Ransomware

Key Benefits

- Self-learning Cyber AI neutralizes emerging ransomware – without relying on rules or threat signatures
- The Enterprise Immune System identifies even novel and highly targeted strains of ransomware
- Antigena autonomously responds in real time – no matter where, when, or how the attack is launched
- Cyber AI Analyst automatically investigates ransomware incidents, pulling together the key information you need to jumpstart remediation

Figure 1: Cyber AI identifies a ransomware attack

$381 million combined ransomware losses in the last year for just 350 firms

Source: Hiscox, 2020

As today's workforce norms and technical innovations are rapidly evolving, ransomware attacks are becoming increasingly sophisticated and widespread.

New ransomware strains are emerging to leverage fileless malware and data exfiltration tactics, while opportunistic attackers are using any change in circumstances to launch more effective campaigns. Conventional security tools, which detect only known cyber-threats using rules and signatures, are blind to evolving strains of ransomware for which such signatures do not exist.

Security teams cannot keep up with these threats using traditional controls alone, especially when they are understaffed or out-of-office. Instead, businesses must employ security technology that can stop ransomware as it emerges, before it can do any damage.

Darktrace Cyber AI Platform: Identifying and Responding to Emerging Ransomware

The Darktrace Cyber AI Platform is distinctly capable of neutralizing advanced ransomware in real time – without relying on any known threat intelligence or signatures. Grounded in unsupervised machine learning and deep learning techniques, Cyber AI learns normal 'patterns of life' for every user and technology in the organization in order to recognize the subtle deviations that point to an emerging threat.

The Enterprise Immune System uses Cyber AI's evolving knowledge of 'self' for your business to shine a light on all cyber-threats, including never-before-seen ransomware that evades all other defensive strategies. A key part of the immune system approach, Cyber AI Analyst automatically investigates every threat, helping you easily identify every device affected and communicate the full scope of a ransomware incident.

Upon flagging a serious attack, Darktrace Antigena – the platform's Autonomous Response technology – contains the malicious activity in seconds, surgically neutralizing attacks while letting normal business operations continue. The technology intelligently adapts to threats as they unfold and provides 24/7 coverage of your entire workforce, when security teams are overwhelmed or simply aren't around.

Machine-speed resilience is critical in minimizing the impact of ransomware, which can often encrypt a company infrastructure in a matter of minutes. The Cyber AI Platform is also uniquely able to correlate patterns across the business, providing unified insight and control when ransomware attacks hit diverse parts of the digital ecosystem: from email or SaaS platforms, to corporate networks or industrial systems.

Antigena Network: Neutralizing Attacks at Machine Speed

When ransomware emerges, Antigena Network is the only solution that can interrupt the attack at machine speed with surgical precision, even if the threat is highly targeted or entirely unknown. It autonomously responds with intelligent, proportionate actions – from severing a connection, to enforcing a normal 'pattern of life' for a specific device. When your security team is overwhelmed or out-of-office, Antigena Network gives you the peace of mind of knowing that your entire business is always protected, 24/7.

Darktrace is the creator of Antigena Autonomous Response technology, which uses Cyber AI's evolving knowledge of the organization to adapt to threats in real time and execute the most appropriate action based on your specific context. Rather than applying a binary block (e.g. completely quarantining the device) as legacy tools would, Antigena acts surgically to stop the attack, ensuring all normal business operations can continue. The technology can also integrate with your existing security investments to enhance your entire security stack, feeding AI-powered insights and actions to firewalls, SIEMs, and other tools.

Interrupting Ryuk Ransomware During a Darktrace Trial

When Ryuk ransomware hit a firm that was trialing Darktrace, the Enterprise Immune System detected it instantly – and revealed how Antigena Network could have stopped it entirely.

First, Cyber AI noted highly unusual admin activity not previously seen on the network. Following the incident, the business traced the initial compromise to a part of their network that Darktrace did not have visibility over during this trial period.

Cyber AI then observed the infamous TrickBot banking trojan being downloaded, after which command and control traffic was seen. While many devices exhibited anomalous behavior, Cyber AI pinpointed one device at the source.

When the Ryuk ransomware was finally deployed, over 200,000 files were encrypted in just 12 hours. During this "noisy" period with many suspicious SMB activities, Cyber AI even more clearly indicated the extent of the attack.

Though the team did not action Darktrace alerts until after encryption, this ransomware attack could have been stopped as soon as the Enterprise Immune System detected the first sign of compromise.

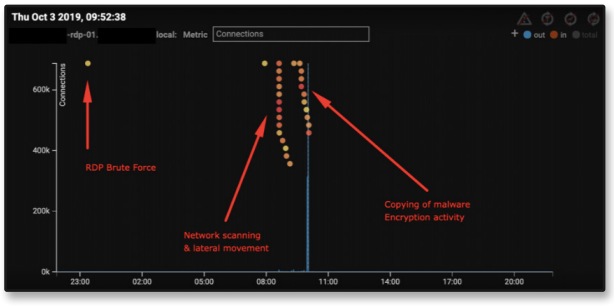

Figure 2: UI graph shows a sample ransomware attack: each dot represents a Darktrace alert.

Autonomous Response in Seconds

Had the firm deployed Antigena Network Autonomous Response technology, the lack of attention given to Darktrace's alerts would not have mattered: whereas four hours passed from the executable download to the first encrypted file, Antigena would have neutralized the threat within seconds. Actions that Antigena would have taken in response to a few of the alerts for this incident include:

- **Unusual Admin SMB Session:** Compromised credentials used to login to server
  - **Antigena action:** This single anomaly prompts no action, but heightens alert level.
- **New Admin Credentials on Client:** The attacker used multiple new admin credentials on the device
  - **Antigena action:** Now with high-confidence evidence of a threat, Antigena would enforce the device's typical login 'patterns of life'; all admins who normally log in to this device can continue to do so, whereas new logins are blocked for one hour.
- **Network Scan:** The attacker scanned the network to identify further victims
  - **Antigena action:** This server has never scanned the network before — only admin devices do this. Antigena would therefore stop the device from scanning the network for two hours.
- **EXE from Rare External Location:** Later-stage payloads downloaded for further infection
  - **Antigena action:** Antigena would still allow the device to conduct normal downloads while blocking downloads from rare locations.

Antigena Email:
Stopping Ransomware at the Source

Many ransomware attacks originate via email platforms, proving that traditional email gateways and legacy detection approaches relying on rules and signatures are not strong enough to catch advanced ransomware every time. What's more, these traditional solutions are limited in scope and fail to connect email activity to related malicious actions throughout the digital infrastructure.

With the power of Cyber AI, Antigena Email builds a deep understanding of the unique human behind the email address. The technology adapts to your dynamic workforce in order to recognize the nuanced shifts in behavior that indicate a ransomware campaign.

It then responds autonomously and proportionately to stop the threat at machine speed and protect your organization from exposure – whether that means holding back the email entirely, locking a link, or converting attachments to a harmless file type.

Should ransomware make it past the inbox and enter the network, Antigena Email is uniquely able to work with the Enterprise Immune System to trace the origin of the attack and prevent lateral spread.

By correlating patterns of activity from the rest of the business with the email environment, Cyber AI can do a root cause analysis to identify the email source and other email activity that may be linked to the incident. Antigena Email will then retrieve any additional threatening emails from other employee inboxes, minimizing the extent of a ransomware attack.

By 2021, there will be a ransomware attack every 11 seconds.

Source: Cybersecurity Ventures

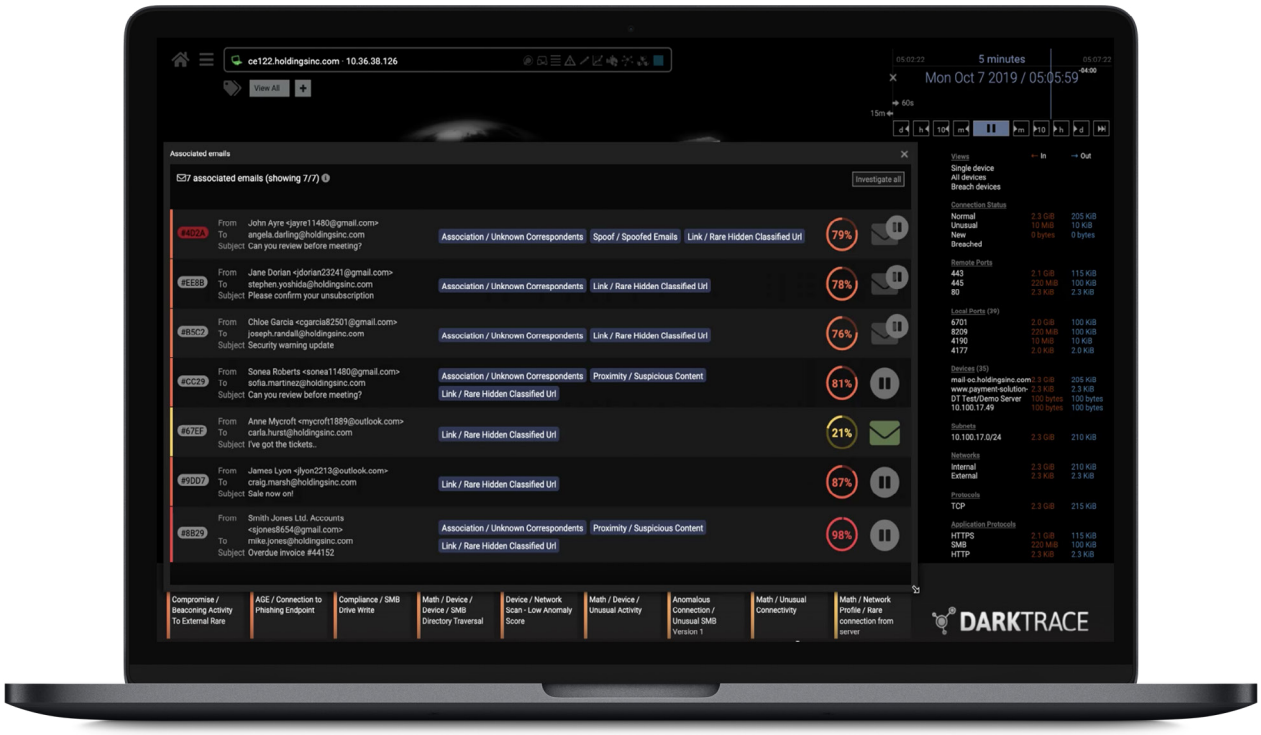

Figure 3: Antigena Email detects a series of emails associated with a ransomware campaign

Malicious Links Neutralized at a City Government

A well-known municipality government in the United States recently fell victim to a targeted email-borne attack that may have been an attempt to deliver ransomware into the organization. Instead, Antigena Email saw the threat as soon as it emerged and ensured no malicious payloads, ransomware or otherwise, could be downloaded.

The threat actor appeared to have access to the government address book, as each well-crafted email was tailored to the intended recipient and delivered alphabetically, from A to Z. While each email appeared harmless, the messages all contained a malicious payload hiding behind a button that was variously disguised as a link to Netflix, Amazon, and other trusted services.

Antigena Email was able to analyze these hidden links in connection with the normal 'patterns of life' of the intended recipients. When the first email came through, Antigena immediately recognized that neither the recipient nor anyone in his peer group or the rest of the city's staff had visited the sender's domain before.

The technology instantly raised a high-confidence alert, and suggested autonomously locking each link as it entered the network.

Because Antigena was deployed in 'Passive Mode,' it couldn't act independently to stop the threat at machine speed – but it did reveal the efficacy of Cyber AI and Autonomous Response. While Antigena spotted and sought to neutralize the campaign at the letter 'A', the security team's legacy tools woke up to the threat at 'R.'

In 'Active Mode', Antigena would have neutralized the attack before it could reach a single user, defending the critical organization from a widespread potential ransomware attack.

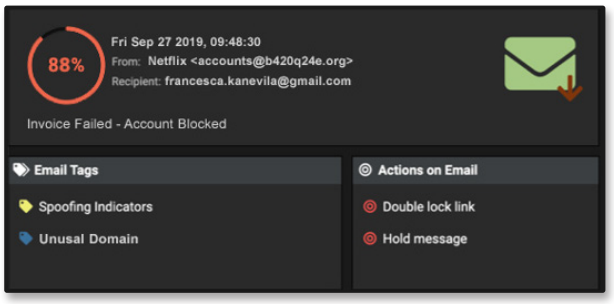

Figure 4: Antigena Email flagged each email as highly anomalous.

Ransomware Traced to Personal Email Account

As ransomware arrived in the inbox at a large telecommunications firm, the Darktrace Cyber AI Platform was able to detect and autonomously contain the attack before it could encrypt a single file.

The initial compromise occurred when an employee accessed his personal email from a corporate smartphone and was tricked into downloading a malicious file containing ransomware. Seconds later, the device began connecting to an external server on the Tor network, and SMB encryption activities began.

Within just nine seconds, Cyber AI raised a prioritized alert signifying the need for immediate investigation of the rare behavior.

As the behavior persisted over the next few seconds, Cyber AI revised its judgment and Antigena responded autonomously.

While the security team had left the office for the weekend, Antigena Network was able to independently stop the attack, interrupting all attempts to write encrypted files to network shares.

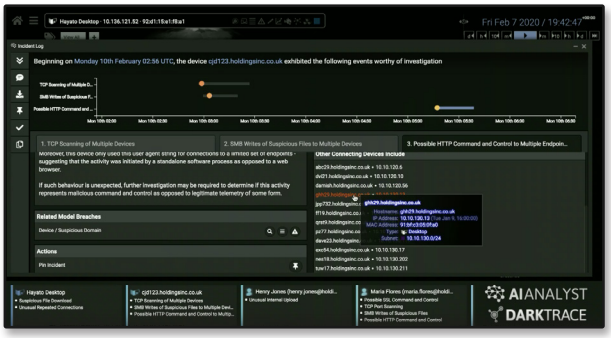

Figure 5: Sample UI shot shows Cyber AI reporting on similar anomalous SMB activities.

Had the company deployed Antigena Email, it is likely that the ransomware never would have been downloaded. No tool is a silver bullet – but even if the ransomware did make it into the network via the inbox, Antigena Email would then correlate the malicious activity detected in the network with the original compromised email. The technology would then retrieve other similarly dangerous emails from across the workforce.

Only with a deep, evolving understanding of your organization's DNA can Antigena Email and the entire Darktrace Cyber AI Platform offer such real-time detection and response to sophisticated ransomware attacks.

The Enterprise Immune System with Cyber AI Analyst: Understanding the Full Scope of a Ransomware Incident

Self-learning Cyber AI allows the Enterprise Immune System to detect the nuanced changes in activity that indicate emerging ransomware – without relying on known threat intelligence. With its bespoke and evolving understanding of normal "patterns of life" across your infrastructure, the Enterprise Immune System illuminates even the most subtle deviations, ensuring your security team knows as soon as a machine-speed attack strikes.

Cyber AI Analyst, a key component of the immune system approach, automatically investigates every anomalous event detected. For ransomware campaigns, it can shine a light on every device affected, the source of infection, and all the contextual information you need to jumpstart response.

Cyber AI Analyst has been known to reduce triage time by 92% and can expertly highlight emerging ransomware as a critical threat that requires human consideration. An AI-generated "Incident Report" will offer an interactive timeline, a concise narrative summary of the campaign, as well as granular data on related device or user behavior.

These reports autonomously update as the threat evolves and are crucial for helping security experts gain situational awareness, as well as for sharing key information with even non-technical stakeholders.

Expertly Analyzing a Dharma Attack

When a targeted Dharma ransomware campaign was launched at a UK company, the Enterprise Immune System was critical for detecting the threat – and revealed Cyber AI Analyst's powerful ability to recognize and report on an emerging attack.

Cyber AI instantly saw the risk when an RDP server received a large number of connections from rare IP addresses. Later investigation revealed the RDP credential had likely been compromised sometime prior to the attack.

The next day, Cyber AI observed the threat actor abusing the SMB version 1 protocol. Then, an unusual external connection to a rare Moroccan IP and a failed SMB session to the IP over a highly unusual port were observed. Two hours later, the threat actor established stronger command and control channels, connecting to rare destinations in India, China, and Italy.

Cyber AI further detected internal reconnaissance when inbound RDP connections began to scan the network and a large volume of data was transferred to an unusual IP in Panama.

Finally, the Dharma payload was executed. Parallel to the encryption activity, the ransomware tried to infect other machines using an administrator credential seen during the internal reconnaissance. As encryption began, IT staff pulled the plug from the RDP server.

Although the team neglected to action Darktrace alerts earlier, Cyber AI was still able to recognize every step of this advanced attack, allowing the team to effectively respond and prevent further damage.

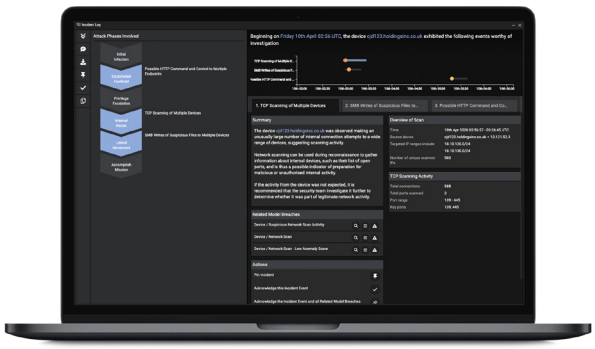

Figure 6: Sample UI shot shows Cyber AI Analyst reporting on a ransomware attack.

The Enterprise Immune System detected every step of this campaign based on abnormal behavior in the context of this company – without depending on matching threat signatures.

When it comes to an attack like this one, carried out over a long period of time with disparate indicators of malicious activity, Cyber AI Analyst is critical for clearly showing the nature and extent of the threat.

With a Cyber AI Analyst Incident Report, the team could easily parse through both a high-level summary of the ransomware attack, and granular details of every stage of the incident.

The Industrial Immune System: Defending Operational Systems from Ransomware

When it comes to defending against ransomware, the Industrial Immune System is the most powerful solution for modern operational environment security. Especially in the face of threats like the EKANS ransomware, which is the first known ransomware to target ICS-specific machinery, it is vital to leverage security tools that can continuously adapt to OT environments and defend these systems against even zero-day attacks.

Many ransomware campaigns also target industrial environments through vulnerabilities in IT infrastructure. Indirect compromise poses an additional threat, as OT systems may become collateral damage during IT-focused attacks. Given the potential harm to critical infrastructure, the need for a security technology that can correlate patterns across disparate infrastructure is increasingly urgent.

Self-learning AI allows the Industrial Immune System to clearly identify threats even as advanced as novel ransomware. The technology can learn normal 'patterns of life' for radically different technologies and deployment types, from decades-old PLCs to distributed sensors and industrial IoT.

Moreover, with its unified view, Cyber AI understands the connection between malicious activity in IT systems and behaviour in OT systems – making it distinctly capable of stopping threats that move between what have traditionally been security siloes.

Finding Ransomware at an Oil Refinery

At an integrated oil refiner and supplier, Darktrace's Industrial Immune System was crucial for stopping a ransomware attack that originated in the corporate network.

Cyber AI identified the first signs of a ransomware infection in a desktop device on the network. As well as writing its own ransom note files, the device was found to be making a series of connections to rare external destinations via an internal proxy server, and then downloading potentially malicious files – activities that Darktrace could detect and correlate based on its granular knowledge of self for the business.

The device proceeded to make a number of SMB directory queries, more activity that Cyber AI recognized as deviant based on its understanding of the particular device.

The Industrial Immune System flagged this activity and highlighted it as likely ransomware, alerting the customer's security team before the infection was able to spread into the OT environments.

With Cyber AI's ability to connect patterns from across diverse infrastructure, the industrial system was defended from this machine-speed attack.

Figure 7: Sample UI shot shows a device infected with ransomware identified by Cyber AI.