No.70
July 17th 2023

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UN-SPONSORED**

Where's DNS in the XDR Roadmap?

- Whether it's managed from a SIEM, the endpoint itself, or a dedicated XDR platform, endpoint data inevitably features at the heart of first phase XDR implementations.
- As XDR architectures and portfolios evolve to ingest more data and use that data more effectively, security teams and their vendors should consider how DNS detection and response (DNSDR) can enhance XDR – and where to source it from.
- Providing enriched context around malicious domains; DNS tunnelling events; command and control messages; suspicious domains and lookalike domains are among the high value features of an effective integration of DNSDR into XDR.

XDR is an architecture first and foremost…

As threat actors have got better at evading the protection layer in the security stack, attention has shifted to the augmentation of detection and response. Once something suspicious-looking has got past your protections; how do you figure out exactly what it is; how much you should care about it; and what (if anything) you should do about it?

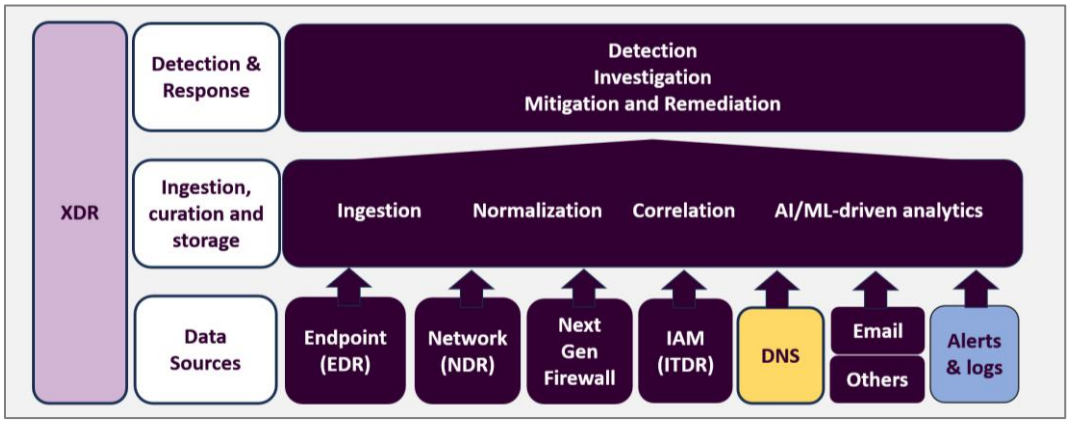
Extended Detection and Response (XDR) is the answer vendors have come up with, most of whom have approached building better solutions from one of two starting points. Security Incident and Event Management (SIEM) vendors are adding better response capabilities to log storage and detection features. Endpoint Protection Platform (EPP) vendors have added response capabilities to compete in the Endpoint Detection and Response (EDR) product category.

There's plenty of debate as to just how helpful the still nascent XDR product category is.

…whether or not it's also a product is up to individual users to decide

There's plenty of debate around how helpful the still-nascent XDR product category is (or isn't) for driving detection and response roadmaps. Palo Alto Networks, a pioneer in driving the XDR product market, recently reported bookings of $1 billion for its Cortex XDR product line. The last six months have seen VMware Carbon Black, Forescout and Cisco join the ranks of vendors launching XDR-branded products (the latter most recently at RSA Conference in April).

Figure 1: XDR is the right architecture - with or without 'XDR'-branded product



Source: HardenStance

There is significant resistance among some users and vendors too. This tends to centre on how amorphous XDR is as a product category, how much it suffers from feature bloat, or the higher than usual risk from vendor lock-in arising from how central – hence powerful – a position an XDR platform occupies in the Security Operations Centre (SOC).

In contrast to some sharply differing views on the merits of XDR as a product, there is widespread agreement that XDR is right as an architecture or framework for detection and response operations. Whether what matters most is what each component of the architecture does and how they all fit together – or whether it necessarily needs an XDR-labelled product at its heart – is for each user organization to decide.

There is widespread agreement that XDR is right as an architecture or framework for security operations.

The goal of XDR is to be driven by data ingested from multiple sources

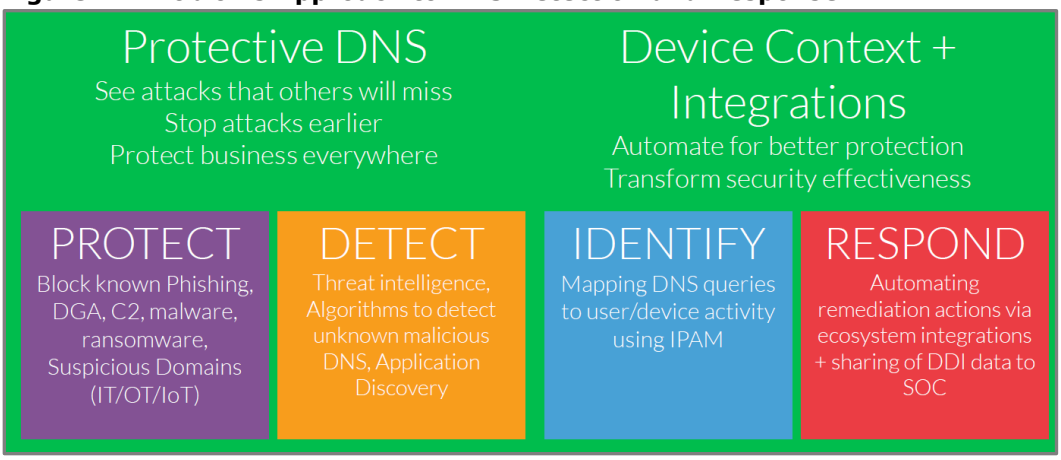
General industry alignment on the value of XDR as an architecture centres on the principle that while the endpoint is the right place to start, greater detection and response efficiency requires ingesting data from as many other sources as possible – on premises, in the data centre or in the cloud. This is depicted in **Figure 1**.

In product terms, that means that as well as from EDR platforms, XDR needs to ingest data - either natively or via third party vendor integrations – from platforms such as Network Detection and Response (NDR), Next Generation Firewalls (NGFWs); Identity Threat Detection and Response (ITDR) and other sources. That data then needs to be normalized and curated with up-to-date threat intelligence and presented to SOC analysts. It's then for them to figure out how a suspicious-looking event happened, what (or who) drove it to happen, and what kind of a risk it represents. Options then need to be provided by which a threat can be mitigated or remediated.

HardenStance was prompted by a recent meeting with DNS solutions vendor, Infoblox, to take a look at where DNS fits in XDR. Why, they asked, are DNS security features and DNS threat intelligence barely featuring – or not featuring at all – in XDR conversations? And isn't it about time that DNS Detection and Response (DNSDR) started featuring more prominently?

Infoblox's view of where DNSDR fits in XDR is summarized in **Figure 2.** Taking into account the ideas shared by Infoblox, the remainder of this Briefing lays out six summary points depicting HardenStance's take on where DNS and DNS security have featured in XDR until now – and where it ought to go from here.

Figure 2: Infoblox's Approach to DNS Detection and Response



Source: Infoblox

1. There's no reason for DNS to feature in the first phases of XDR

Once you recognize that endpoints are easily your most exposed targets, dropping EDR agents onto them and monitoring them is a critical first step in getting started with XDR. Layering in NDR to watch for malicious behaviours that EDR might miss is usually the next priority. Some organizations flip this sequencing around but it's unusual for these two not to feature as priorities one and two in an XDR roadmap. Integrating Next Generation Firewalls (NGFWs) to enhance the detection and response efficacy of NDR is a common Step 3 (although perhaps better thought of as a Step 2.5). Along with ITDR (a new product category that is only now coming to the market) and email detection and response (EMDR), DNSDR starts to become a potential contender for tight integration into XDR after these initial priorities.

2. By driving adoption of Protective DNS (PDNS), leading national cybersecurity agencies are raising the profile of DNS security, including in the XDR context.

Blocking access to malicious domains by declining to resolve them isn't new to cybersecurity. Vendors have offered these solutions going back many years – some called 'DNS Firewalls'; some using a specific method or protocol such as DNS Security Extensions (DNSSEC); others just called 'DNS Security'.

The PDNS service category was launched at scale in 2017 by the UK's National Cyber Security Centre (NCSC). Today, PDNS is supported in their product portfolios by a number of leading specialist DNS vendors like Infoblox and Akamai. It's also supported by a number of network security vendors like Palo Networks, Cisco and Zscaler.

In 2022, the NCSC's PDNS service blocked over 5 million requests for domains associated with ransomware.

PDNS has boosted the profile of DNS security in cybersecurity for two main reasons:

- First, PDNS is a threat-intelligence driven service rather than a traditional, more static, feature or protocol driven approach to DNS security. It has gained significant industry support for the way it addresses the trustworthiness of upstream DNS infrastructure that may be compromised as well as DNS registrations that may be maliciously provisioned.
- Second, several leading national security agencies around the world are heavily promoting PDNS for their public sector organizations as well as advocating its adoption by the private sector. It isn't just the NCSC in the UK. Among others, PDNS is supported by the Cybersecurity and Infrastructure Security Agency (CISA) in the United States and by the Australian Cyber Security Centre (ACSC).

Figure 3 shows the most blocked attributed threats by the NCSC's PDNS service in the UK during 2022. The service also blocked over 5 million requests for domains associated with ransomware. The specific threats blocked, with number of requests blocked shown in brackets, were Conti Ransomware (1,350,986); Petya (641,135); NotPetya (529,442), FiveHands (522,434) and Knot Ransomware (239,864). Notifications were also sent to 56 organisations to warn them about pre-ransomware malware infections.

Figure 3: Most Blocked Attributed Threats by the NCSC's PDNS Service (2022)

Threat Name	Unique Domains	Total Blocks
Cobalt Strike	295	15,414,417
SUNBURST	29	7,109,940
Flubot	109,415	5,880,600
Cryptostealer	42	3109,973

Source: UK's National Cyber Security Centre (NCSC), "Active Cyber Defence – the 6th Year" 2023

3. There are Layers of 'Response' to DNSDR Use Cases
Consistent with the goal of XDR, security teams need to respond to DNS threats, not merely detect and block them. For instance, you can congratulate yourself for blocking outbound communications from a user device to a command and control network. But if the malware is able to bounce domains over time, you are only as safe as how fast your PDNS or other security controls are informed of that new domain by DNS threat intelligence. Moreover, when that same user device connects from a home network, it won't necessarily be protected by enterprise DNS security controls so it may be able to resume beaconing successfully. And what if other devices are also infected but haven't started beaconing yet?

In security operations, responses comprise actions like quarantining and re-imaging devices – ultimately according to an automated playbook. In the DNSDR context, Infoblox defines 'Response' as starting with something as simple as making relevant contextual data available when raising a trouble ticket. For example, when a PDNS platform flags up that a given IP address has tried communicating with a malicious domain, contextual information can automatically be included in the event report. This includes a profile of the user, the specific device and the OS that it's running. The analyst doesn't have to spend time manually tracking down that contextual data for themselves.

Infoblox defines 'Response' as starting with something as simple as making relevant contextual data available when raising a trouble ticket.

4. In terms of DNSDR capabilities, all vendors in the XDR space are not created equal. In this context, it's useful to think in terms of three tiers of vendors:

- **i**. DNS specialists like Infoblox and Akamai occupy the top tier. They provide DNS servers and supporting security features and services, giving them a unique capability to block DNS threats at source rather than in an NGFW or web proxy.

  Infoblox positions its differentiators here as things like the ability to detect and respond to DNS tunneling; command and control messages; suspicious domains that are not yet clearly exhibiting malicious behaviors; and lookalike domains that are used by attackers to attract an organization's user community or employees. With growing adoption of Multi Factor Authentication (MFA) a study by the Infoblox Threat Intelligence Group (TIG) found over 1,600 domains used that contained a combination of corporate and MFA lookalike features since the beginning of 2022. Worldwide targets ranged from large corporations to major banks, software companies, internet service providers, and government entities.

- **ii**. In the middle tier are vendors with a strong pedigree in network security. Most in this second tier range from middling to strong-ish in terms of their DNS security, although some would argue that being able to view DNS data at multiple points in a broader XDR architecture is a differentiator for security teams.

- **iii**. In the bottom tier, vendors whose XDR portfolios are rooted in endpoint security or SIEM platforms tend to range from the middling to the fairly limited when it comes to their own DNS security capabilities.

5. In terms of their ability to leverage DNS or any other threat intel in detection and response operations, all users are not created equal. It's always useful to think in terms of a couple of different layers when it comes to any kind of threat intelligence. In the case of DNS, there's the core threat intel that's delivered via a PDNS platform. Any user organization can benefit from this because the user's own security team doesn't have to manipulate the data (or even look at it). The delivery and application are automated and abstracted from the user organization itself.

However, as was demonstrated once again by HardenStance's recent threat intelligence survey carried out at RSA Conference on "Barriers to Effective Use of Threat Intelligence", many organizations are severely limited as regards the capabilities needed to apply threat intelligence in security operations themselves. Hence, in the case of DNS

threat intel, something like monitoring for and acting on lookalike domains can be very useful for elite security teams but is beyond the capabilities of most teams as of today.

Every useful anecdote or artefact contributes to a picture which enables an analyst to better understand a sequence of events.

6. Planning a review of DNS threats and how to respond to them within a broader XDR framework should be a matter of 'when' rather than 'if'. In the broader context of XDR, DNS is indeed just one more from multiple potential sources of data. As demonstrated, however, it contains a lot of valuable contextual information that can be critical to understanding events and building an organization's detection and response capabilities. Even where they are merely a useful addition rather than critical, every useful anecdote or artefact contributes to a picture which enables an analyst to better understand a sequence of events and the nature of the threat it poses (if any).

Users need to carefully consider whether DNS threat detection and blocking is good enough for them to achieve their target cybersecurity posture. If they determine that it is for the foreseeable future, that can be a sound choice – so long as the question has been asked and the rationale has been understood. If it's not, security teams should start working with their XDR partner or partners to understand how they are going to fulfil their DNSDR requirements.

The need is more pressing for vendors in the XDR space as DNSDR is going to start bubbling up as a requirement among some of their advanced customers. Vendors don't necessarily need intrinsic DNS security capabilities of their own - but they are going to need open integrations with those vendors that do have them. ■

- *HardenStance received no payment - direct or in-kind - for publishing this Briefing.*

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, OASIS, ETSI and TM Forum. www.hardenstance.com.

To receive an email notification whenever HardenStance releases new reports in the public domain, register here (there are only four fields): Registration Link

HardenStance Disclaimer