Proof of Value: Antigena Cyber AI Response Email Module

Darktrace's Cyber AI Response Module for Email works with Darktrace AI in the network to neutralize malicious emails that other tools miss.

While point solutions in this area work by analyzing a given email in isolation and at a single point in time, correlating it against signatures, blacklists, and pre-definitions of bad, Antigena's Cyber AI Response Module for Email works by learning the normal 'patterns of life' for internal and external address identities in connection with the rest of the Enterprise Immune System. By leveraging its rich understanding of normal activity across email and network traffic, Antigena can neutralize malicious emails that deviate from the normal 'pattern of life' for a given user in relation to their past, their peer group, and the wider organization.

This rich network context allows Antigena to spot and stop sophisticated email-borne threats that would otherwise go unnoticed, from targeted spear phishing campaigns to account hijacks along the supply chain. The solution's autonomous actions range from flattening attachments or stripping suspect links, through to holding emails back entirely if they pose a sufficient risk.

The Cyber AI Response Module for Email also includes a dedicated Email Console, which can be used to investigate threats, create models, and gain better insight into the email hygiene of an organization. This can help the security team implement programs which protect key executives and other likely targets from attack.

The Proof of Value

For customers who've deployed the Enterprise Immune System for at least three months, an Antigena Proof of Value (POV) is available at no cost. The POV deployment is cloud-based, requires minimal configuration, and can be paused or disabled at any time from within your Office 365 environment.

During the POV, you will receive three Executive Summary Reports over the course of 30 days. Each report will cover any hazardous email activity identified by Antigena over the previous week and outline the autonomous actions Antigena would have taken in each scenario. The Antigena models are first run in Passive Mode, where these actions are suggested but not performed. By the second report, the client may choose to run some or all models in Active Mode, where the system is fully autonomous within its defined operating parameters.

POV Timescale
A Joint Commitment: Executive Summary Report Reviews

Schedule	Steps	Darktrace resource	Your company resource
Pre POV	• Provide the necessary Activation information on the Darktrace Customer Portal • Ensure Darktrace Master has network access to Antigena Virtual Cloud	Account Executive (AE), CT	Technical Sponsor
Day 1	• Follow the registration link to begin setup and connect Antigena to your Office 365 instance (5 mins) • Enable Journaling Rules in Office 365 instance (5 mins)	CT	Technical Sponsor
Week 1	• Antigena performs email activity baselining and credential mapping to establish organizational and individual 'patterns of life'	CT	Technical Sponsor
Week 2	• Executive Summary Report Review Meeting • User Interface familiarization (1.5 hour)	CT, AE	Technical Sponsor
	• The client may choose to run some or all models in Active Mode		
Week 3	• Executive Summary Report 2 Review Meeting • User Interface familiarization (1 hour)	CT, AE	Executive Sponsor, Technical Sponsor
	• At this stage, the client may wish to activate some or all models such that the proposed actions are performed.		
Week 4	• Executive Summary Report 3 Review Meeting • User Interface familiarization (1 hour) • Presentation of standard Darktrace Terms and Conditions sheet	CT, AE	Executive Sponsor, Technical Sponsor
	• POV finishes • Schedule overall Executive Summary Report Review (optional) • Commercial next steps agreed • Discussion of implementation - pre-emptive or reactive	CT, AE	Executive Sponsor, Technical Sponsor

Darktrace commits to providing a POV at no cost and without obligation, from installation through to subsequent services and consultancy with our cyber specialists. In addition, each Executive Summary Report is produced exclusively for your organization, detailing specific anomalies that are discovered during the POV. For every Executive Summary Report delivered, a Report Review Meeting or Call is held with your team, helping you understand the results of the POV, and evaluate those findings. In order to get the full value from this commitment, Darktrace requires that the appropriate personnel are involved in each step of the process.

Prerequisites & Requirements:

• Office 365 with Exchange Plan

• Darktrace's Enterprise Immune System deployed for at least three months

• One or more domains that you wish to be protected by Antigena. These domains must be actively sending and receiving real email communications.

• An email address within one of these domains to function as the default login for the setup environment.

• Global Administrative credentials for Office 365.

• Ability for your Darktrace Master appliances and those running the Unified View Component to contact the Antigena cloud endpoint.

Privacy & Legal Considerations

• Email data analyzed by Antigena is already stored within the Office 365 Cloud Environment.

• Your nominated Darktrace Analysts will be able to access only the extracted meta-data.

• Full audit logging of user actions is available in the interface.

• Data is securely deleted if you do not wish to proceed beyond the POV.

• The results of meta data analysis from Antigena is shared with your Darktrace Master appliance in your data center.