that will enable the success and growth of the organization that has trusted you with the CISO role. In the contemporary business environment, a well-run cyber security program will enhance the earning power of the organization.

The following steps will also allow you to take advantage of the willingness of the business to undergo a digital transformation, taking full advantage of how digital technology can both accelerate a business plan and reduce the cost of running the business. You'll have a lot of research and questions up front, so roll up those sleeves and get ready to dig in!

Weeks 1-3

Step 1: Understand Business Risk

Put aside worries about technology for a moment. Spend your first two weeks getting to know the business; how it operates, its strategy for addressing the market and how its goods and services are sold. Spend time with your Chief Operating Officer, and your Chief Technology Officer. Understand how products are developed and brought to market and develop an intimate understanding of the organization's supply chain. Gage their willingness to "move security left" within the development life cycle to reduce costs and increase reliability and security. While it may be difficult to get on their calendar, spend some time with your Chief Legal Counsel. Work with them to understand your existing contractual and legal obligations, as well as how they evaluate the contracts and capabilities of their suppliers and vendors.

If your organization has a Chief Privacy Officer, spend some time with them to understand how your organization meets the needs of current and emerging privacy regulations - otherwise your Chief Legal Counsel is likely the best person to inform you on these matters. If your organization has a Chief Risk Officer, or internal audit function, spend sufficient time with them to understand the risks that your business faces as it operates, and the challenges it has from existing laws and regulations.

Try to arrange a meeting with the members of the Board of Directors' audit committee if a publicly traded organization. If not, a meeting with your Chief Financial Officer will be extremely important to understand the organization's finances and cashflow. Meet with your Chief of Human Resources to understand the employee life cycle and how the organization manages disciplinary issues. Lastly, meet with your Chief Information Officer, and begin to work with this person to lay out the separation of duties and responsibilities that your two organizations will have as the basis of their governance. Get an understanding of the technology stack. This person will be a key partner in your success, and it is essential that you re-assure them that you want to help them succeed too.

Weeks 1-3

Step 1: Understand Business Risk

Questions to ask:

- What is the business strategy?
- Does the business plan to enter new markets or expand on existing ones?
- Who are the business main competitors, and how well do our products sell against them? Why?
- Does the business sell internationally, and if not, is that in the plans?
- Does the business sell to the US government, and if not, is that in the plans?
- Does the business have a digitalization strategy, and if so, has it begun to execute on it?
- Does the business track custom customer requirements? If not, why? If so, how?
- How aggressive is the business in pursuing trademark infringement? Why?
- Has there been a data breach in the last five years? If yes, get details on what happened and how it was handled.
- Other than the pandemic, has the business needed to execute either its disaster recovery plan or business continuity plan? If so, what were the lessons learned, and how much has been done to address them?
- What does the business view as its critical assets, and how are they valued?
- Is the business the custodian of its customer' personal and private information?
- Has there been a formal risk assessment performed, and if so, can you see both the report and the inputs to the report?

When you sit down with your team, spend more time listening than talking.

- Ask them about their understanding of their roles and responsibilities, and how they relate to other teams in the organization.
- Find out from them their perspective on how those relationships are working and what they think can be improved.
- Ask them for their critical assessment of each capability and tool they use in their jobs.
- Ask for both performance and effectiveness metrics.

Be prepared to discuss cyber risk as a quantitative measurement in dollars. In the August 2019 Gartner Blog, Jack Freund said:

> "Boards all want quantitative risk measurement in dollars, like the other areas in the company."

IBM recommends the following approach in their cost of a data breach report.

Weeks 4-5

Step 2: Understand Organizational Processes In The Use of Technology & Begin Developing Your Team

Cyber security depends more on people following well defined processes than on the technology that provides critical controls for your organization. Plan to meet with your team to discuss the various processes that are followed within your organization. Pay particular attention to the incident management and account life cycle management processes, as understanding how both work currently - if at all - will be essential. Look over process documentation and standards that exist, and make note of any documentation and technologies that lack documented standards.

Meet with your peers in Engineering and IT to discuss processes and technology that overlap with your team's scope. Get a good understanding of the Software Development Life Cycle and how engineering projects are managed. Get a good understanding of how inventory is managed through the technical life cycle. Make certain that you understand how each evaluate third party vendors. Ask for documentation and pay careful attention to both gaps in documentation and to lapses in keeping documentation current.

Sit down with each member of your staff and discuss their career goals. Ask them how they think you can help them achieve those goals. Discuss desired training, and what opportunities they've had for training in the past. Take the time to explain to them how cyber security is essentially a problem of time, and discuss opportunities for automation across the organization.

Meet with human resources to learn about career paths that are set up for your team's growth. If this doesn't match the goals of your staff, ask human resources what kind of flexibility they have to redefine those career paths.

Step 3: Build a Strategy

You now have most of the inputs needed to start your own planning. Create a strategy to meet the overarching business strategy, goals, and objectives. Create a strategy to meet your staff's career goals and objectives. Create a strategy to use automation to augment staff. If cyber-risks aren't well considered in the organization's risk assessment, then plan an assessment of the cyber risks facing the organization as one critical gap you need to incorporate into your strategy.

- Within your strategy consider opportunities to automate processes to free your staff to do things that require intelligence and nuance rather than following repetitive processes.
- Consider a modern Extended Detection and Response (XDR) platform to consolidate and bolster threat protection with automated response capabilities.
- Consider a Managed Detection and Response (MDR) service for handling your first line incident management, with a clear escalation path to a lean and focused internal staff.
- If appropriate, consider a cloud hosted Web Application Firewall (WAF) with integrated Content Delivery Network (CDN).
- Consider use of both Static and Dynamic Application Security Testing (SAST and DAST) to automate application code review, with a clear escalation path to a lean and focused internal staff performing threat modeling in partnership with engineering.
- Most of all, move security as far left in the development life cycle as possible to reduce cost as well as increase security and reliability of your applications.
- Encourage the organization to use SaaS solutions wherever possible to allow your team to focus on the security of the information rather than the platform.
- Where you must support an infrastructure, work with your IT department to help them move to a zero-trust architecture (ZTA).

All of these strategic choices on where to outsource and where to insource expertise allows you to focus on building business value.

John Wheeler of Gartner in his 20 for 20: IRM Critical Capabilities and Top 20 Functions/Features provides guidance on what to look for as you automate your risk management and incident response. Five of these are focused on incident response and provide excellent guidance on what to look for in a partnership with an MDR provider:

The Gartner Market Guide Recommends

1. Ensure that the vendor can properly capture incident data to enable forensic analysis.
2. Ensure the vendor can automate incident workflow and reporting.
3. Ensure that the vendor can assist in root cause analysis.
4. Ensure that the vendor can assist in crisis management.
5. Ensure the vendor has a robust investigative case management capacity.

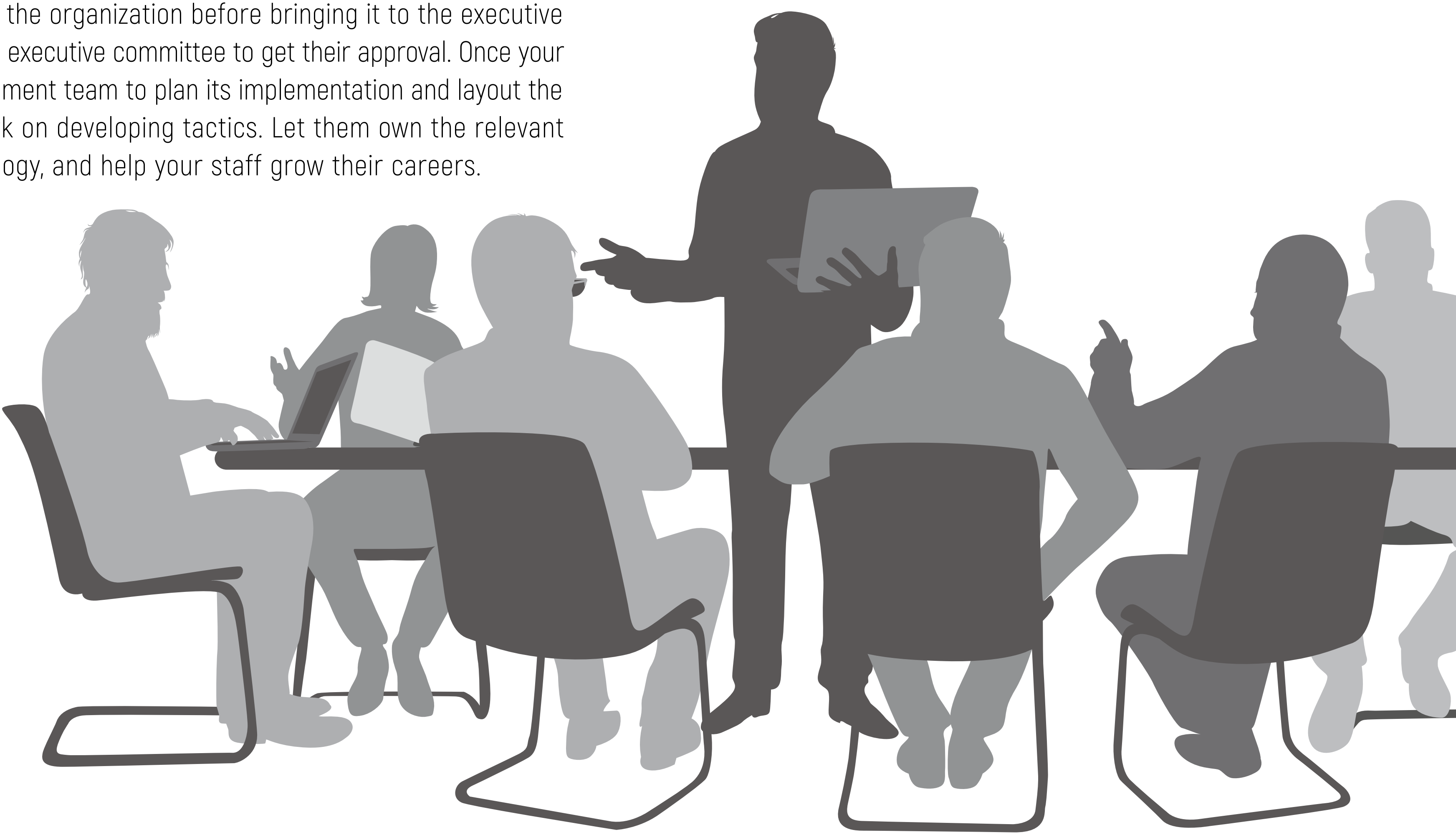
The Gartner Market Guide for Managed Detection and Response Services recommends:

> **"Use MDR services to add remotely delivered modern 24/7 security operations center functions in a turnkey approach when there are no existing internal capabilities, or when the organization needs to accelerate or augment existing capabilities."**

- Assess how the MDR provider's containment approach can integrate with your organization's policies and procedures.
- Ensure the MDR providers technology stack fits well with your existing security controls and IT environment, from on-premises to cloud.
- Use MDR providers that have experience with use cases appropriate to your organization's size, location and industry vertical. Use any unique challenges in your industry vertical to differentiate potential providers.
- Consider managed security service providers that offer MDR services when security technology and device management, and compliance use cases are required. Data residency requirements may also drive consideration of an MSSP over an MDR service provider.

Step 4: Finalize Your Strategy and Plan Implementation

Communicate your strategy and get critical feedback from your peers within the organization before bringing it to the executive committee (and the board). Once you've adjusted your strategy, present it to the executive committee to get their approval. Once your strategy is approved, it is time to work with the organizations' program management team to plan its implementation and layout the tactics that will drive success. This is where you sit with your team and work on developing tactics. Let them own the relevant projects - it will build trust in you, education them in more than just technology, and help your staff grow their careers.



Week 8

○ ○ ○ ○ ○ ○ ○ ● ○ ○ ○ ○

Step 5: Become Agile

Transition your team to using an agile project management style to ensure fast wins of functional elements. Scrum should work well, as you'll have a small, focused team of experts. If your organization is already using sprints, set your sprint cycle to have the same duration as your engineering team. Otherwise, start with a three-week sprint

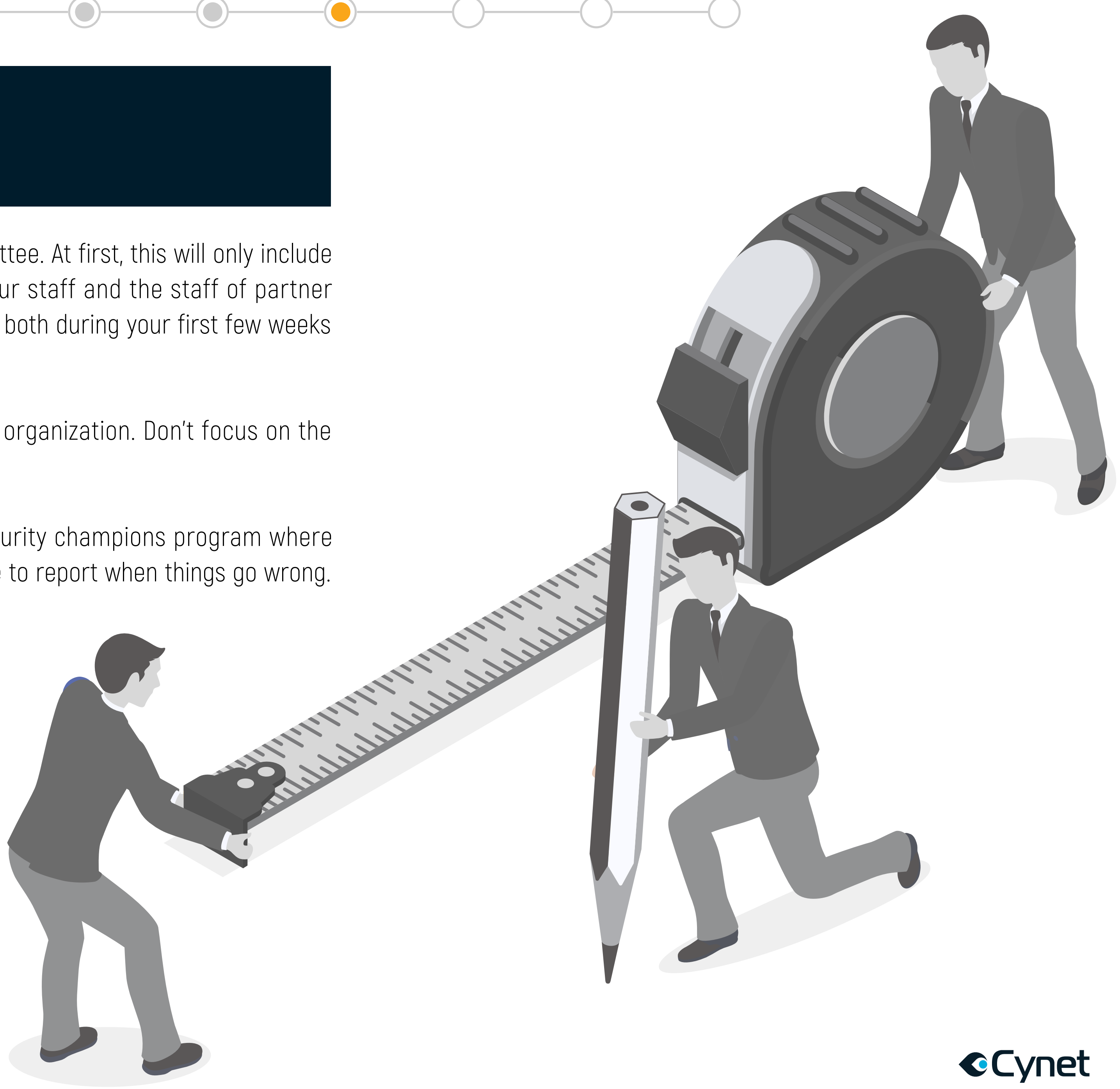
Prioritize projects that bring automation and intelligence into the organization. Consider a modern XDR solution that includes extensive Response Automation that greatly reduces the manual effort and burden of ongoing threat protection, or consider outsourcing this to an MDR provider.

Step 6: Begin Measuring and Reporting

Begin a regular cycle of measuring and reporting back to your peers and to the executive committee. At first, this will only include the progress you've made on the various strategic initiatives. Highlight the efforts for both your staff and the staff of partner organizations such as IT and Engineering. It is important to keep up the good will you earned with both during your first few weeks instead of focusing on the problems and the gaps.

Also begin a regular cycle of educating and communicating about cybersecurity to your entire organization. Don't focus on the problem, but encourage partnership, engagement, and the fact that you all succeed together.

Look for security champions within other parts of your organization. If none exist, create a security champions program where you reward people for their engagement. Never focus on the mistakes but do encourage everyone to report when things go wrong.



Step 7: Time to Pen Test

It is time to get some data on how bad things are. Plan for, schedule, and execute a thorough penetration test or red team exercise of your infrastructure and applications. Look for a penetration testing organization that follows either the PTES or OSSTMM3 methodology for your infrastructure testing and uses the OWASP Testing Framework for each of your applications. If you have an MDR vendor in place, or if you are still doing incident management internally, ensure that your blue team leverages the test to learn how to tune for a real attack instead of trying to stop the assault. This way you get both an accurate assessment of your capabilities and a better tuned defense.

Week 11

Step 8: Get Your ZTA Plan Moving

The first part of the zero-trust framework to implement is enhancing the security of your Identity and Access Management (IAM) through the gradual elimination of passwords wherever possible and the transition to secure multifactor authentication (MFA). Your infrastructure and applications, especially those that are cloud hosted, should be transitioned to using strongly authenticated TLS. Transition to TLS 1.3 everywhere where strongly authenticated TLS is not possible, as TLS 1.3 has added protections to prevent "system in the middle” attacks. "System in the middle” attacks are used by criminals as part of phishing campaigns to steal credentials from organizations, even where multi-factor authentication is used, so encouraging the use of strong authenticated TLS and TLS 1.3 will go a long way to reducing this cyber risk.

Week 12

Step 9: Evaluate SaaS Providers

With the goal of using SaaS solutions wherever possible, it is also necessary to have a good means to evaluate the security of your SaaS vendors. The quality SaaS vendors will be certified as compliant with the CSA CCM, and registered as such in the CSA STAR Alliance, or at least have SOC 2 type 2 to attest to compliance with the CSA CCM and be registered as such in the CSA Star Alliance. For those vendors who have not done this, you will need to develop a program to evaluate their security. Generic SOC 2 Type II reports are not a good indicator of security as the audit will leave out critical controls, but they may be all you have from some vendors. Consider outsourcing SaaS vendor assessment to a vendor that specializes in third party risk management, as long as the vendor can look at more than just the vendors' marketing sites.

Day 90

Now that you've reached your 90-day mark, you have the beginnings of a functioning cyber security team that makes its decisions based on board defensible risk analytics, leverages a Zero Trust framework, and relies on an XDR platform and/or MDR services to drive down the risk of a data breach within your organization. These changes also introduce needed automation that frees up valuable time for your security staff to focus on more strategic initiatives.

You have built an organization that is empowering the growth of the enterprise and partners with your peers within the organization to help them achieve their goals and objectives through integrating security into their own organizations. You measure your successes and failures and use those measurements to drive improvements within your organization. While you still have both strategic and tactical goals ahead of you, selection of good partners to augment capabilities leveraging the skills of an industry will help you do more than achieve your goals and objectives. You'll be helping the business achieve their goals and objectives.

Congratulations, you are a CISO that is well on the way to being the trusted business advisor for cyber risk management!

Learn more about XDR and MDR services:

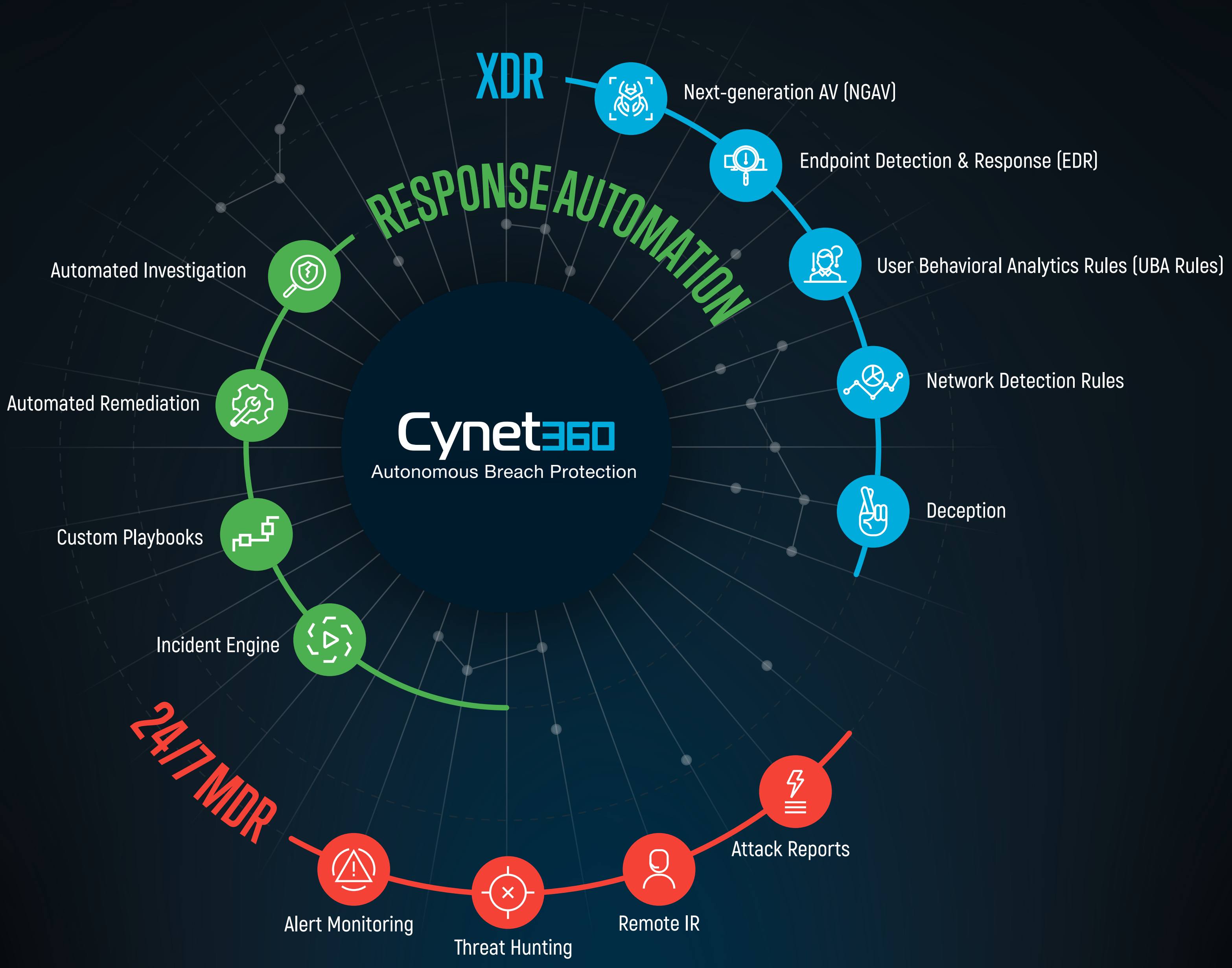
Cynet Website

Contact Us

About Cynet

Cynet enables any organization to put its cybersecurity on autopilot, streamlining and automating their entire security operations while providing enhanced levels of visibility and protection, regardless of the security team's size, skill or resources and without the need for a multi-product security stack. It does so by natively consolidating the essential security technologies needed to provide organizations with comprehensive threat protection into a single, easy-to-use XDR platform; automating the manual process of investigation and remediation across the environment; and providing a 24-7 proactive MDR service - monitoring, investigation, on-demand analysis, incident response and threat hunting - at no additional cost.

Learn More



Cynet