The CISO's Guide:

Incident Management in 2023

CONTENTS

Achieving Cyber Resilience in 2023

The past decade has seen a rise in dominance of new IT models based on the cloud, designed to support digitalization by enabling anytime, anywhere access to information. This has transformed the risk and threat landscape, as malicious actors have found it easier to compromise internal systems, gain access to this sensitive corporate data, and realize financial gain through manipulating this information.

The number of cyber security incidents is only expected to grow in the years to come. These incidents are having growing financial, operational, and reputational costs for organizations, ranging from the loss of customers' personal data, to corporate systems being held hostage in exchange for ransom, not to mention regulatory risks like fines and penalties.

Protecting the business from cyber disruption has long been an executive- and board-level priority.

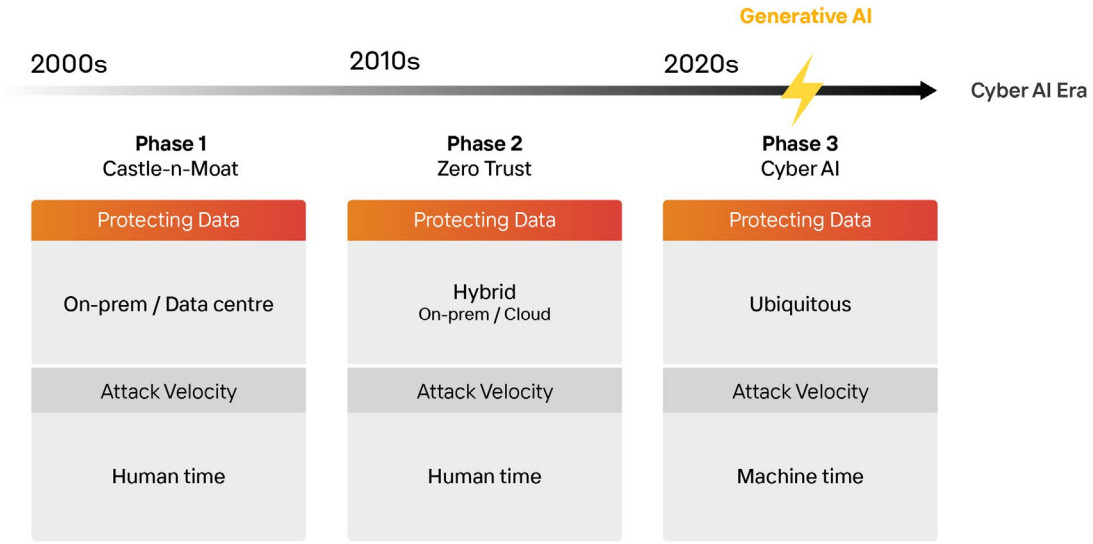
Organizations have spent substantial sums to build out the human skills and technology stack to improve cyber resilience.

Part of this means improving cyber defense – the ability to identify and shut down a threat as close to real time as possible. But as breaches become inev- itable, particularly given the advent of AI-generated or -led attacks, CISOs need to have a continuously updated understanding of their readiness for a cyber-attack.

In other words: if there is a security incident, how ready are my people, processes, and technology, to prevent escalation into a full-blown crisis?

Evolution of the Threat Landscape & Impact of Generative AI

The Phases of Cyber Resilience



The first phase of cyber readiness emerged in a period where sensitive resources were mostly on premise, protected by a security perimeter. Attacks were in 'human-time', meaning they were conceptualized and propagated by people.

The second phase of cyber readiness was defined by the advent of cloud and mobility. In this phase, security practitioners assumed that critical resources could either be on premise or in the cloud, that defenses were focused on categorizing threats (using signature-based techniques), and that frameworks like Zero Trust and Security Services Edge could ensure lateral movement of threats across this expanded attack surface were mitigated.

This was largely effective because as with the first phase of cyber readiness, attacks continued to be in 'human-time'. This meant that a signature-based approach to detection and remediation could also be done in 'human-time'.

However, the techniques deployed in this previous phase can no longer keep up with the realities of the world around us.

The seismic shift that is occurring right now is driven by the rise of Generative AI. What once took humans hours or days to complete can now be done in a matter of minutes by machines – and not just in terms of time to execution, but also in terms of variation of execution.

Machines can dramatically increase the velocity, frequency and diversity of attacks propagated towards businesses. With the introduction of AI-Generated Threats (AGTs), cyber-attacks need to be considered no longer in 'human-time', rather in 'real-time'.

As such, this next phase of cyber readiness will be critically reliant on AI-based approaches to provide a full lifecycle of risk mitigation. Organizations should urgently review and revisit their approach to cyber readiness given the critical risks of both brand and financial exposure.

Generative AI, powered by Large Language Models (LLMs), allows malicious code to morph rapidly thereby evading signature-based attempts to classify and remediate. It creates the concept of "evergreen novel attacks" – brand new attacks that are generated on a continuous basis. Because of the infinite permutations of attacks, signature-based approaches (the approach taken by legacy tools) are constantly out of date. Secondly, the human hours required to review, categorize, and define remediation plans for threats can and will never keep pace with machines.

Darktrace has recently seen novel attack generation take place in a matter of minutes, with generative AI continuously morphing the attack until a vulnerability is exploited.

13 days

average time between an attack being launched to that attack being detected [1]

135% increase

in 'novel social engineering' attacks in 2023 amidst widespread availability of ChatGPT [2]

[1] 13 days mean average of phishing payloads active in the wild between the response of Darktrace/Email compared to the earliest of 16 independent feeds submitted by other email security technologies

[2] Based on the average change in email attacks between January and February 2023 detected across Darktrace/Email deployments with control of outliers

Cyber Resilience: Being Ready for an Attack

The increase in the sophistication and frequency of attacks has led to a shift in mindset for security teams. In an era of machine-attacks, it is no longer enough to assume that detection mechanisms – whether they be firewalls, anti-virus, or even a more advanced XDR – will stop every attack targeting your organization.

For this reason security teams need also to focus on cyber resilience – establishing how prepared an organization is in the face of an emerging incident.

For most organizations, this means some combination of tabletop exercises, IR playbooks, and drills.

Tabletop Exercises

These simulated incident response exercises are often conducted in a conference room setting. The exercise typically involving a group of those responsible for responding to cyber security incidents, such as IT professionals, security analysts, and management. Tabletop exercises test the team's ability to respond to a cyber security incident in a realistic and collaborative environment. The exercise typically follows a scenario based on a real-world incident.

The team is then asked to walk through the steps they would take to respond to the incident. Tabletop exercises can be a valuable tool for improving a team's cyber security readiness.

They can help:

- Identify gaps in your cyber security incident response plan.
- Improve your team's communication and coordination skills.
- Test your team's ability to respond to a cyber security incident in a realistic and collaborative environment.

But security teams need to overcome several challenges in order for these exercises to have a useful, real-world impact. They must decide on a realistic scenario that is based on a plausible incident.

They need to rely on the attendance of the right people to participate in the exercise and provide those participants with enough information to understand the scenario and their role in the exercise. They need to facilitate the exercise in a way that encourages discussion and collaboration, and they should follow up with the participants after the exercise to discuss what went well and what could be improved.

Tabletop exercises are a valuable tool for improving cyber security readiness, but they have some downsides as well:

- They can be unrealistic. Tabletop exercises are often based on hypothetical scenarios that may not be realistic for your organization. This can make it difficult to assess how your team would actually respond to a real incident.
- They can be time-consuming. Tabletop exercises can take a lot of time to plan and execute. This can be a challenge for organizations that are short on resources.
- They can be ineffective. If the tabletop exercise is not well-planned or executed, it can be ineffective in improving cyber security readiness.

Traditional Incident Response Playbooks

Incident response playbooks outline the steps an organization should take to respond to and recover from an attack, and are widely accepted as a necessity to meet compliance requirements.

These, too, suffer from several of drawbacks:

- They are usually outdated, often based on historical data and may not be up-to-date with the latest threats and vulnerabilities.
- They can be inflexible, designed to handle a specific type of incident and may not be flexible enough to handle novel or emerging threats.
- They aren't tailored to an organization's bespoke needs, often designed for general use and not a fit for the bespoke needs of your organization. This can lead to delays in responding to incidents as your team tries to adapt the playbook to your unique environment.
- They are difficult to use, especially for teams that are not familiar with them. This can lead to errors and delays in responding to incidents.

While these playbooks help satisfy auditors and compliance requirements, they aren't often used in the real world, because the reality of an attack never quite aligns with the generic parameters set out in the playbook.

Playbooks are static, while businesses – and the threats that target them – are constantly evolving. This is especially true with the rise of generative AI, which allows attackers to carry out novel attacks on a large scale.

As a result of these limitations, static incident response playbooks can sometimes lead to delays in responding to incidents, which can increase the risk of data loss or other damage.

Security teams often spend considerable time and resources adressing the limitations of static incident response playbooks, regularly reviewing and updating playbooks, or attempting to make them more flexible.

But in the era of AI-Generated Threats (AGTs), a fundamentally different approach is needed to shore up cyber resilience – a defensive method that itself uses AI to ensure readiness for a cyber-attack, and to facilitate quick recovery.

Getting the Timing Right

When it comes to responding to an incident, bad timing wastes resources. If an organization starts recovery efforts too early, it can start acting on events that turn out to be benign, therefore wasting resources. If an organization starts recovery too late, it can end up letting attacks continue so that the issues become more widespread and complex, which in tturn can have greater impacts on the business and require more resources to remedy.

Somewhere in between, there is an optimal stage in which the security teams are not wasting time on benign events, but in which incidents are not allowed to escalate too far.

But this sweet spot is difficult to ascertain, especially when detection tools are prone to false positives, and more sophisticated or novel attacks often fly under the radar of signature-based tools.

Incident response can be optimized by adjusting the timing. By responding to incidents earlier, security teams diminish the amount of recovery needed before the attacks mature. By accelerating the pace of recovery with more effective playbooks, security teams maximize the impact of their efforts. Darktrace HEAL™ uses AI technology in an effort ito optimize the response timing, enabling your team to recover both earlier and faster.

***For illustration purposes only**

How to Be Ready and Recover Quickly in the New Era of Threat

Introducing Darktrace HEAL™

Darktrace HEAL is an AI engine that learns your data to provide an ongoing assessment of both human and system readiness to mitigate an active security incident. HEAL can determine the most effective path to eradicate the threat, recover to an operational state, and adapt your organization's security posture to harden against repeat or similar offenses.

Continuously assess and optimize the incident response readiness of your teams and technology	Address incidents early and recover quickly	Save valuable time with automated reporting and easy collaboration
Is everything going to work when I need it to? Including my people?	*How can I get ahead of an in-progress attack?*	*How can I maximize the time of my limited team?*
• Incident Simulations and Readiness Drills • Readiness Reporting	• Bespoke, AI-Generated Playbooks • Automated Remediation and Recovery Actions	• Automated Incident Reports • Secure Collaboration & Communications • Integrations

Readiness Analysis

HEAL provides continuous testing and assessment of third party integrations, configuration, and scope as well as Darktrace product configuration and scope. This can allow your defenders to answer the question:

"When we're up against an attack and time is of the essence, will everything work when I need it to?"

Darktrace's Self-Learning AI generates an exportable report presenting current results of continuous testing and analysis in the background. These reports assess the configuration and scope of the third-party products to ensure they'll work when needed, providing your security team with visibility into coverage, configuration, and effectiveness of product deployments that affect recovery but aren't necessarily under security's purview. They also assess your other Darktrace products' configuration and coverage.

Reports can be pulled at any time to give an understanding of tech stack readiness, including details of HEAL's configuration, including whether a tool is unresponsive or showing outdated information, or recording errors when trying to complete its normal tasks. You can in turn use these reports to shape simulated incident drills, targeting areas of complexity or where a lack of technology coverage may mean you have less visibility.

Recovery Decision-Engine

Darktrace HEAL creates dynamic, AI-generated playbooks that leverage an evolving understanding of your organization to determine recovery steps that are tailored to the specific incident and the environment where it has occurred. For example, a cloud migration may introduce new architecture that a traditional, static playbook may not consider, but HEAL does.

Since these dynamic playbooks can keep up with changes in both the business and the broader threat landscape, they facilitate more efficient incident response during and after an incident by taking relevant actions and not over-responding.

The AI also prioritizes the order of remediation actions based on factors like the risks of further damage, how much the attack relies on the specific compromised asset as a pivot or entry point, and whether Darktrace RESPOND™ has temporarily contained the asset's unwanted activity.

HEAL's dynamic playbooks apply both in the case of critical incidents needing quick eradication and recovery as well as during day-to-day triage of any emerging incidents. With dynamic playbooks, organizations can supplement what they have to meet their compliance requirements with something offering real-time, practical value.

Simulations

In a modern threat landscape with ever-changing threats and ever-changing organizations, cyber security teams need to have a better understanding of their cyber readiness. AI-simulated incidents offer this insight.

Darktrace HEAL allows defenders to simulate real-world incidents that allow businesses to test their cyber security incident response plans in realistic environments.

HEAL uses its rich real-time knowledge of your environment to give human defenders an understanding how your organization – including both your technology and personnel – would respond to a live incident.

Incident Reporting

When an analyst needs a quick summary of an in-progress incident to inform stakeholders and expedite responding, HEAL can instantly generate a comprehensive incident report. Completed and planned HEAL actions, decisions, and notes will automatically be recorded and combined in an exportable PDF.

These can also be used by third-party forensic teams who need evidence from an impacted company following a critical attack, as well as insurance providers, IT teams, and legal advisors to better understand the impact and consequences of an incident.

Incident reports provide essential information that helps decision-making during important incident response and recovery stages. Report creation is automated and saves writing and formatting time that could be better spent on other critical activities.

Secure Collaboration Channels

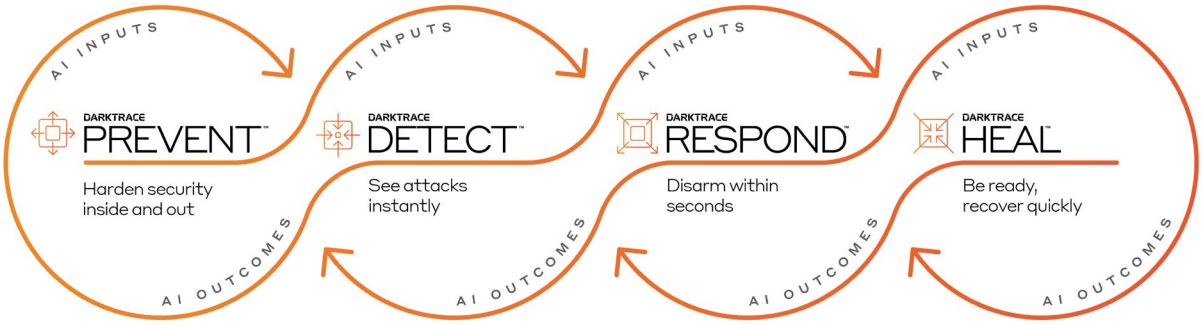
Darktrace HEAL allows easy collaboration and engagement between assigned response roles, with an integrated channel for instant messaging platforms like Microsoft Teams or Slack in the Darktrace Threat Visualizer UI. This helps teams centralize and coordinate teams, enabling users to quickly gather the correct incident responders while swiftly transferring essential information.

A centralized channel provides immense value for security teams who need to quickly and securely contact other important members of the business with private network details. It also helps ensure all stakeholders are aware of a critical incident as it happens, and supports the development of clear communication practices.

A Full Lifecycle Approach

HEAL is just one component of Darktrace's offering which augments defenders at every stage of an attack lifecycle. The power of our industry leading Cyber AI is best understood through the lens of how it allows CISOs and security practitioners to deploy a complete lifecycle approach to cyber resilience. Darktrace provides a comprehensive set of solutions for preventing attacks, detecting them when they do occur, responding rapidly to remediate the impacts of an attack, and healing the environment to ensure a complete return to the prior state.

To zero in on this unique capability, Darktrace is the only provider that can apply Self-Learning AI – that is trained to understand each organization's unique characteristics – to every stage of the lifecycle of cyber resilience. Furthermore, our Cyber AI Engine has the ability to combine insights from a variety of stages of the lifecycle to optimize outcomes.



Darktrace has further leveraged its AI expertise to deliver Cyber AI Analyst™ – which reduces the number of human hours needed to maintain cyber resilience by using AI models to sort through large quantities of outputs, including false positives and alert fatigue. The typical Darktrace customer reports a reduction in triage time by 92%.

Darktrace PREVENT™

Hardens security inside and out by continuously monitoring your attack surface for risks, high-impact vulnerabilities, and external threats. It also looks inside the environment to expose potentially vulnerable attack paths and high value targets.

Darktrace DETECT™

Analyzes thousands of metrics to reveal subtle deviations that may signal an evolving threat – even unknown attacks and AGTs. It distinguishes between malicious and benign behavior, identifying attacks that typically go unnoticed.

Darktrace RESPOND™

Works autonomously to disarm attacks whenever they occur. Customizable to your desired state of autonomy, the offering leverages the intelligence of the Cyber AI Engine to provide decisive action for novel and existing threats no matter where they occur.

Darktrace HEAL™

Enables organizations to restore assets and systems affected by a cyber-attack to a trusted operational state using the assistance of the Cyber AI Engine. The capability automates the remediation and recovery planning, decisions, actions, and communications needed while avoiding unnecessary business disruption.

Thee security industry is rife with point products promising protection for only one of a variety of domains (e.g., endpoint, OT, cloud). Darktrace is committed to providing end-to-end cyber resilience across the entire organization. Our Cyber AI Loop spans across the digital business, as needed in the current era of novel, generative AI-based threats.

Point solutions are still reliant on legacy signature-based approaches to threat detection and mitigation, and are also incapable of integrating data streams from every domain into a single engine to provide the complete lifecycle of cyber resilience.

Darktrace delivers our full lifecycle approach to any domain including network, email, public and private clouds, SaaS applications, endpoints, and operational systems (e.g., OT). Additionally, Darktrace can incorporate data feeds from many of these point solutions (e.g., CrowdStrike, SentinelOne) to further improve the security posture by allowing the Cyber AI Loop to have a complete view of the entire environment.

While Darktrace does provide complete protection across any domain, customers do not have to take an all or nothing approach. Many Darktrace customers start with Email or Network and expand to other domains like Cloud and SaaS over time.

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. Breakthrough innovations from its R&D Centers have resulted in over 135 patent applications filed. Darktrace employs over 2,200 people around the world and protects over 8,400 organizations globally from advanced cyber-threats.

Scan to
LEARN MORE

DARKTRACE
Evolving threats call for evolved thinking™

North America: +1 (415) 229 9100
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
Latin America: +55 11 4949 7696
info@darktrace.com
darktrace.com

© 2023 Darktrace Holdings Limited. All rights reserved. The Darktrace name, logo, and other trademarks used herein are trademarks of Darktrace Holdings Limited.
The names of other companies, products and services are the property of their respective owners.