SOLUTION BRIEF

HYAS **PROTECT**

for Digital Forensics and Incident Response (DFIR)

The Situation

Your client has experienced a cyber attack or suspected incident. They've engaged your organization to leverage your managed detection and response services to help them identify the source and root cause of the incident. You're now focused on remediation efforts and are working to ensure that your client's environment is clean and that all vulnerabilities have been eliminated.

As you begin to deploy tools to monitor inbound traffic and identify potential threats that may still be trying to penetrate your client's organization and re-activate the attack, you select an EDR solution, deploy it and start to monitor the network. But how can you definitively determine the threats have been neutralized if you're not actively monitoring the DNS traffic for beaconing communication?

The Ongoing (or Undetected) Threat

Once breached, it is difficult to determine the source and complete scope of an intrusion. The attacker will reside in the network an average of 99 days before it is detected (source: Microsoft). During this time the adversary is likely moving around, expanding their malicious footprint and making it more difficult to identify and isolate their damage.

A Holistic (or Proactive) Approach

Nearly all cyber attacks have one thing in common: a DNS query. Nearly 90% of cyber attacks begin with a phishing attack that leverages a compromised or malicious domain (source: Deloitte.com) and close to 80% still involve a DNS query. (source: Incyber.org)

> "Nearly 90% of cyber attacks begin with a phishing attack that leverages a compromised or malicious domain."

Why are these stats important? Because in order for malware that has been planted to be activated, it has to communicate with the adversary's Command & Control (C2) infrastructure for instructions. EDR solutions, and other tools that monitor inbound traffic, cannot detect this beaconing behavior.

If you are going to deploy a post-incident tool to help ensure that your client's network is clean, a Protective DNS solution is critical. It monitors outbound DNS traffic and looks for beaconing activity from compromised devices that are trying to communicate with C2 infrastructure.

HYAS Protect Protective DNS

HYAS Protect is a cloud-native Protective DNS solution that uses domain-based intelligence and attribution at the DNS layer to preemptively protect enterprises from cyber threats. It combines authoritative knowledge of attacker infrastructure and unrivaled domain-based intelligence to proactively enforce security and block the command and control (C2) communication used by malware, ransomware, phishing, and other cyber attacks.

Key Features

- **Proactive Security:** HYAS Protect identifies and prevents attacks before they happen, independent of protocol, for devices inside and outside the network. It blocks C2 communication used by malware, ransomware, phishing, and supply chain attacks.
- **Detection and Response:** HYAS Protect provides a high-fidelity threat signal to reduce alert fatigue and improve network intelligence. It detects and blocks low-and-slow attacks, supply chain attacks, and other intrusions hiding in the network. In the event of a successful breach, HYAS Protect can help detect the C2 traffic used by the malware and block it.
- **Investigation:** HYAS Protect allows IR teams to perform static analysis and determine the presence of latent or active threats. This can be crucial in understanding the nature of the attack and preventing future incidents.
- **Seamless Integration:** HYAS Protect can be quickly and easily integrated via APIs with existing SIEM, SOAR, firewalls, and endpoint solutions to enhance the value of all current security investments.
- **Visibility:** HYAS Protect provides an essential additional layer for defense in depth strategy. It helps to identify where people are doing things they should not be doing, both for end-users and the engineering environment.

Benefits

- **Proactive Security:** HYAS Protect operates as a cloud-based Protective DNS solution or through API integration with existing security solutions. It takes the most proactive security possible to support the high speed of business.
- **Real-time Threat Intelligence:** HYAS Protect uses authoritative knowledge of attacker infrastructure and unrivaled domain-based intelligence to augment existing security solutions, proactively protect organizations, and mitigate threats in real-time.
- **Customizable Threat Blocking:** New capabilities in HYAS Protect allow deeper customization of threat blocking and reputation analysis. Admins gain options to control undetermined network traffic based on risk tolerance, isolating and handling unclassified queries according to security needs.
- **Ease of Deployment:** HYAS Protect is a cloud-native infrastructure-as-a-service that scales infinitely and deploys in minutes. This modern framework allows organizations to act immediately.

The HYAS DFIR Solution

As a HYAS ONPOINT Partner program partner, HYAS Protect protective DNS is deployed as part of your post-incident monitoring and management services. You will gain:

1. **Increased visibility:** The ability to identify any remaining unseen threats and proactively block network traffic to them.
2. **Client confidence:** You will be able to present reports to your clients that prove adversary communication has been contained.
3. **Improved bottom line:** Your MDR service value will broaden and deepen, increasing the stickiness of your managed services and open additional new revenue streams with a proven-value solution.

> **"A Protective DNS solution that monitors outbound DNS traffic, and looks for beaconing activity from compromised devices that are trying to communicate with C2 infrastructure is critical."**

HYAS DFIR Case Study

Using HYAS Protect for Digital Forensics and Incident Response

A medium-sized financial services firm experienced a sophisticated cyber attack targeting its customer data. The firm's IT team needed an advanced solution to manage the incident and prevent future attacks. They chose HYAS Protect for its unique ability to contribute to the digital forensics and incident response (DFIR) process.

Phishing attacks are becoming more difficult to detect. Phishing attackers are using increasingly sophisticated techniques

Overview of the Incident

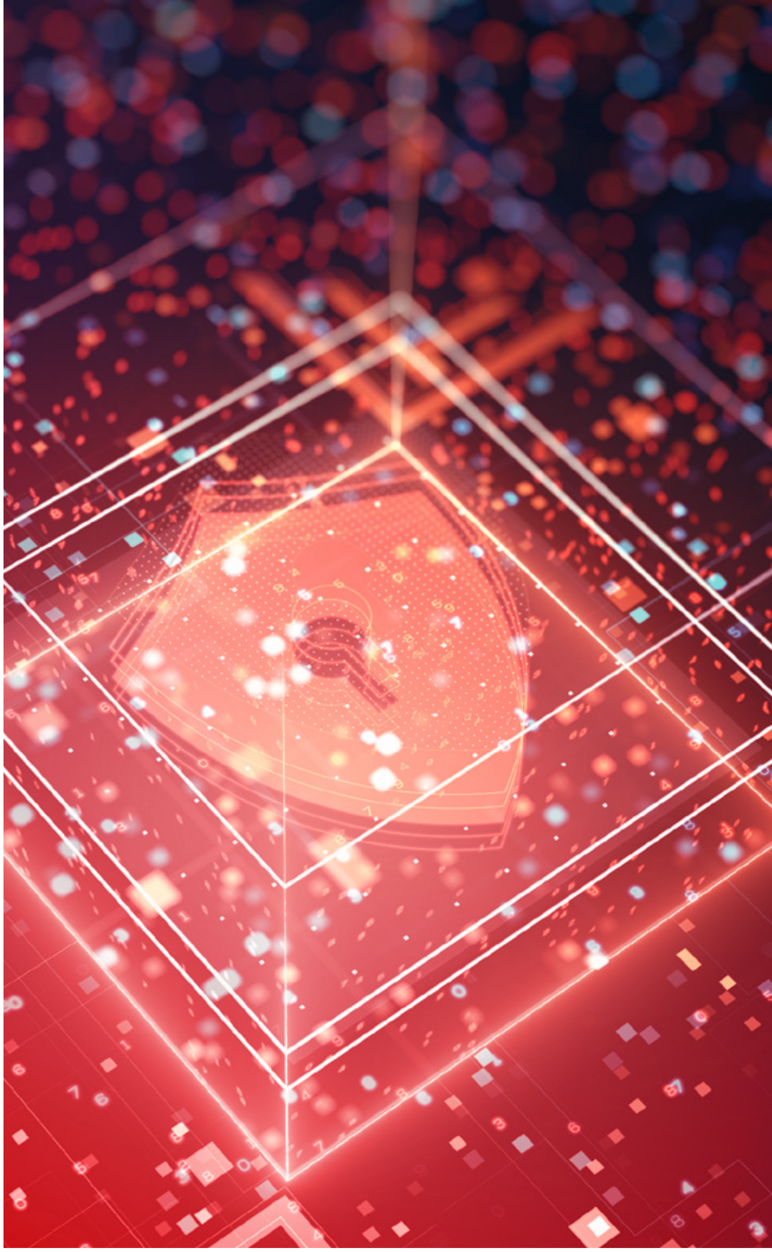
The attack involved a sophisticated phishing scheme leading to a data breach. Sensitive customer information was at risk, and the firm faced potential regulatory penalties and reputation damage.

Implementation of HYAS Protect

The organization's IT team quickly deployed HYAS Protect.

Key steps included:

1. **Initial Assessment:** HYAS Protect quickly analyzed network traffic to identify malicious activities.
2. **Threat Identification:** The solution identified the phishing domains and traced them back to three user devices.
3. **Containment and Mitigation:** HYAS Protect provided actionable intelligence to block the IP addresses and domains related to the attack.



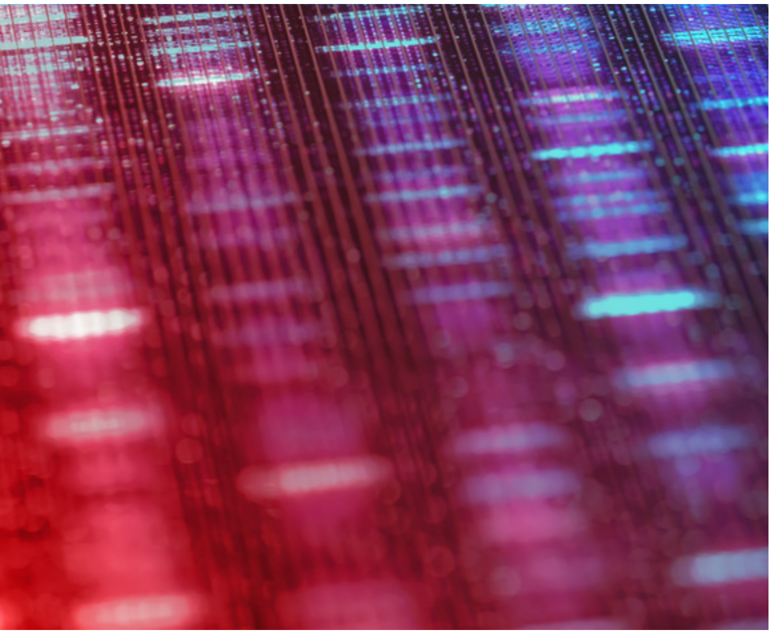
> "They chose HYAS Protect for its unique ability to contribute to the digital forensics and incident response (DFIR) process."

Results and Analysis

Immediate Impact: The attack was contained within hours of deploying HYAS Protect, significantly reducing potential damage.

Long-Term Benefits: The organization developed stronger security protocols based on insights from HYAS Protect.

On-Going Protection: The HYAS solution enabled additional protection against any new threats which could seriously affect corporate reputation, revenue, and employee morale if successful. The organization recognized that a second successful attack could be detrimental to the business.



Lessons Learned and Best Practices

Proactive Monitoring: Continuous monitoring is crucial for early detection of threats at the DNS layer.

Integration with Existing Systems: Seamless integration with existing security infrastructure is key to effective DFIR.

Conclusion

HYAS Protect proved to be an invaluable asset for the financial services firm for managing a critical cyber incident. Its capabilities not only helped to resolve the immediate crisis but also provided the firm with tools and insights to bolster its cybersecurity posture moving forward. This case study serves as a testament to the effectiveness of HYAS Protect in real-world DFIR scenarios.

Future Implications

The client plans to further integrate HYAS Protect into its security strategy, emphasizing prevention and rapid response. The firm is also exploring additional HYAS solutions to enhance its overall cybersecurity framework.

CONTACT US
hyas.com/contact

IDENTIFY AND BLOCK
ATTACKS BEFORE THEY HAPPEN

HYAS PROTECT

HYAS Protect enforces security and blocks command and control (C2) communication used by malware, ransomware, phishing, and supply chain attacks. All the while, it delivers on-demand intelligence to enhance your existing security and IT governance stack.

HYAS

PROTECTING BUSINESSES AND SOLVING INTELLIGENCE PROBLEMS
THROUGH DETECTION OF ADVERSARY INFRASTRUCTURE AND ANOMALOUS COMMUNICATION PATTERNS

HYAS is a world-leading authority on cyber adversary infrastructure and communication to that infrastructure. We help businesses see more, do more, and understand more about the nature of the threats they face in real time. HYAS turns meta-data into actionable threat intelligence, actual adversary visibility, and protective DNS that renders malware inoperable. HYAS's foundational cybersecurity solutions and personalized service provide the confidence and enhanced risk mitigation that today's businesses need to move forward in an ever-changing data environment. Visit for more details.

HYAS.COM