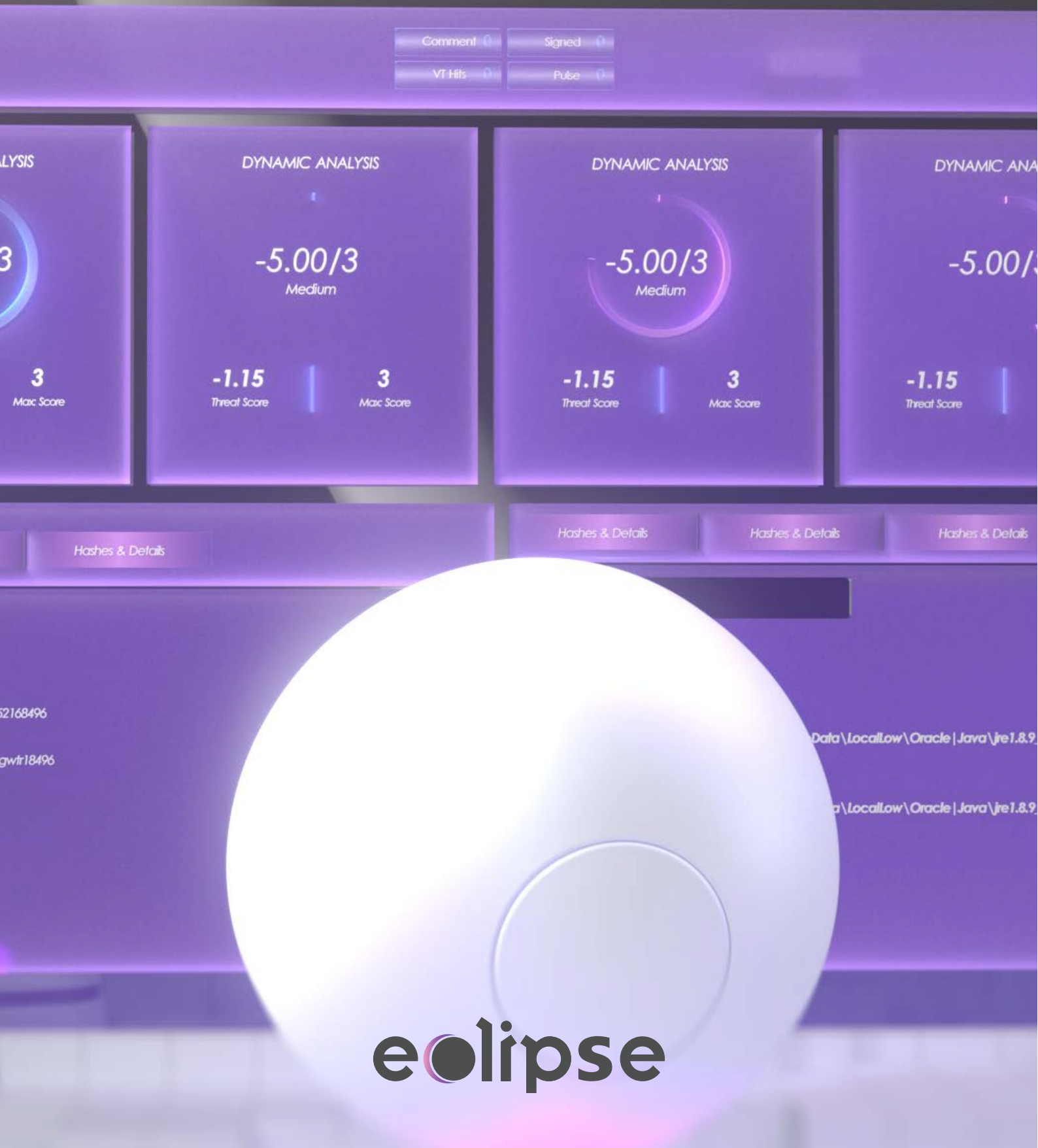
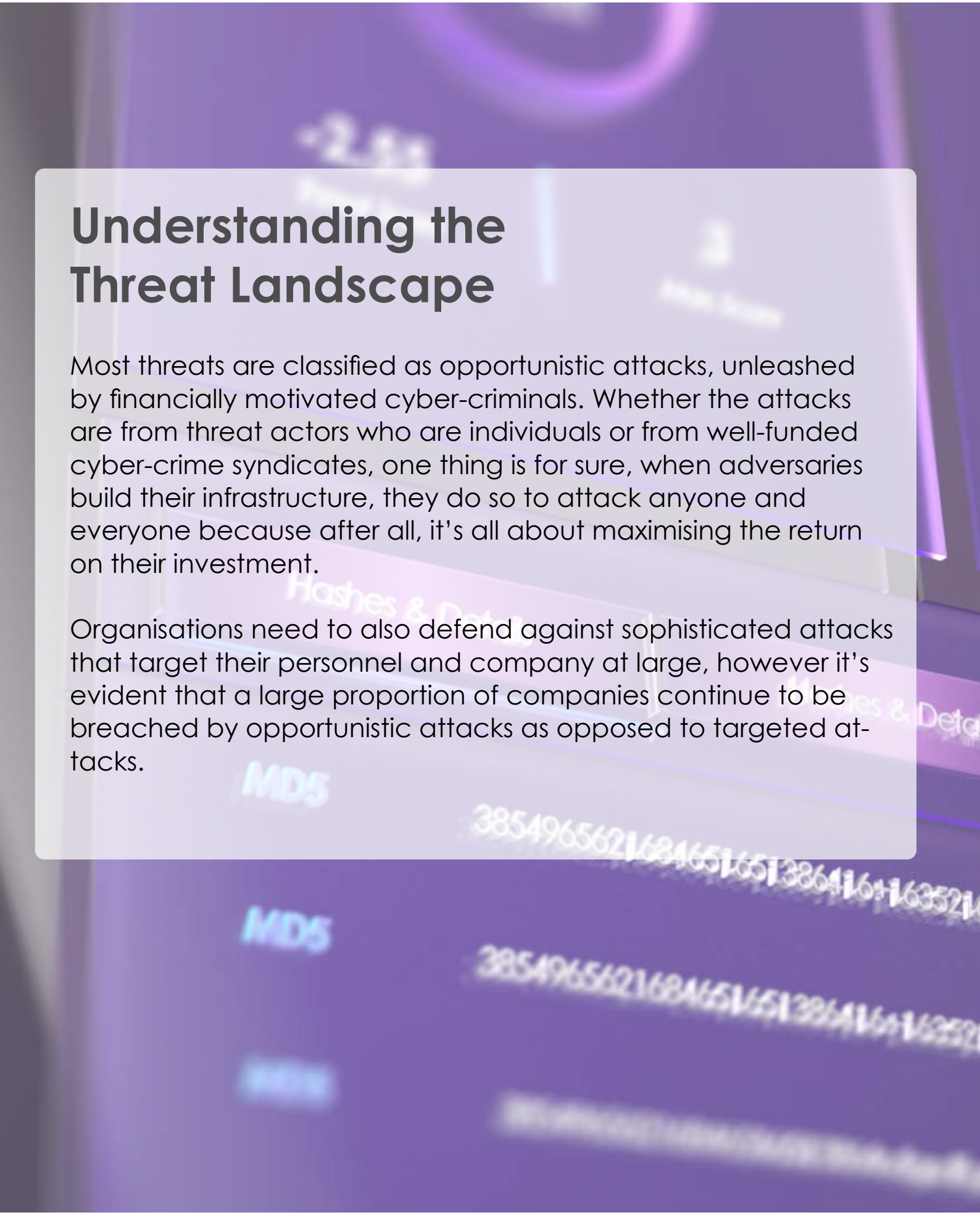
CYBER STASH

Automated “Defensive” Threat Intelligence that Optimises Risk and Resources



eclipse



Understanding the Threat Landscape

Most threats are classified as opportunistic attacks, unleashed by financially motivated cyber-criminals. Whether the attacks are from threat actors who are individuals or from well-funded cyber-crime syndicates, one thing is for sure, when adversaries build their infrastructure, they do so to attack anyone and everyone because after all, it's all about maximising the return on their investment.

Organisations need to also defend against sophisticated attacks that target their personnel and company at large, however it's evident that a large proportion of companies continue to be breached by opportunistic attacks as opposed to targeted attacks.

Reducing Exposure

Organisations can massively reduce their exposure to most attacks out on the Internet by blocking the source of the attack using a massive number of threat intelligence indicators.

Regardless of the attack vector, almost all attackers depend heavily on successful communication being established with the infrastructure they have setup. Whether this is an IP address or a fully qualified domain name, using threat intelligence, organisations can block the source of the traffic on the way into their company to defend exposed services.

Similarly, on the way out, the traffic destined to known bad IP addresses, domains, ASNs or countries, can be blocked, to massively reduce a company's exposure to attacks.

What's important to appreciate is that the level of sophistication of the attack is of no concern to this defensive methodology because once you learn about the reputation of a particular source, the most effective method to defend your business is to simply block all communication with that source. Unfortunately, many companies and the security controls they deploy today, only leverage threat intelligence to detect threats and do not block the threat in line, in real-time.

This results in inefficient security operations, whereby neither risks nor resources are optimised.

Threat Intelligence

Threat intelligence is a valuable commodity but one which if used without context can turn out to be a very costly resource. When it comes to collecting threat indicators, it's especially important to collect from as many high-quality sources as possible. These include:

Commercial: There are commercial cybersecurity companies that specialise in the art of harvesting threat indicators. CyberStash has integrated with several commercial providers, including Webroot, DomainTools, and Proofpoint (Emerging-Threats) so that our clients don't have to.

Open Source: From the 950 million threat indicators that are freely available from the open-source community, a vast number are valuable. There are also many low quality open-source indicators. At CyberStash, we have integrated with only high-quality open-threat feeds to ensure we keep the number of false-positive detections to a low. This is particularly important to our methodology as we are blocking the source of the threat on the way in and out of a company's network.

Government: It's no secret that nation state cyber groups attack each other using cyber-attacks. Cyberwarfare has been increasing but many cybersecurity agencies are now better prepared to detect and release adversaries on emerging and ongoing threats. At CyberStash, in helping to defend Australian businesses and government agencies, we collect and immediately block the indicators of compromise published in advisories released by the Australian Cyber Security Centre (ACSC). We also check all endpoints for presence of compromise and take response actions to help cleanup discovered breaches.

Risk And Resource Optimisation

Risk Optimisation – Blocking a known bad source, stops the attack in its tracks and thereby immediately bring the risk level down to zero. By not blocking, the risk of an endpoint being compromised is higher. The risk of the attack remaining undetected is also higher because a company now has to detect the threat, investigate it, and respond to it, in a time that's meaningful to prevent business impact. With increasing "snatch and grab" type attacks, whereby the attacker has no intension of remaining undetected, sensitive information can be compromised within several minutes. It's therefore far more risk-averse to block an attack instead of attempting to detect and respond to it.

Resource Optimisation – Allowing communication with known bad sources, means that there is more work created for security analysts who then need to investigate the threat. To optimise resources, if you are confident about an IP address or a domain being malicious, it's far more effective to automatically block that source in its tracks.

Compromise Assessment Service, provides

Its Important To Use Multiple Threat Feeds

What's important when gathering threat intelligence indicators to defense 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.

Furthermore, 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.
- Moreover, 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.

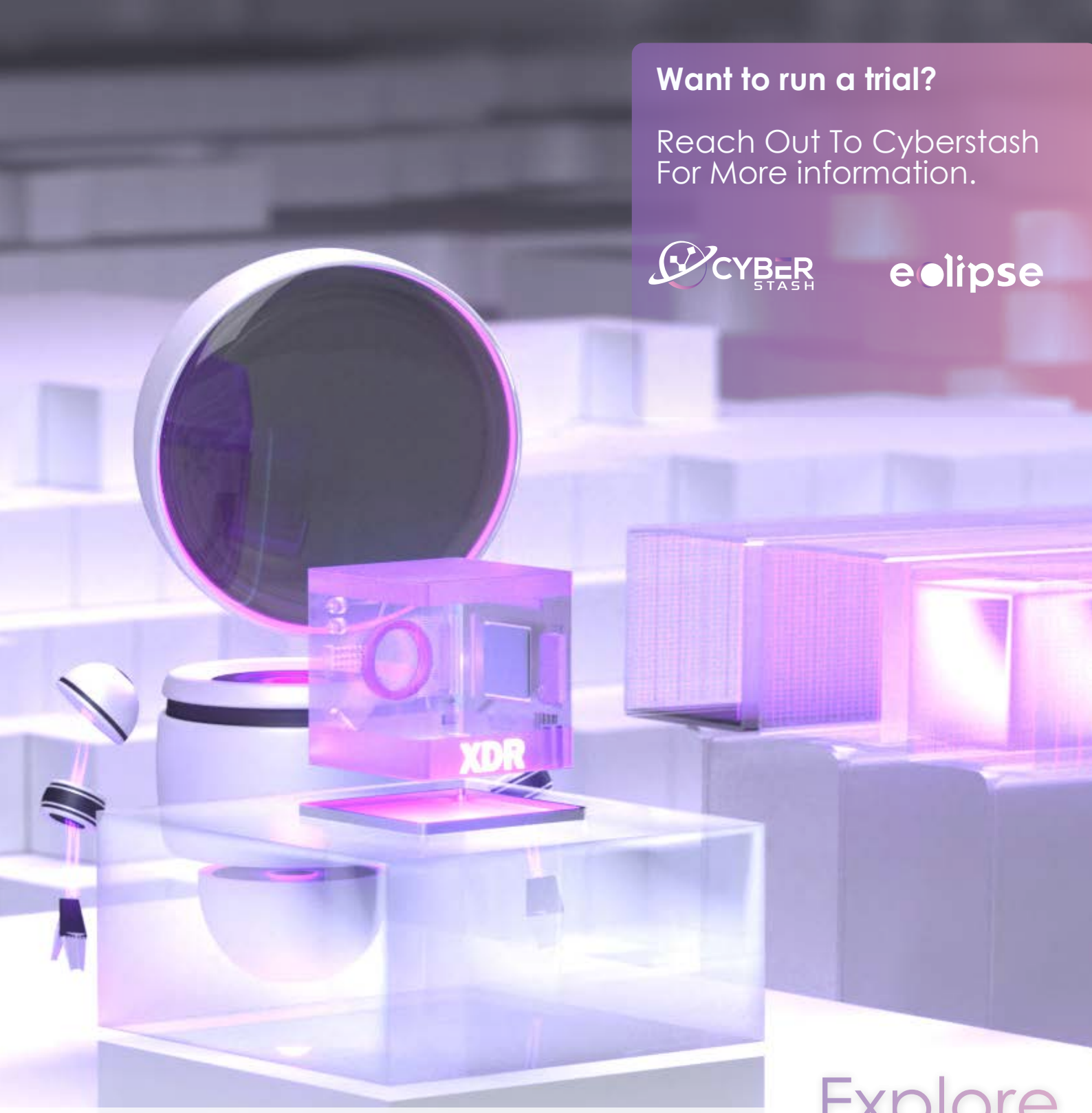
Concluding Remarks

Cyber criminals make big business by expanding their attack surface. They typically don't care which organisations they attack if they can make a quick buck.
As defenders, we must leverage threat intelligence to better protect our businesses, and this must be accomplished through security practices that are setup for success.

Specifically, leveraging threat intelligence to block the source of an attack, irrespective of how sophisticated the attack may be, is a proven method deployed by CyberStash to optimise both risk and resources.

CyberStash, in leveraging millions of threat indicators from commercial, community, and government sources, helps organisations to minimise the likelihood of breach that can lead to business impact.

By processing up to 150 million threat indicators at lines speeds of 10Gbps, we're providing companies a cleaner feed from the Internet and discovering previously unknown breaches on their network.



Want to run a trial?

Reach Out To Cyberstash
For More information.

CYBER STASH

eclipse

Explore

eclipse.xdr

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

CYBER STASH