Industry Spotlight: Media and Entertainment

DARKTRACE

AT A GLANCE:

- Protects hundreds of media and entertainment organizations globally
- Self-Learning AI technology autonomously detects cyber-threats in real time
- Neutralizes attacks seconds after they emerge
- Autonomous investigations reduce time to triage by up to 92%

Security teams are tasked with defending an increasingly fragmented digital ecosystem from cyber-attacks that are growing in speed, scale, and sophistication. Faced with this hostile cyber-threat landscape, organizations must look to uplift their security teams with autonomous systems that can detect and neutralize emerging threats before the damage is done.

Industry Challenges in a New Era of Cyber-Threats

The volume of sensitive data in use in the media and entertainment industry has exploded in recent years. More data is generated in one hour today than was created over the whole year of 2000, and the figures for streaming and virtual events only continue to rise.

With users sending and receiving data over a vast range of social platforms and devices in order to access media and entertainment services, safeguarding these digital systems with traditional security measures has become untenable. The high-profile nature of many entertainment events means that they continue to draw attention from some of the most dangerous cyber-attackers.

At the same time, organizations are increasingly transitioning to cloud infrastructure and SaaS collaboration platforms in the interest of supporting dynamic and sometimes disparate workforces.

Human IT resources are being stretched to breaking point, and there is a greater need than ever for autonomous systems to expediate the more manual tasks of triage and investigation.

Meanwhile, cyber-attacks are getting faster and more sophisticated, with several high-profile ransomware attacks targeting media and entertainment organizations reported in recent years. Security teams must balance the protection of sensitive data and valuable IP with ensuring business continuity and an optimized user experience.

Being able to interrupt attacks at machine speed is essential to safeguarding sensitive data and intellectual property, while allowing for seamless operations.

> Darktrace AI learns our systems to detect known and unknown attacks. It also produced a very low false positive rate. When it flagged something, we knew it was worth looking at.
>
> / Manager Information Security, Media & Entertainment

Adapting to the Modern Threat Landscape

Proven to protect hundreds of media and entertainment corporations globally, Darktrace's Self-Learning AI is relied on by some of the world's most forward-thinking organizations to fight back against emerging threats in real time – no matter how novel or sophisticated.

Darktrace learns what 'normal' looks like for every user and device in an organization's digital ecosystem. As a Self-Learning AI technology, its evolving understanding of 'normal' is unique for each organization. Darktrace DETECT spots the subtlest indicators of malicious activity as soon as they arise while these threats are autonomously neutralized with Darktrace RESPOND, allowing normal business operations to continue unimpeded.

Darktrace DETECT + RESPOND are operative across cloud, SaaS, IoT, email, endpoint devices, industrial control systems, and the traditional network.

Darktrace is able to autonomously defend organizations' data and digital systems wherever they are located. This capability is complemented by Cyber AI Analyst, which automates the investigation, triaging, and reporting of security incidents, reducing time to meaning by up to 92%.

In today's era of subtle and sophisticated attacks, media and entertainment organizations need AI defenses to stay one step ahead of the latest attacker innovations.

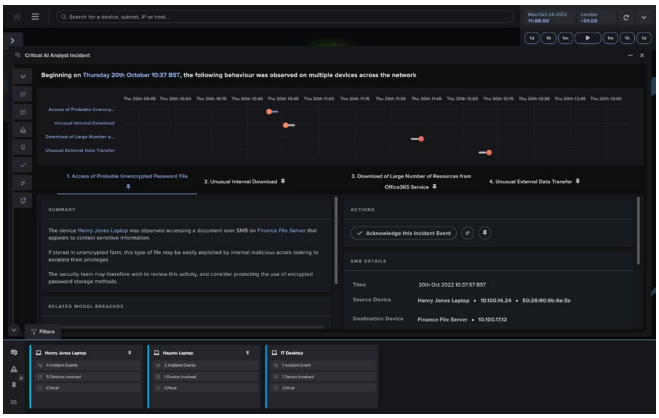

Figure 1: Cyber AI Analyst incident reporting process

Case Study: Topical Phishing Attacks Neutralized

At US television production company Bunim/Murray, Darktrace's Self-Learning AI caught several novel phishing attacks in their earliest stages. The attack started with several emails purporting to deliver corporate COVID-19 updates to the production studio's employees. These emails bore a spoofed corporate address, with the subject line 'COVID-19 Update' followed by the day's date.

While the email appeared legitimate and could easily have persuaded recipient to click on it, Darktrace recognized that this was a spoofed domain and that the emails contained an unusual and malicious link. These subtle signals of attack were enough for Darktrace to prevent the emails from being delivered to recipients' inboxes - neutralizing the threat.

Darktrace's proven ability to stop threats in their tracks has led Bunim/Murray to turn off its legacy email security tools as the team feel safe in their email environment and in the knowledge that AI will autonomously detect and respond to all threat types – wherever they arise.

> All of the stadiums we use for sporting events are protected by Darktrace. We needed a solution that would converge IT and OT together to have a single pane of glass where we can look at all the incidents and alerts related to IT and OT.
>
> / Information Security Manager, Media and Entertainment