



Proactive Intelligence: A Paradigm Shift In Cyber Defense

Published by **David Ratner** on Mar 06, 2024

Traditionally, cybersecurity has been a reactive game: We respond to cyber threats as they arise, analyze the incidents, add pertinent information to “deny lists”, and update stakeholders on “what happened.”

But in today’s threat landscape hackers move too quickly, tactics become too sophisticated and attack vectors are too numerous for security teams to keep up. It’s one of the biggest industry-wide challenges I see right now: taking a

forms of digital risk and cyber threats, which requires a new focus on proactive intelligence and approaches.

It may sound difficult, but change always sounds hard at first. The truth is that we can make a paradigm shift in the way we think about detection, protection, and proactiveness with respect to intelligence and resilience.

I firmly believe that the future of cybersecurity is a *proactive* approach to cybersecurity. Here are the benefits of pivoting.

Early Threat Detection

Understanding attacker infrastructure is the key to not just reactive but true, proactive threat intelligence.

As we've seen from several high-profile hacks of recent years, bad actors often break into a network and lie low for months — even years — as they silently steal data and cause damage fully undetected. As part of this, they need to be constantly communicating with their external infrastructure — command-and-control or C2 — for instructions, data exfiltration, and continuation of the attack.

Even though they may try and hide or obfuscate their communication it's not untraceable. Hackers inevitably leave evidence of their activities which can be used to detect breaches in real-time and allow organizations to proactively address resiliency.

At BlackHat in Las Vegas last year, I kept hearing the buzz phrase “digital exhaust” — the traces left behind like noxious

anomalous patterns and stop the communications, and thus the breach, before the criminals can do any major harm.

In other words, the bad actors might already be in your system, but with the right strategies, you can ensure their digital exhaust tips you off early in the kill chain, before the attack spreads and before significant damage ensues.

Enhanced Security Posture

The evolution of security is becoming less about building higher and bigger walls. It's more about understanding what's going on in real time and ensuring that the systems can be resilient against whatever new threat or risk may occur.

That's even more critical now, as our here-to-stay remote and hybrid work environments dramatically increase an organization's attack surface. Even if employees' devices are secure, the people and **IoT devices** that share the same home network (kids' phones, printers, smart toasters, you name it) may not be protected.

Protect your home network and benefit from enterprise-grade protections with **HYAS Protect At Home** - FREE!

We need to pay attention to where traffic flows and understand what normal versus anomalous communication activities look like before we can respond to the underlying issues.

That's where technologies like **protective DNS** come in.

Protective DNS acts as a first line of defense against malware,

overall security of an organization and is a critical part of any comprehensive security stack. That's why CISA and the NSA now recommend protective DNS as a fundamental element of cybersecurity for every enterprise as part of the Shields Up initiative. And the DoD is making Protective DNS a prerequisite for Maturity Level 3 in its new Cybersecurity Maturity Model Certification (CMMC) standard.

Phishing attacks are becoming more targeted, difficult to detect, and increasingly sophisticated. Protective DNS can help organizations stop phishing attacks before they can do damage. [Learn how.](#)

Cost Efficiency

According to IBM's **Cost of a Data Breach Report 2023**, the global average cost of a data breach in 2023 was \$4.45 million — 15% more than it was in 2020. Cybersecurity Ventures reports that **cybercrime is predicted to cost the world over \$10 trillion by 2025**, and even now is already the world's third-largest economy after the US and China.

Proactive measures like protective DNS can help an enterprise achieve a comprehensive and proactive security stance without significant upfront costs. And while attacks can disrupt business operations, driving overall operational and business resiliency by reducing the likelihood of system outages helps maintain business continuity and protects an organization against all forms of digital risk.

Damage Mitigation

Cybercriminals often aim to steal sensitive data like customers' financial information and intellectual property. If trade secrets are exposed or customers' trust is shattered, many companies may never recover. In fact, it is estimated that **60% of small businesses that are victims of a cyber attack go out of business within six months**. And **if an attack affects a whole supply chain**, we'll feel ripples throughout entire industries — perhaps even entire economies.

Although it's impossible to prevent cybercrime entirely, we can identify breaches and address them before they can be exploited, making ourselves resilient to attacks.

Malware can spread and propagate within a network, infecting devices and capitalizing on vulnerabilities as it goes. But a proactive approach to cybersecurity can spread, too.

Proactive user education and awareness can prevent employees from inadvertently enabling bad actors or falling prey to phishing scams. But ultimately, and inevitably, bad actors will unfortunately always break in. Nevertheless, early and proactive detection of anomalies means quicker response times to malicious behavior and less likelihood of damage, fewer system outages, less time spent recovering from attacks — and more time for innovation. And isn't that the ultimate goal of implementing resiliency and having the confidence to drive business full forward?

*Ready to step up your defensive game? **Learn how HYAS Protect can transform your cybersecurity strategy from reactive to proactive.***