MARSH

Cyber Catalyst by Marsh

DARKTRACE

Darktrace Enterprise Immune System — Cyber Catalyst 2020 Designation

Darktrace's Enterprise Immune System protects against unpredictable cyber-threats through continuous, on-the-job learning that illuminates subtle threats as they deviate from behavioral norms. Darktrace uses the analogy of the human immune system: while your protective defenses know about historical attacks and act like a protective skin, the Enterprise Immune System complements this by learning about the people, systems, and data in your digital business to detect and respond to the strange and unusual activities that are the hallmarks of an emerging attack.

By learning normal "patterns of life" across diverse digital systems and distributed users, the Enterprise Immune System unifies workforce behavior and drastically reduces time to detection and response across the enterprise – from cloud and collaboration tools, to remote endpoints, IoT, and the corporate network. Without relying on static rules or prior assumptions, the Enterprise Immune System learns "self" for your dynamic workforce so it can autonomously discover, contain, and investigate unknown or fast-moving threats, wherever they emerge in the business.

Given that a wide range of threats will exhibit meaningful deviations if analyzed adaptively and at a sufficiently granular level of detail, the risks the Enterprise Immune System detects are numerous:

- Ransomware (whether known or zero day)
- Insider threat
- SaaS account takeover (e.g. M365/SharePoint, Salesforce, etc.)
- Cloud account takeover (e.g. AWS, Azure, GCP, etc.)
- Cloud workload compromise
- Malware (whether known or zero day)
- Cloud misconfigurations
- IP or data theft
- Crypto jacking
- Supply chain attacks
- IoT compromise

The Enterprise Immune System's AI detections are complemented by Autonomous Response and AI Investigation capabilities delivered by Darktrace Antigena and Cyber AI Analyst, respectively. While Antigena instantly interrupts emerging threats with surgical precision, Cyber AI Analyst automatically triages, interprets, and reports on the full scope of security incidents, reducing 'time to meaning' by up to 92%.

The platform is cloud native and can be delivered via software from the cloud, on premises, or a hybrid of the two. It is agnostic to diverse data sources and ingests, analyzes, and learns autonomously from real-time traffic and data across the business. Once deployed, the Enterprise Immune System immediately begins learning normal patterns of life for every user, device, peer group, and the environment as a whole, delivering meaningful AI visibility and detections just days after installation. The system's learning is continuous and adapts autonomously as your dynamic workforce evolves.

**Product information provided by Darktrace*

For more information about Darktrace Enterprise Immune System, visit https://www.darktrace.com/en/

Why Darktrace Enterprise Immune System is a 2020 Cyber Catalyst Designated Solution

ADDRESSES A TOP 5 CYBER RISK:

The 2020 program encouraged the submission of solutions that targeted the top five cyber risks identified by participating insurers: ransomware, supply chain/vendor management, cloud migration/management, social engineering, and privacy regulation/data management.

Darktrace Enterprise Immune System specifically targets ransomware, but also has wider utility and applicability in addressing other types of cyber risk.

INSURER RATINGS AND COMMENTARY:

Cyber Catalyst participating insurers rated Darktrace Enterprise Immune System highest on the criteria of cyber risk reduction, key performance metrics, flexibility, and differentiation.

In their evaluation, the insurers commented:

- "This is a unique product where machine learning/AI plays a core part in protecting, detecting, and responding to threats. A clear, effective application of technology that follows an increasingly popular approach of 'don't bring humans to a machine fight.'"
- "Unsupervised machine learning that – as opposed to EDR – has no pre-defined 'malicious' rules. The detection of behavior is particularly useful as it does not rely on knowing the current flavor or attackers' preferred malware, but the behavior of the devices it protects. Suggests use cases at all stages of attack lifecycle – a very useful service."
- "An excellent platform from a security engineer's perspective. Provides a material reduction of risk; is accessible to multiple levels of analysts; and provides a force multiplier to the security operations center."

Insurance Policies and Implementation Principle

Organizations that adopt Cyber Catalyst designated solutions may be considered for enhanced terms and conditions on individually negotiated cyber insurance policies with participating insurers.

Those insurers, when considering potential policy enhancements, will expect organizations to deploy Cyber Catalyst designated products and services in accordance with certain "implementation principles" that have been developed by the insurers and product vendors.

The implementation principle for Darktrace Enterprise Immune System is:

- The organization has deployed the solution for at least 1 month and there are plans to remediate critical findings within 2 weeks.

Evaluation Process

Applications for evaluation of cybersecurity products and services were accepted from March 10 to May 15, 2020. More than 90 offerings, spanning a broad range of categories, were submitted.

The insurers evaluated eligible solutions along six criteria:

1. Reduction of cyber risk.
2. Key performance metrics.
3. Viability.
4. Efficiency.
5. Flexibility.
6. Differentiation.

Cyber Catalyst designation was awarded to solutions receiving positive votes from at least six of the eight insurers, which voted independently. Marsh did not participate in the Cyber Catalyst designation decisions.

More Information on Cyber Catalyst

The next Cyber Catalyst program will occur in 2021.

For more information on the 2020 Cyber Catalyst designated solutions, or the 2019 class of Cyber Catalyst solutions, visit the Cyber Catalyst pages on the Marsh website: www.marsh.com/cybercatalyst.

For more information about Marsh's cyber risk management solutions, email cyber.risk@marsh.com, visit www.marsh.com, or contact your Marsh representative.

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.