CYBER STASH

The Business Case For Operationalising Threat Intelligence

eclipse

Introduction

The purpose of this paper is to provide decision makers the information they need to evaluate the potential financial impact of CyberStash Managed Network Detection and Response (NDR) Service powered by its eclipse.xdr platform.

Prior to using the CyberStash Managed Threat Intelligence Gateway Service, customers used manual processes to proactively block threats based on threat intelligence data by utilising a Threat Intelligence Platform (TIPs) or a Security Information and Event Management (SIEM) platform. Additionally, customers used manual processes to prepare and implement changes on their corporate firewalls, web proxy servers and e-mail gateways. These prior efforts returned limited success, with customers unable to scale their labourexhaustive security practice in cost-effective ways. However, following an investment in the CyberStash Managed Network Detection and Response Service, in addition to the immediate risk-reduction, customers were able to benefit from the native threat-feed integration, in-line data correlation, and automated threat detection and incident response.

The primary reason organisations subscribe to the CyberStash Managed Network Detection and Response Service, and also the primary benefit, is that it enables them to detect and block threats that their existing network security controls miss, such as firewalls, web proxy servers, endpoint security solutions, mail gateways and intrusion prevention systems. The service effectively guarantees an immediate reduction in the level of exposure to a massive number of cyber-attacks.

The success rate for our service in demonstrating return on investment (ROI) is extremely high. This is because the vast quantity of threat intelligence data that we use to block attacks is typically not provided by existing security solutions. We guarantee that we can also detect and block incremental threats, thus providing organisations with continual benefits realisation.

These benefits pairs nicely with the relatively affordable cost of our service, not only in terms of the actual cost of the solution but also that it is simple to deploy, highly automated, and doesn't add material overhead to client teams because we deliver it as an end-to-end solution packaged with a managed service.

In conclusion, the combination of our platform and service manifestly reduces cyber risk and adds substantial value very quickly without introducing significant overhead.

This business case focuses on the importance of using a Defence in Depth security architecture and substantiates the value of using threat intelligence to effectively manage the type of cyber risks faced in today's threat landscape. By comparing our blocking-methodology solution and service with those of Threat Intelligence Platforms (TIPs), which require manual human effort to investigate and apply proactive blocking policies, we can clearly demonstrate the efficiencies gained when using our CyberStash Managed Network Detection and Response Service.

Customers can expect the following benefits when using CyberStash Managed Threat Intelligence Gateway Service:

- *Risk adjustment – a lower risk profile*
- *Security team efficiency gains – frees up existing resources*
- *Cost savings – avoids manual processes to setup and maintenance the platform*
- *Reduced time to deploy and integrate – realise benefits from day 1*

Business Case

Defence in Depth

Defence in Depth is a comprehensive approach to cybersecurity that recommends using a combination of layers to protect critical data and block threats. This deliberate multi-layered approach increases the security of the system as a whole and addresses many different attack vectors. Defence in Depth was originally a military strategy that aimed to slow down or delay the advance of an attacker rather than using immediate retaliation with one line of defence. As business and technology have evolved, it's become increasingly apparent that the same strategy can be equally effective for managing cyber risk.

Layering security defences reduces the chance of a successful attack. Incorporating redundant security mechanisms requires an attacker to circumvent each mechanism to gain access to a digital asset. For example, a software system with authentication checks may prevent an attack that has subverted a firewall. Moreover, to minimise the risk of a cyber-attack succeeding, you must either prevent the threat or remove the vulnerability from the system. Having a security strategy that controls both the threat and the vulnerability is a type of defence in depth approach that most effectively minimises risk.

The idea behind defence in depth is to manage risk with diverse defensive strategies so that if one layer of defence turns out to be inadequate, another layer of defence will hopefully prevent a full breach leading to business impact.

Currently, most organisations leverage a Nextgen Firewall to control the flow of network traffic. In addition, the Nextgen Firewall inspects traffic looking for specific threats that target known vulnerabilities. The effectiveness of managing risk by focusing on controlling threats against vulnerabilities is only partially effective and using a Network Detection and Response helps to minimise the security gaps outlined in the table below:

#	Gap	How a Network Detection and Response Helps
1	On average, only about 50% of vulnerabilities have been discovered. Many attacks target unknown vulnerabilities and remain undetected.	A Network Detection and Response prevents the source of the attack irrespective of the vulnerability or how advanced the attack is. Preventing known "bad" IP addresses, domains, ASNs and Countries, massively reduces an organisation's exposure to cyber threats.
2	NextGen Firewall vendors take time (up to a week sometimes) to develop intrusion prevention signatures that would protect an asset from Zero-Day vulnerabilities. Furthermore, most organisations do not patch application and system vulnerabilities fast enough to reduce the risk to an acceptable level.	A Network Detection and Response provides defence against emerging threats because it blocks attacks based on the level of maliciousness associated with the source of the traffic and thus reduces the level of exposure to Zero-Day exploits.
3	Non-system-vulnerability based intrusions, such as phishing and social engineering attacks, entice or lure users to websites where their credentials are compromised or replayed to the real website through a man-in-middle attack. Nextgen Firewalls, vulnerability remediation, or Mufti-factor authentication, cannot prevent these types of attacks. The stolen credentials are simply used by the attacker to "legitimately" log in to business systems or sold in the dark web to other attackers.	A Network Detection and Response can: 1 – prevent the user's traffic from ever reaching the phishing website, and/or 2 – prevent the attacker from accessing the business system if they are sourced from a known "bad" IP address, ASN or country.

4	Remote access services that are externally exposed, are exposed to everyone on the Internet, from any country and any ISP (Autonomous System). This means the attack surface to the application is not controlled. Firewalls allow traffic to these exposed services from ANY source, thus leaving the application an open target without any real restriction on where the traffic is sourced from.	A Network Detection and Response can ensure that traffic to exposed services comes only from trusted or low-risk countries or ASNs. For example, we can create a resource pool that's specific to exposed remote access services, that blocks access attempts from Ukraine, China, Russia, etc., or only allows access from Australia. Further still, for SaaS-based solutions that require a "proxy" server to be hosted in the DMZ of the client's network, we can configure a specific policy to only allow traffic from the SaaS vendor's BGP/ISP, thus avoiding the need to continuously update firewall policies. This is especially helpful for minimising risk without adding management overhead for vendors with a large number of IP addresses that change and expand over time. This enables a balanced approach to security by controlling exposure to external applications.

Threat Landscape

The current threat landscape is mostly opportunistic, whereby cybercriminals build their infrastructure to attack anyone and everyone. No organisation is impervious to such attacks. Most users and organisations continue to be breached because of this type of attack and not because they've been specifically targeted. In addition to these opportunistic attacks, sophisticated targeted attacks also need to be managed.

Defending an organisation against cyber threats, therefore, requires threat intelligence. At any given time, the Internet plays host to millions of IP addresses and domains with links to malicious cyber activity. As we're all connected to a global network, none of us works in isolation, and we all face similar threats from adversarial sources that typically do not discriminate when it comes to which organisations they target. We can, therefore, leverage the collective threat intelligence gathered globally to detect and block known threats and thereby defend business systems and sensitive information.

Predictive intelligence must be used both effectively and efficiently. Knowing about the sources of threats but doing nothing until they begin to target your organisation is neither an effective nor an efficient approach to cybersecurity.

To optimise risk and resources, a Threat Intelligent Gateway enables a better practice that:

- Proactively blocks inbound communication from IP addresses used by attackers.
- Proactively blocks outbound communication to IP addresses and domains used by attackers.
- Proactively blocks inbound and outbound communication from "risky" countries where there is no business activity taking place.
- Proactively blocks inbound and outbound communication from "risky" ASNs.
- Applies risk-based policies that are triggered by threat intelligence and informed by the risk levels of an ASN and/or Country.

NextGen firewalls are incapable of processing an adequate subset of threat intelligence indicators. This leaves organisations operating with a limited subset, resulting in security coverage gaps and/or the need to invest in expensive deep packet inspection processing power to stop the massive volume of known threats.

With close to 950 million shared threat indicators available in open-source feeds alone, a purpose-built defence capability such as the Network Detection and Response is clearly required to consume the dynamic and growing sources of threats and stop them in their tracks.

The CyberStash Network Detection and Response automates the blocking of threats, thus optimising risk and resources. It enables risk-aware security policies and addresses rapidly emerging security threats. It also permits organisations to add their own block-lists and provides threat detection and hunting capabilities against known threats to support the organisation's overall cyber threat detection, investigation, and incident response capability.

ROI And Prevention VS Detection And Response

In addition to the immediate risk reduction attained when blocking traffic based on its reputation, organisations can expect the following resource optimisation:

#	Resources Stage	Detection and Response Methodology	Protection Methodology	Expected ROI using Protection Methodology over 3 Years
1	Correlation	To automate detection, you need to correlate eventsfrom your other securitytools with the threat indicators available from a Threat Intelligence Platform. This integration is not so easy and will consume a ma-terial amount of resourcesand processing power toimplement. Furthermore, with software changesand vendor device replace-ments, this integration is expect-ed to break and will requireeffort to re-establish – all ofwhich takes ample time and resources to address. A typical integration would be expected to require 3 months of resource effort to implement.	By placing the Threat Intelligence Gateway inline with traffic flow, the integration of trafficflows and cyber threatindicators is instant,natively available and out-of-the-box automated. Moreover, it's not necessary to spend valuable resources on integrating andmaintaining theintegration as vendor devices are upgraded or changed.	Upfront: 3 Months x 173 hours per month of expected effort = 519 hours of effort. Annual: 3 weeks per year = 120 hours of effort per year to main-tain. Total over 3 years = 519 + (3 x 120) = 879 hours over 3 years. Total Effort 879 Hours Saving: 879 Hours

2	Investigation	Best practice necessitates that every significant attack against an organisation is investigated. The reality today is that no organi-sation has sufficient resources to investigate every at-tack with the potential to impact business. This number can range from 10s to 1000s per day. With the massive number of threat intel data available and continuously evolving, trying to manually investigate every item of traffic that traverses an organisation that has related intel data is simply not going to be feasible. Organisations are forced instead to accept the risk and trust that their other security controls will protect or detect the attack. Without blocking the source of the attack in its tracks,organisations must detect those attacks that are not blocked and associated with threat data, and then investigate each individ-ually and take responsive actions.	By blocking the sourceof attacks and reducingthe attack surface, thenumber of attacks withthe potential impactbusiness, or that do impact business, ismassively reduced. Thenumber of investigationsrequired is consequentlyalso reduced andexpected to be between1 and 5 per month.	Using a lower-range (worst-case scenario) requiring the investigation of 10 attacks or threat advisories each day compared to 5 per month, with each investigation needing a minimum of 4 hours to complete. 10 x 4 x 365 x 3 years = 43,800 hours 5 x 4 x 12 x 3 years = 720 hours Saving: 43,080 hours

3	Threat Containment	By not blocking attacks, organisations typically need to design and raisechange requests to be approvedbefore they can implement the change to block an attack or a potential threatbased on threat intel data. Thenumberof containment actions and/or the number of proactive blocking that is implemented as a result of threat intel data is expected to range between 10s and 100s per day.	By blocking the attack inline and in real time, there is no additional demand on resources. Furthermore, clients can raise a request against the team to have custom blocklists added, which means a further reduction in resource demand from their own team members.	Using a lower range (worst case scenario) requiring the investigation of 10 attacks or threat advisories each day compared to none, with each containment needinga minimum of 1 hour tocomplete. 10 x 1 x 365 x 3 years = 10,950 hours Gain: 10,950 hours
4	Incident Re-sponse	During an attackor an incident, an organisation's abilityto investigate and implement swift response actions is critical for minimising business impact. Containing the sourceof the attack is one method that can be used to immediately reduce risk to an organisation. Therelative effort of takingresponse actionsusing a Threat Intelligence Platformis far higher than usinga Threat Intelligence Gateway becausethe Threat Intelligence Platform is not doingthe blocking.	With a Threat Intelligence Gateway, as the traffic associated with the attackis in line with the gateway,it can simply be blocked inbound and/or outbound with relative ease and swiftness.	Based on the number of incidents, however, if using a Threat Intelligence Gateway prevents 5 breaches per year, and it takes 6 hours to investigate and contain each occurrence, then that results in a saving of 10 x 6 x 3 years = 90 hours Saving: 180 hours

		Organisations need to design the required response accordingly, once again deciding where to implement the blocking action and then raise anurgent change requestto have it implemented.		
Total Gain over 3 years with Threat Investigation (On an annual basis, an FTE is considered to be 2,080 hours)				55,665 Hours Equivalent to 26 FTEs
Total Gain over 3 years without Threat Investigation (On an annual basis, an FTE is considered to be 2,080 hours)				12,009 hours Equivalent to 6 FTEs

The growing importance of threat intelligence

With significant availability of threat intelligence feeds and services, organisations are increasing their use of threat intelligence to improve cyber situational awareness, cyber defence, and as a tool to better scale their existing security staff and operations.

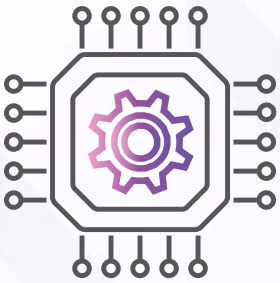
This adoption has been fuelled by the aforementioned threat scale problem, which requires organisations to have a broad-based view of threat activity across a range of sources, including commercial, open source, industry, and government.

Until recently, organisations relied on the threat intelligence provided by existing security controls like Next Generation Firewalls (NGFWs), Unified Threat Management (UTM) solutions, Intrusion Prevention Systems (IPS), Secure Web Gateways (SWG), and endpoint security controls. However, while still relevant and necessary, only a narrow view of threat actor activity is represented based on telemetry from a particular vendor's perspective.

ces

Threat Intelligence must come from Multiple Sources and Perspectives

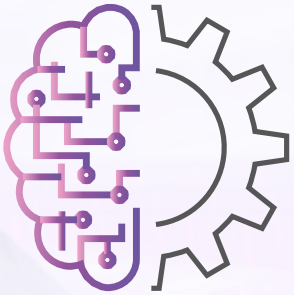
Organisations are leveraging threat intelligence from multiple sources, including commercial,open-source, industry, and government sources:



Commercial

Threat intelligence is available from a wide range of leading commercial sources Commercial sources include large established cybersecurity vendors like Webroot and Proofpoint to threat intelligence specialistslike DomainTools, IntSights, and Recorded Future.

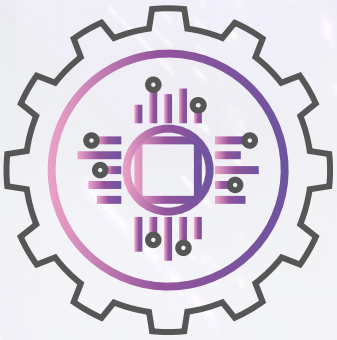
A key point is that each of these vendors brings their own unique threat intelligence based on their approach and focus



Open Source

There is a significant amount of free, open-source threat intelligencethat organisations can access. As we have seen with commercialsoftware like operating systems (Linux), the open source community canoffer significant value. The same is true in the area of threat intelligenceSome of the high quality, open-source threat intelligence sourcesincluding AlienVault's Open Threat Exchange, Blocklist de, CI Army List,Feodo Tracker, and others.

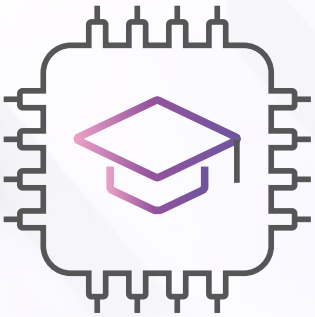
Industry



Context is key when it comes to threat intelligence, and threat actors are increasingly launching campaigns targeted at specific industries. To guard against these targeted campaigns, having visibility intothreat actor activity in the industry one operates in is critical Inthe U S , this need is being served by Information Sharing Analysis

Centers (ISACs) and Information Sharing Analysis Organisations (ISAOs). Currently, there are more than 20+ ISACs/ISAOs operating across a range of industries. There are also organisations like Global Resilience Federation, that facilitate cross-industry threat information and indicator sharing.

Government



Government organisations are some of the most sophisticated when itcomes to threat intelligence gathering and sharing Nation-state cyberactivity is the "new normal" and cyber operations (offensive and defensive)is now a critical domain of all countries' protocol. In many countries, thereare increasing efforts by government organisations to collaborate with theprivate sector to share threat intelligence.

For example, in the U S, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) shares threat intelligence with the private sector through its Automated Indicator Sharing (AIS) and its Cyber Information Sharing and Collaboration Program (CISCP) programs.

Use of Threat Intelligence becoming more Critical in Security Frameworks & Regulatory Focus

The use of threat intelligence, including information sharing, is becoming more critical in cybersecurity frameworks.

For example, the use of threat intelligence is now specifically identified in the Risk Assessment Category of the NIST Cybersecurity Framework Core. Additionally, sharing of threat intelligence is key to progressing through the Framework implementation tiers.

Regulatory and compliance efforts are also increasing their focus on threat intelligence use and sharing. For example, in the financial services industry, using and sharing intelligence, including FS-ISAC threat intelligence, is an increasing focus of regulators conducting Federal Financial Institutions Examination Council (FFIEC) exams.

It is clear that over time, the use of threat intelligence will continue to gain importance as it pertains to regulatory and compliance efforts.

The challenges of Threat Intelligence (TI)

While there is an abundance of threat intelligence available to organisations, many find challenges with effectively and efficiently incorporating and operationalising it into their business and IT workflows.

Accessing Threat Intelligence

Ti Challenge 1

The majority of security organisations in Fortune 1000 companies have made threat intelligence a key element of their cybersecurity operations. These organisations realise that the threat intelligence offered by existing security controls like next-generation firewalls are insufficient, and that a broader view of threatactor activity is required.

Large enterprise organisations are fortunate to operate with significant staff and budget resources. For thisreason, threat intelligence has historically been the domain of large enterprises, however, most still repotthat they don't have the skills and sufficient capacity to make threat intelligence actionable.

Unfortunately, attackers don't only target large organisations and, due to the resource constraints of smaller organisations, there is a perception that using threat intelligence is beyond their reach. However, with the innovation of the CyberStash Network Detection and Response, organisations of all sizes can incorporate threat intelligence into their security operations in an easy and automated way.

Ti Challenge 2

Managin Threat Intelligence

Managing and maintaining threat intelligence can be challenging. This is true for those new to threat intelligence, as well as its power users Threat feeds are produced in different formats, include different categories, and have different scoring systems.

To address this challenge, many large organisations have turned to Threat Intelligence Platforms (TIPs) from companies like Anomali, IntSights, ThreatConnect, and Threat Quotient TIPs help companies manage TI in a more effective and efficient way TIPs to threat intelligence are analogous to the role SIEMs play for security events and alerts TIPs aggregate, normalise, correlate, and apply analytics to multiple sources of threat intelligence TIPs play an important role in enabling organisations to efficiently manage their TI, and to help security analysts determine what TI is most actionable.

The challenge with TIPs is that the use of this technology is limited to large organisations that have the budgetary resources to purchase, and—more importantly—the skilled staff to operate, this technology. Even when integration is successful, this doesn't address the lack of real-time action that is still necessary to evidently reduce risk for an organisation.

Ti Challenge 3

Making Threat Intelligence Actionable

Gartner defines the three critical elements of threat intelligence as "Acquire, Analyse, and Act" Of these three elements, "Act" remains both the most critical — and the least implementable--component of threatintelligence. In the words of Gartner analyst, Craig Lawson, "If you have intelligence that tells you your house is going to burn down, and you don't do anything with that intelligence, then what's the point?

Acting on Threat Intelligence remains both the most critical and least implementable component of threat intelligence.

Taking Action

With threat intelligence is the ability to use threat intelligence indicators to prevent (block), detect, and respond to threats. The challenge with taking action with TI lies in the significant limitations of existing network security controls, specifically next-generation firewalls. Typical next-generation firewalls have two key limitations:

- An inability to efficiently process large volumes of third-party threat indicators, resulting in coverage gaps or expensive and inefficient use of firewall processing power.
- A narrow, single-vendor focus and source of threat intelligence data, which often leaves out threat indicators from external sources.

While firewalls are particularly good at detecting and blocking threats based on their own indicators, the majority of firewalls are limited in the number of third-party threat indicators that they can process. This is due to an inherent bias towards their own proprietary threat intelligence combined with performance challenges as firewalls increasingly spend precious computing cycles on a never-ending array of functions.

According to Gartner's Emerging Technology Analysis: Network Detection and Responses report, "Because
multifunction firewalls apply so many security inspection and prevention capabilities, they typically are limited from as low as 30,000 threat indicators to as high as 300,000 for larger (higher end) appliances

Gartner's Emerging Technology Analysis: Threat Intelligence Gateways Report

"Because multi-function firewalls apply so many security inspection and prevention capabilities, they typically are limited from as low as 30,000 threat indicators to as high as 300,000 for larger (higher end) appliances. Therefore, existing solutions have significant TI-based threat blocking limitations."

According to data from next-generation firewall market leader, Palo Alto Networks, on each firewall platform, you can configure a maximum of 30 unique sources for external dynamic lists Additionally, depending on the platform, Palo Alto Networks firewalls support a maximum of 50,000-150,000 total IP address threat indicators and a maximum of 50,000 to 4 million domain threat indicators, This number is greatly inadequate when one considers that the number of malicious IPs and domains launched every day: actual numbers are in the tens of millions!

These threat intelligence indicator limitations inhibit an organisations' ability to take action on threat intelligence at the scale required to protect their networks in a modern, constantly evolving threat landscape. Additionally, even if we set aside threat indicator volume limitations, managing and maintaining threat intelligence in a firewall—including managing firewall rules, external blocklists, and access control lists (ACLs)—is cumbersome and time consuming: a burden for those organisations who are already strapped for resources.

The majority of organisations that are using threat intelligence are integrating threat feeds into their SIEM systems to aid with manual detection and response efforts. While this is useful, it leads to the use of TI being reactive instead of proactive. Leading security organisations are shifting their threat intelligence strategy to a more proactive stance in order to prevent threats, reduce the workload on their staff, and offset the previously discussed limitations of their traditional security measures.

Network Detection and Response Technology

Over the last few years, a next-generation technology known as Network Detection and Responses has emerged to scale threat intelligence efforts, provide organisations with a proactive way to block threats based on threat intelligence, and fill in the cybersecurity gaps of next-generation firewalls and other security controls Network Detection and Responses solve many of the challenges associated with threat intelligence by helping organisations aggregate, integrate, and make threat intelligence actionable in an easy and automated way.

This is enabling TI power users to gain more value from their TI investments by enabling automated action and bringing the power of TI to smaller, more resource constrained organisations. Threat Intelligence Gateways are a unique security technology because they sit at the intersection of network security and threat intelligence. They are also unique in that they complement many of the existing security technologies a company has and often times make those resources more efficient.

Industry Analysts validate Threat Intelligence Firewall as a Category

Network Detection and Response technology has been validated by leading industry analyst firms like Gartner and Enterprise Strategy Group (ESG) Several years ago, Gartner defined this technology in the report, “Emerging Technology Analysis: Network Detection and Responses ” While the name of the technology has now evolved to Network Detection and Responses the core function as described by Gartner remains the same “stand-alone network detection and threat mitigation appliances that leverage large numbers of threat indicators for detection and blocking purposes, ‘on-box’, at wire speed”.

Gartner goes on to say that Network Detection and Responses, “...are differentiated and disruptive to alternative solutions because they offer massive on-box indicator scale that is not provided by other existing network security solutions.

Additionally, in their "Market Guide for Threat Intelligence," Gartner describes Network Detection and Response technology as, "an easy to deploy and maintain solution", where TI is "..aggregated and actionable as an immediate outcome on deployment." Gartner goes on to suggest that organisations choose a solution that is capable of ingesting open standards for threat intelligence, as opposed to those that reduce the options for 3rd party or customised threat feed ingestion. From a narrow perspective, a Network Detection and Response can simply be viewed as network security solution that is purpose-built to filter network trafficbased on large volumes of threat indicators (IPs and domains). On a broader scale, it provides a robust range of threat intelligence protection capabilities.

Choosing the right Network Detection and Response

When choosing the right Network Detection and Response, Gartner has defined the features, both required, as well as optional, for an effective solution:

Required Features:

- Massive on-box indicator support
- Minimum of 500,000 indicators
- TI-based network blocking and detection capabilities on-box Integrated threat feeds
- Filtering support for:
- IP addresses

Optional Features:

- Granular network policy management with threat feed and TI focus
- Threat intelligence platform integration
- Structured Threat Information eXpression (STIX)-formatted indicator support
- Filtering support for:
  - Fully qualified domain names
  - Domains
  - URLs

Threat Intelligence Use Cases are Important

One problem with threat intelligence is that the term gets used loosely; the fact is there are lots of different types of threat intelligence. Leading industry research firm Gartner suggests that when considering threat intelligence, organisations should focus on specific use cases Figure 5 depicts the key uses cases according to Gartner Different use cases will have different vendors specialising in that area.

However, even with a preconceived list of features and functionality, how does one determine the value of one Network Detection and Response vs another. We believe the answer lies in its ability to access, aggregate, and act on threat intelligence, as well as its ability to integrate and interoperate with other security intelligence and technology, and its simplicity in deploying and managing the technology.

Access of Threat Intelligence

As mentioned by Gartner, an effective Network Detection and Response must be able to provide access to the millions of threat intelligence indicators that are available from the many, reputable, threat intelligence sources, available to organisations, associations, and their members. These threat intelligence types include IP and domain reputation feeds and IP and domain blacklists.

As detailed in the section, Threat Intelligence Must Come from Multiple Sources & Perspectives, threat intelligence feed sources include commercial, open-source, industry, and government sources.

Vendor Agnostic Threat Intelligence

What is important when gathering threat intelligence indicators to defence a business, is that the intelligence collected is from multiple sources and of multiple types. In fact, recent research conducted by usenix has shown that from between open and paid threat intel sources, there was almost no overlap in indicators.

The research found:

- 1.3% : 13% overlap in indicators from 2 different commercial vendors whereby 13% of the first vendor's indicators were found in the second vendor's dataset and, 1.3% of the second vendor's indicators were found in the first vendor's dataset.
- In reviewing indicators associated with 22 threat actors for which both vendor 1 and vendor 2 had indicators, they found an average overlap of less than 2.5%:4.0% per dataset group, depending on the type of indicator.

The CyberStash Managed Threat Gateway Service leverages intelligence from both commercial and opensource threat feed providers as well as from government advisories. We then continuously measure the quality of intel data received from each source to determine whether we are continuing to receive a high yield from each source.

Aggregation of Threat Intelligence

While most security devices enable organisations that are using threat intelligence to integrate these feeds into their devices, oftentimes they cannot be done at scale, requiring individual block lists to be manually entered.

According to Gartner, an effective Network Detection and Response solution should have the ability to easily
aggregate multiple threat feeds, at a central point, as well as update in an automated fashion. Both of these features realise time savings for IT staff and resources.

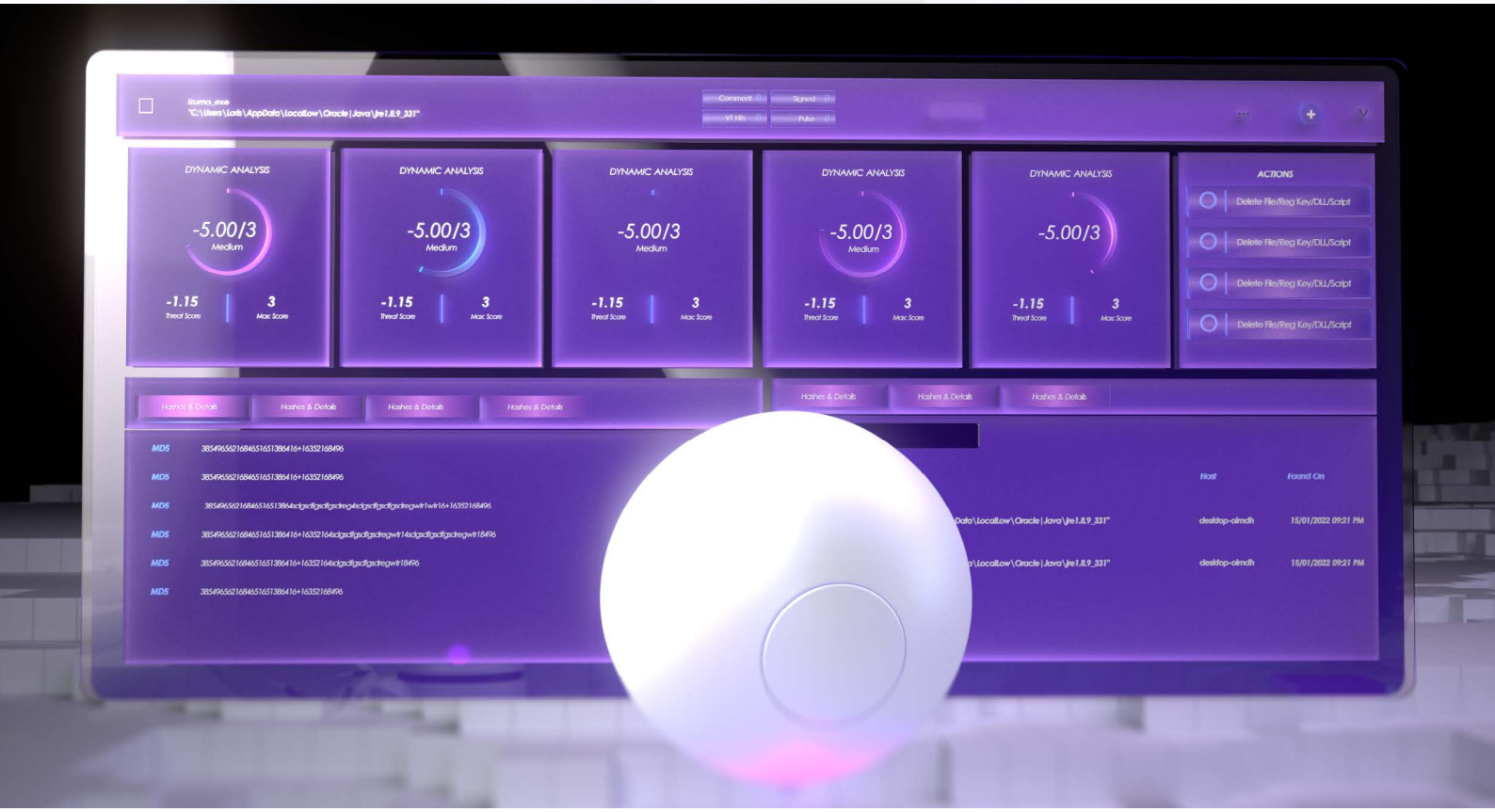
Automation of Threat Intelligence

The ever-changing nature of threats means that threat intelligence is dynamic, and the tools that process or utilise threat intelligence must seamlessly adapt to and enable this constant change. Reputation scores of IPs and domains are constantly changing, and IPs and domains are constantly being added and deleted from blacklists. Therefore, it is critical that threat intelligence be constantly updated within the security tools that process it, and it is equally critical that this is done in an automated manner.

The ever-changing nature of threats means that threat intelligence is dynamic, and the tools that process or utilise threat intelligence must seamlessly adapt to and enable this constant change.

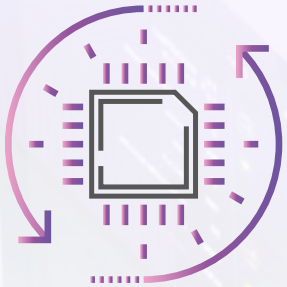
Acting on Threat Intelligence

Arguably, the most critical aspect of threat intelligence is the ability to make it actionable. On a more granular level, taking action is the ability of a threat intelligence solution to enable policy-based blocking of known threats and unwanted traffic based on threat intelligence, country IP, and/or organisation IP
This functionality is key to the value proposition of Network Detection and Response technology



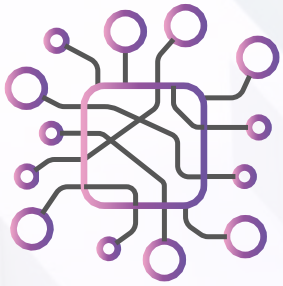
Network Detection and Response Use cases

There are many Network Detection and Response use cases, and they vary based on the size and sophistication of security organisations. A common theme in all cases is that customers are deploying Network Detection and Responses as another layer of defence to improve cyber situational awareness and threat defence.



Ti Protection & Automation

This use case is typically seen with small and mid-sized enterprises that are looking to incorporate threat intelligence as another layer of a defence-in-depth approach to security. Many of these companies are also using some form of threat intelligence -in many cases, threat feeds from ISACs These organisations are finding value in the ability to automate the management (reduced staff workloads) of this threat intelligence and the ability to take action with it to protect their networks. Ease of deployment, automation, and affordability, are key value propositions for this use case.



Operationalising TI

This use case is geared towards security organisations that are heavy users of threat intelligence. The key challenge these organisations face is operationalising TI at scale This includes the ability to do threat intelligence-based blocking (prevention) as well as the ability to detect and respond to network threats based on threat intelligence. In some instances, these organisations have deployed both Threat Intelligence Platforms (TIPs), as well as Network Detection and Responses to provide the action piece. However, there are also instances in which customers have not deployed a TIP and find value in the Network Detection and Responses aggregation and automation capabilities.

Alleviating Firewall Overload

The massive volume of known, noisy threats is forcing organisations to continually spend more on expensive deep packet inspection (DPI) processing capabilities to keep up with the volume. By deploying a Network Detection and Response in front of their NGFWs, organisations are able to significantly reduce the volume of known threats before they hit the firewall, enabling more efficient use of firewall resources

Threat Investigation, Pivoting, Hunting

By reviewing network traffic logs with context, a security analyst can easily pivot against a specific hypothesis and then investigate the traffic as part of the organisation's threat hunting practice. As an example, a security analyst could effortlessly filter outgoing traffic that is destined to high-risk countries such as China, North Korea, Russia and Ukraine, and then enrich discovery by investigating the domain and/or IP address against threat intelligence indicators. By running such querying, organisations can detect previously unknown or undetected threat within the enterprise and then contain risk using the Network Detection and Response or by cleaning up the compromised endpoint

Network Detection and Response Benefits

Organisations are adopting and deploying the Network Detection and Response technology to operationalise
their threat intelligence, and/or improve the effectiveness and efficiency of their cyber defence and security operations. These organisations realise many benefits, such as:

- Improved cyber-situational awareness and network defence by leveraging threat intelligence to gain a broader view of cyber threat activity.
- Attack surface reduction through more effective and efficient filtering of inbound traffic.
- Improved security staff efficiency through reduced manual workloads related to threat feed management, firewall rule and ACL management, alert reduction, and fewer manual firewall log reviews.
- Increased return on existing security technology investments, including next generation firewalls, threat intelligence, SIEMs, and threat intelligence platforms.
- Faster threat detection and response, through automated blocking for known threat indicators and detection of stealthy attackers operating within your network through threat hunting with contextual intelligence.

Qualification Self-Assessment Questionnaire

The CyberStash Network Detection and Response Service aggregates and integrates threat intelligence in the
cloud and makes it actionable by blocking known bad traffic before it hits your network. The CyberStash Cyber Network Detection and Response platform can block up to 150 Million IP and domain threat indicators at line speed of 10 Gbps, far exceeding the capabilities of next-generation firewalls.

Our turnkey solution and service can be quickly installed, easily deployed, and securely managed.

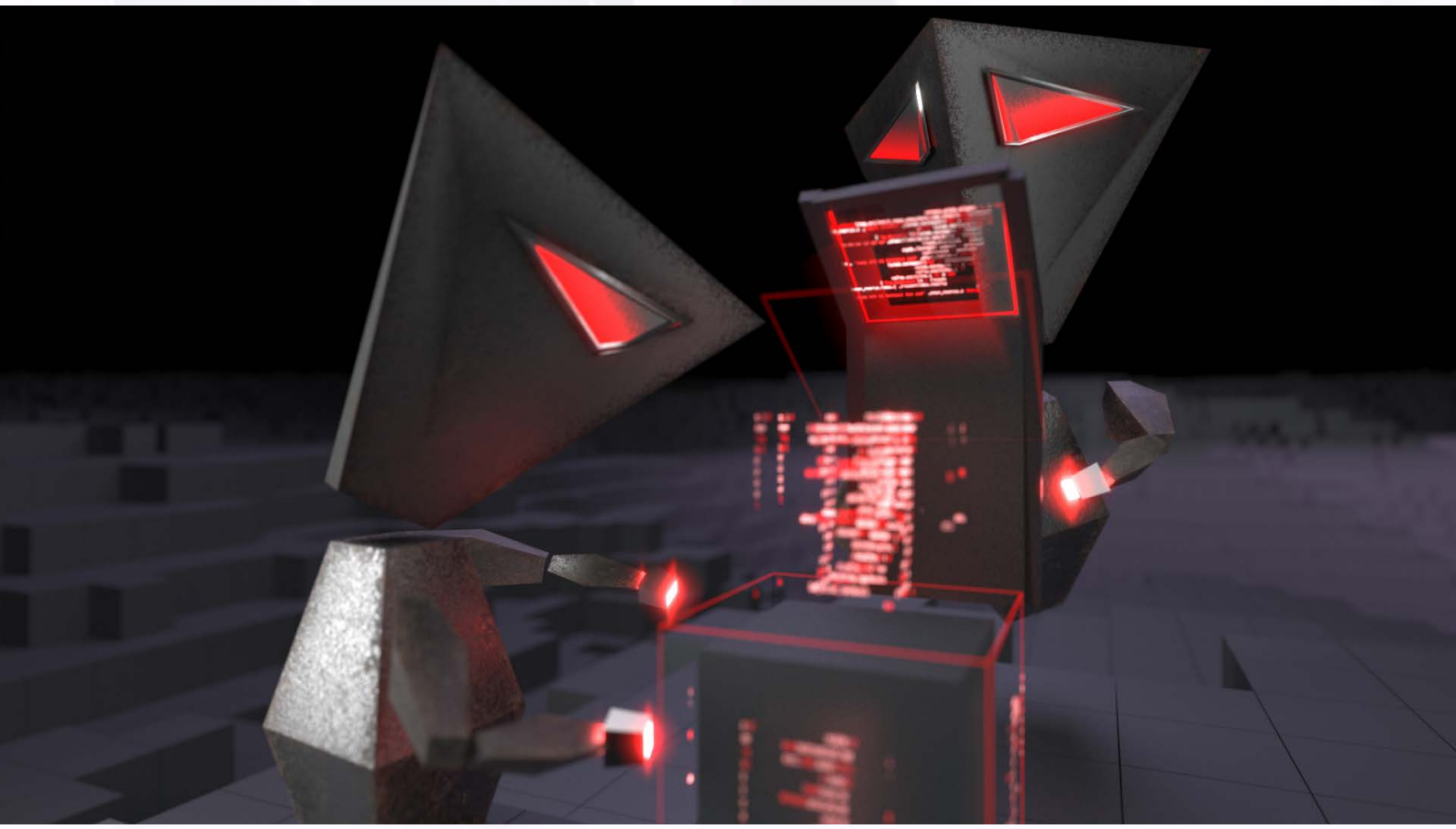
The CyberStash Network Detection and Response Service helps organisations strengthen network defences,
complement existing firewalls, and reduce staff workload.

Complete a Self-Assessment against the qualification question below to understand whether the

How are you protecting your exposed services from inbound threats?

#	Qualification Questions	Answers
1	Are you minimising your organisation's exposure to known cyber threats by blocking traffic originating from millions of known external attack sources associated with? • Web Exploits • Advanced Persistent Threats (APTs) • Scanners • Denial of Service Attacks • Brute Force Passwords	

1	Qualification Questions	Answers
2	Are you reducing the load on your websiteand other assets that provide public- facing services by preventing unwanted traffic from reaching them?	
3	Are you preventing traffic sourced from Countries and ASNs that you do not operate in that are considered high-risk?	
4	Are you optimising human resources by preventing known sources of attacks in their tracks before these reach your network and result in manual processes being required to detect, investigate and response to the threat?	



How are you protecting your outbound traffic from your users and internal systems?

#	Qualification Questions	Answers
1	Are you minimising your organisation's exposure to known threats by blocking outbound traffic to millions of known malicious destination IP addresses anddomains associated with? ● Malware drop sites. ● Endpoint exploits. ● Trojan distribution sites ● Command and Control servers ● Phishing and Spam sites ● Advanced Persistent Threats(APTs)	
2	Are you minimising your organisation'sexposure by blocking outbound traffic from users and systems attempting touse anonymiser services and high-risk sites such as? ● TOR / Anonymiser sites ● Proxy / VPN sites ● Fraudulent Activity sites ● Illegal Activity sites ● P2P Notes sites ● Remote Access sites	

1	Are you minimising your organisation's exposure by detecting and responding to? • Domain generated algorithm command and control behaviour • Cobalt Strike Command and control beacon • DNS Tunneling Traffic • Abnormally Large DNS Response • Tor Activity to the internet • Unusual DNS Activity via Machine Learning (ML)	
2	Are you preventing outbound traffic destined to Countries and ASNs that youdo not operate in that are considered high risk?	

What is your Current Capability?

#	Qualification Questions	Answers
1	Does your organisation have the capability to access a large volume of accurate threat intelligence indicators from open source, commercial and government threat intelligence providers?	
2	Does your organisation have the capability to store, process, normalise and enrich threat intelligence that's collected?	

3	Does your organisation have the capability to block inbound and outbound traffic at scales that are meaningful to minimise risk based on the known risk level of the IPaddress or domain?	
4	Does your organisation have the capabilityto apply real-time risk-based decisions to traffic traversing to or from knownmalicious threat sources?	
5	Does your organisation have the capability to block risky countries andASNs and thereby massively reduce your organisation's exposure to high-risk countries and risky infrastructure?	
6	Does your organisation have the resourcesand skills to collect threat intelligence and make it actionable in real-time without requiring manual effort?	
7	Does your organisation have the resources and skills to correlate threat intelligence with DNS traffic and detect advanced and stealthy threats, and breached systems, that are currently present within your network?	
8	Does your organisation have the resources and skills to block indicators of compromise published in Government advisories?	
9	If you are an OT or utility business, are you specifically blocking known sources of attacks that target OT environment both inbound and outbound from your network?	

About CyberStash

CyberStash combines threat intelligence with technology, processes, and skills to massively reduce an organisation's exposure to most known sources of threats on the internet.

We provide real-time, automated, and predictive threat protection, detection and incident response, by leveraging threat intelligence to minimise an organisation's risk to cyber threats.

info@cyberstash.com
1300 893 802
cyberstash.com
Sydney, Australia

Want to run a trial?

Reach Out To Cyberstash
For More information.

Explore
eclipse.xdr

CYBER STASH