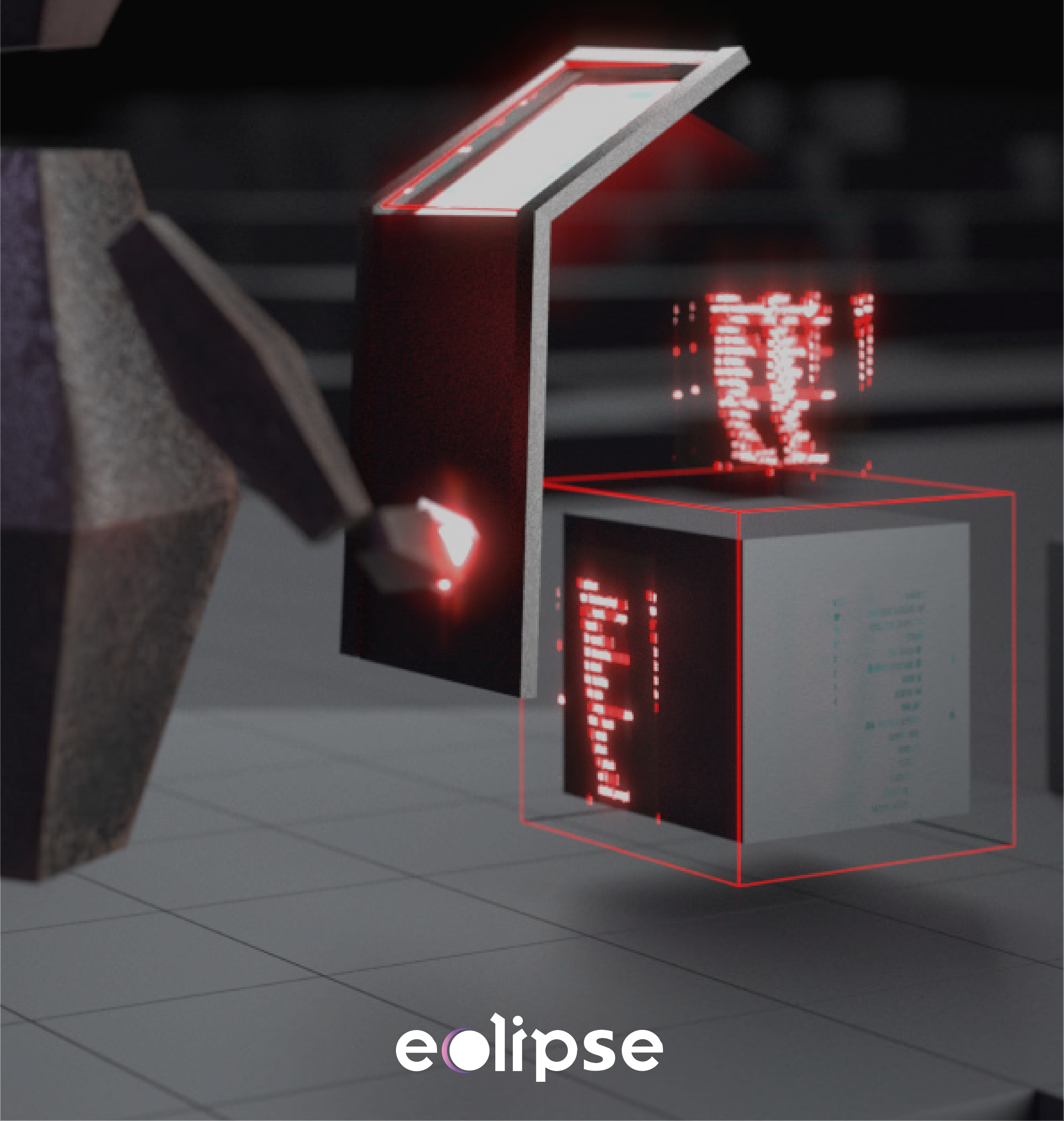
CYBER STASH

5 Mistakes CIOs and CISOs Must Avoid when Building a Cyber Threat Detection and Response Capability

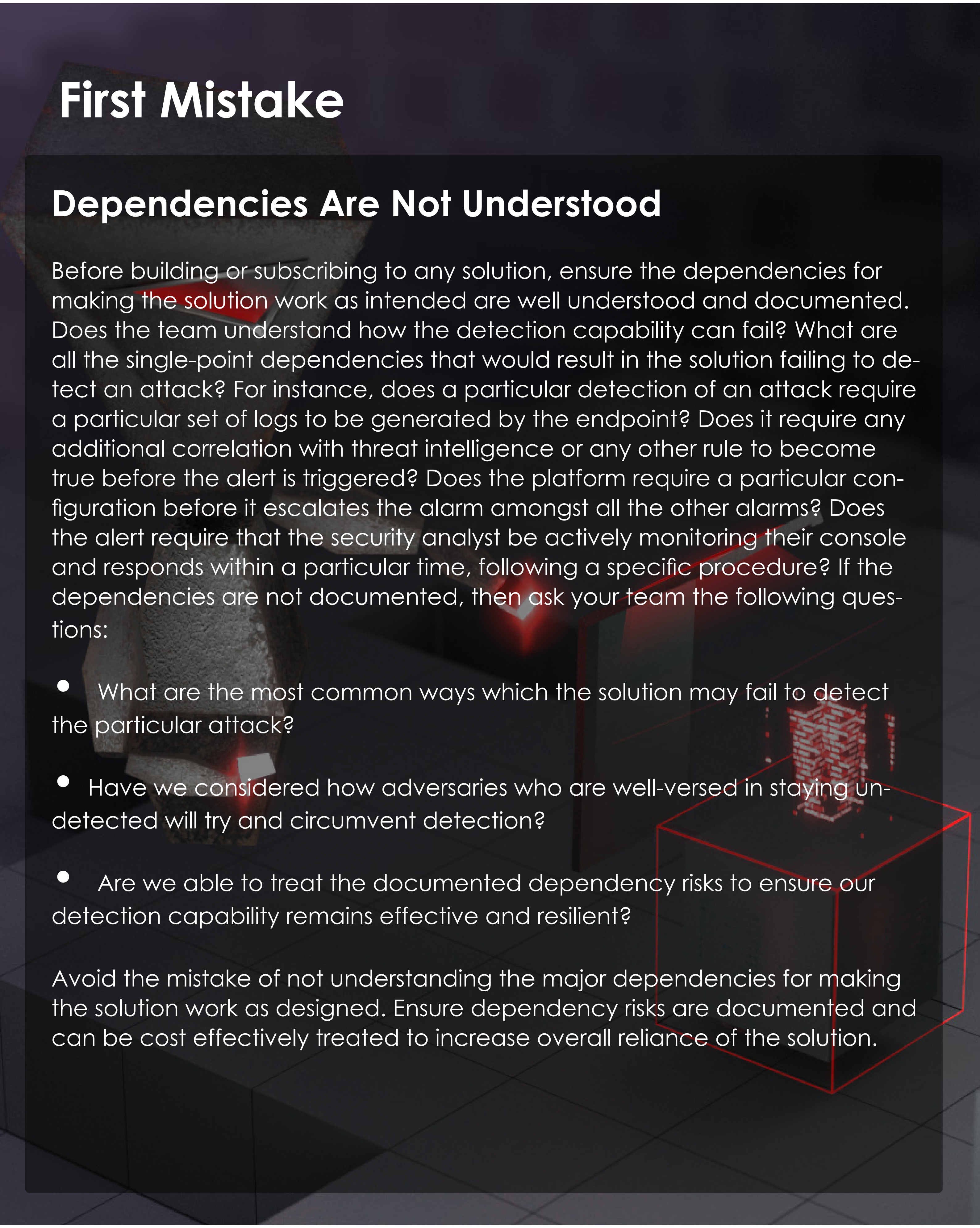


eclipse

Preface

As the ICT executive for your organisation, at some point you will be asked by your security team to sponsor a program with the objective to build or acquire capability to detect and respond to cyber threats.

In this paper, we will explore the top 5 mistakes to avoid when deciding whether to sponsor the threat detection program and the questions you should ask your team as part of due diligence.



First Mistake

Dependencies Are Not Understood

Before building or subscribing to any solution, ensure the dependencies for making the solution work as intended are well understood and documented. Does the team understand how the detection capability can fail? What are all the single-point dependencies that would result in the solution failing to detect an attack? For instance, does a particular detection of an attack require a particular set of logs to be generated by the endpoint? Does it require any additional correlation with threat intelligence or any other rule to become true before the alert is triggered? Does the platform require a particular configuration before it escalates the alarm amongst all the other alarms? Does the alert require that the security analyst be actively monitoring their console and responds within a particular time, following a specific procedure? If the dependencies are not documented, then ask your team the following questions:

- What are the most common ways which the solution may fail to detect the particular attack?

- Have we considered how adversaries who are well-versed in staying undetected will try and circumvent detection?

- Are we able to treat the documented dependency risks to ensure our detection capability remains effective and resilient?

Avoid the mistake of not understanding the major dependencies for making the solution work as designed. Ensure dependency risks are documented and can be cost effectively treated to increase overall reliance of the solution.

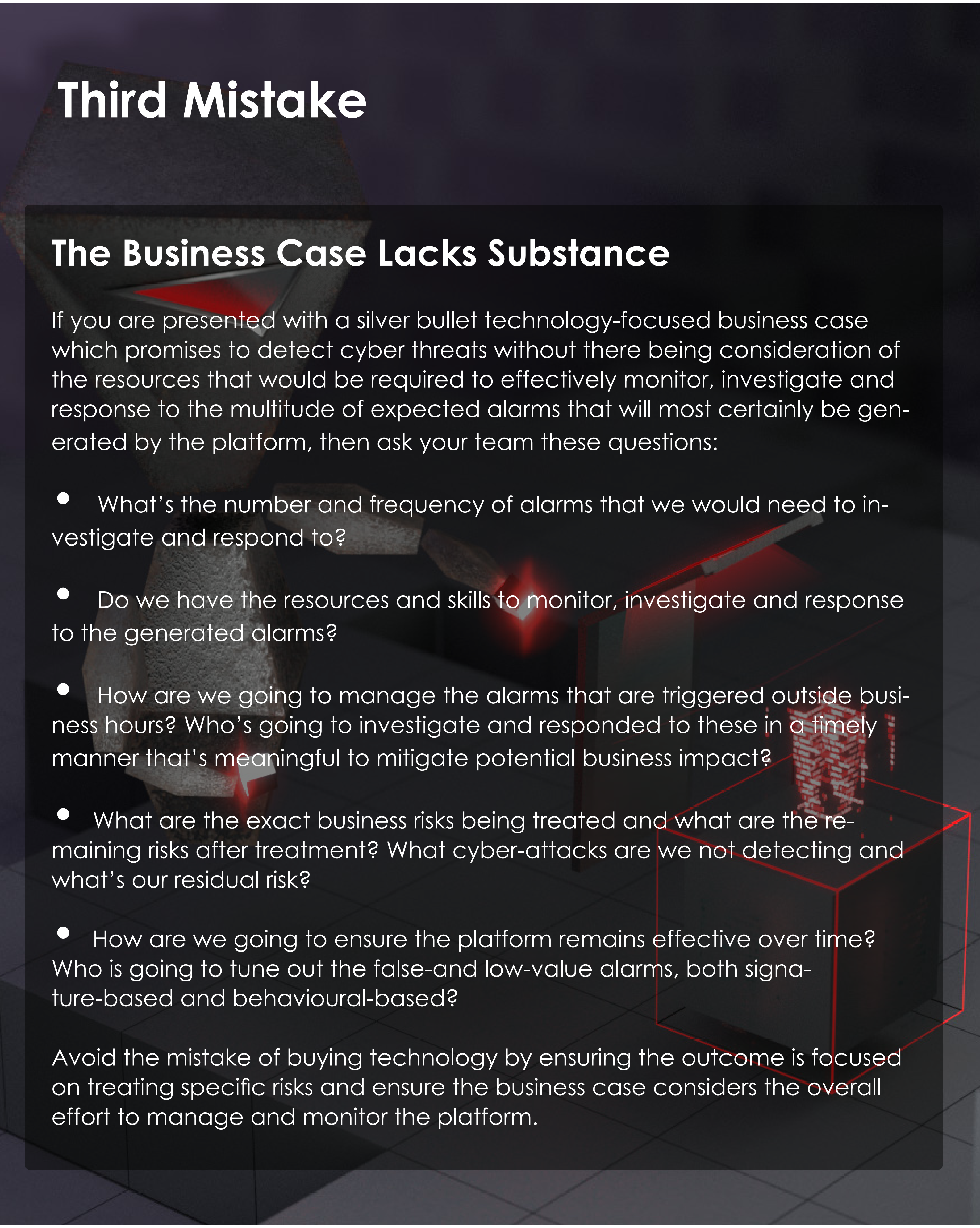
Second Mistake

There’s Too Much Dependency on Skills And Availability Of Resources

Following on from the major dependencies not being clearly understood, the greatest dependency is always going to be people, their skills, knowledge, availability and capacity to effectively manage the platform. If you have a key-person risk for maintaining the platform, ask your team the following questions:

- How often does the platform need to be maintained to ensure it operates as expected?
- How often does the platform need to be maintained to ensure it remains effective in its capacity to detect the particular business risks identified?
- What are the particular technical skills required to maintain and monitor the platform?
- How will environmental and specific configurations be documented for the next person?

Avoid the mistake of building a platform or subscribing to a service which depends on a key person to operate and manage. Ensure you have a team of people who are cross trained to manage and ovperate the platform. If there is no business case to have more than a single person who manages and operates the platform, then consider outsourcing these functions to a service provider if the business case can be justified.



Third Mistake

The Business Case Lacks Substance

If you are presented with a silver bullet technology-focused business case which promises to detect cyber threats without there being consideration of the resources that would be required to effectively monitor, investigate and response to the multitude of expected alarms that will most certainly be generated by the platform, then ask your team these questions:

- What's the number and frequency of alarms that we would need to investigate and respond to?

- Do we have the resources and skills to monitor, investigate and response to the generated alarms?

- How are we going to manage the alarms that are triggered outside business hours? Who's going to investigate and responded to these in a timely manner that's meaningful to mitigate potential business impact?

- What are the exact business risks being treated and what are the remaining risks after treatment? What cyber-attacks are we not detecting and what's our residual risk?

- How are we going to ensure the platform remains effective over time? Who is going to tune out the false-and low-value alarms, both signature-based and behavioural-based?

Avoid the mistake of buying technology by ensuring the outcome is focused on treating specific risks and ensure the business case considers the overall effort to manage and monitor the platform.

Fourth Mistake

The Focus Is On Detecting Cyber-Attacks Instead Of Detecting Compromised Hosts

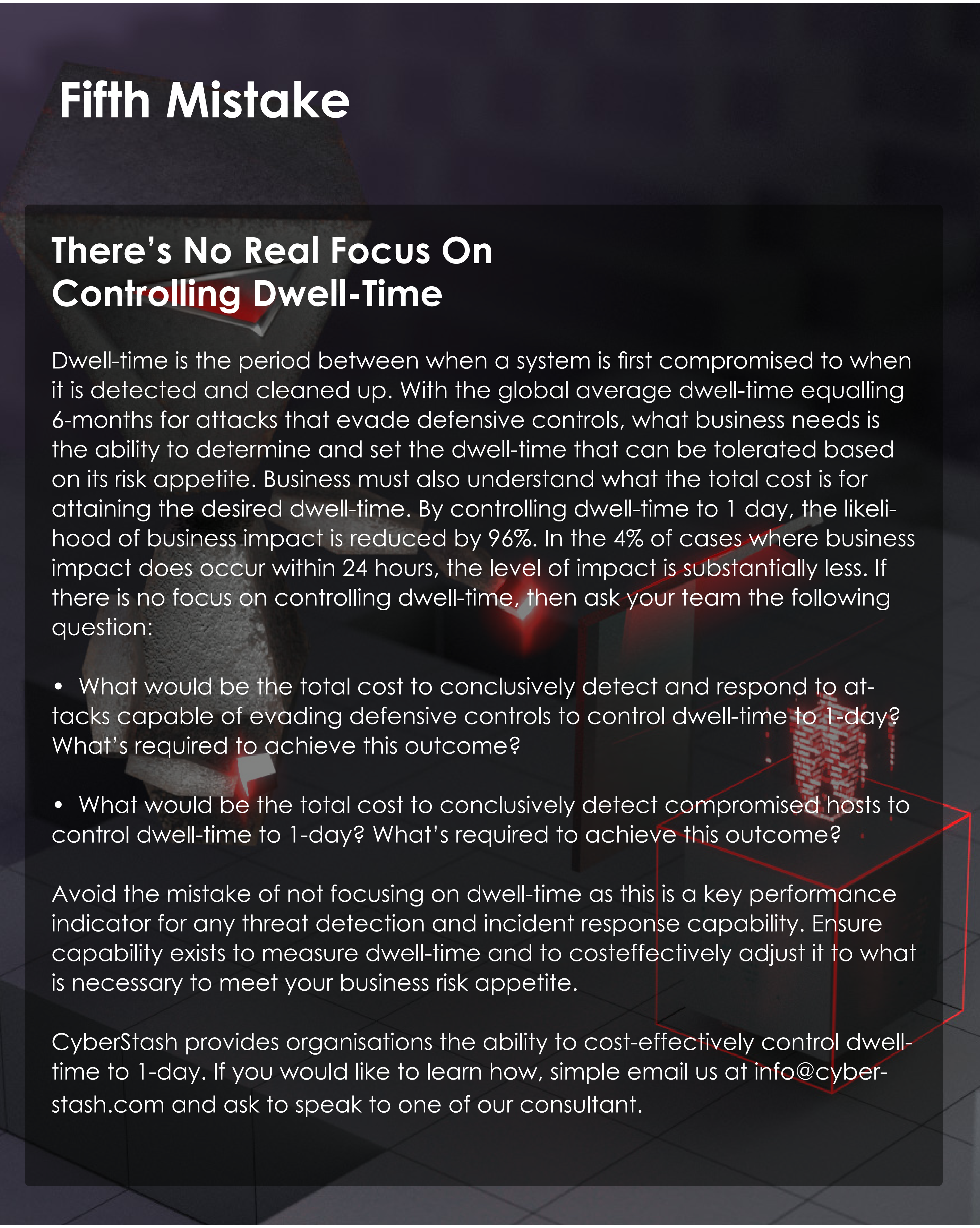
Advanced attacks are in nature designed to bypass real-time protection and detection engines such as those used by EDR, EPP, XDR, UBEA, SIEM, TI, ML and AI-based solutions If the overall solution proposed is based around detecting attacks by detecting all the potential different combination of tactics and techniques on the way in, whether these are based on detecting patterns or behaviours, then ask your team the following questions:

- What is our post-breach detection strategy assuming specific attack patterns or behaviours are not detected? How are we going to detect the compromise before these lead to business impact?

- What level of assurance can be provided that the detection mechanisms cannot be circumvented?

Avoid the mistake of depending too heavily on real-time detection engines by ensuring your team has a post-breach strategy that detects compromised systems in a meaningful time. Remember that most attacks do not lead to compromise and trying to therefore detect attacks on their way in, is not a cost-effective strategy.

Another way to think about this is this. If you are depending on the same tools and methods that allowed the breach to occur in the first place, to then detect the compromise, your overall security capability is not truly independent.



Fifth Mistake

There’s No Real Focus On Controlling Dwell-Time

Dwell-time is the period between when a system is first compromised to when it is detected and cleaned up. With the global average dwell-time equalling 6-months for attacks that evade defensive controls, what business needs is the ability to determine and set the dwell-time that can be tolerated based on its risk appetite. Business must also understand what the total cost is for attaining the desired dwell-time. By controlling dwell-time to 1 day, the likelihood of business impact is reduced by 96%. In the 4% of cases where business impact does occur within 24 hours, the level of impact is substantially less. If there is no focus on controlling dwell-time, then ask your team the following question:

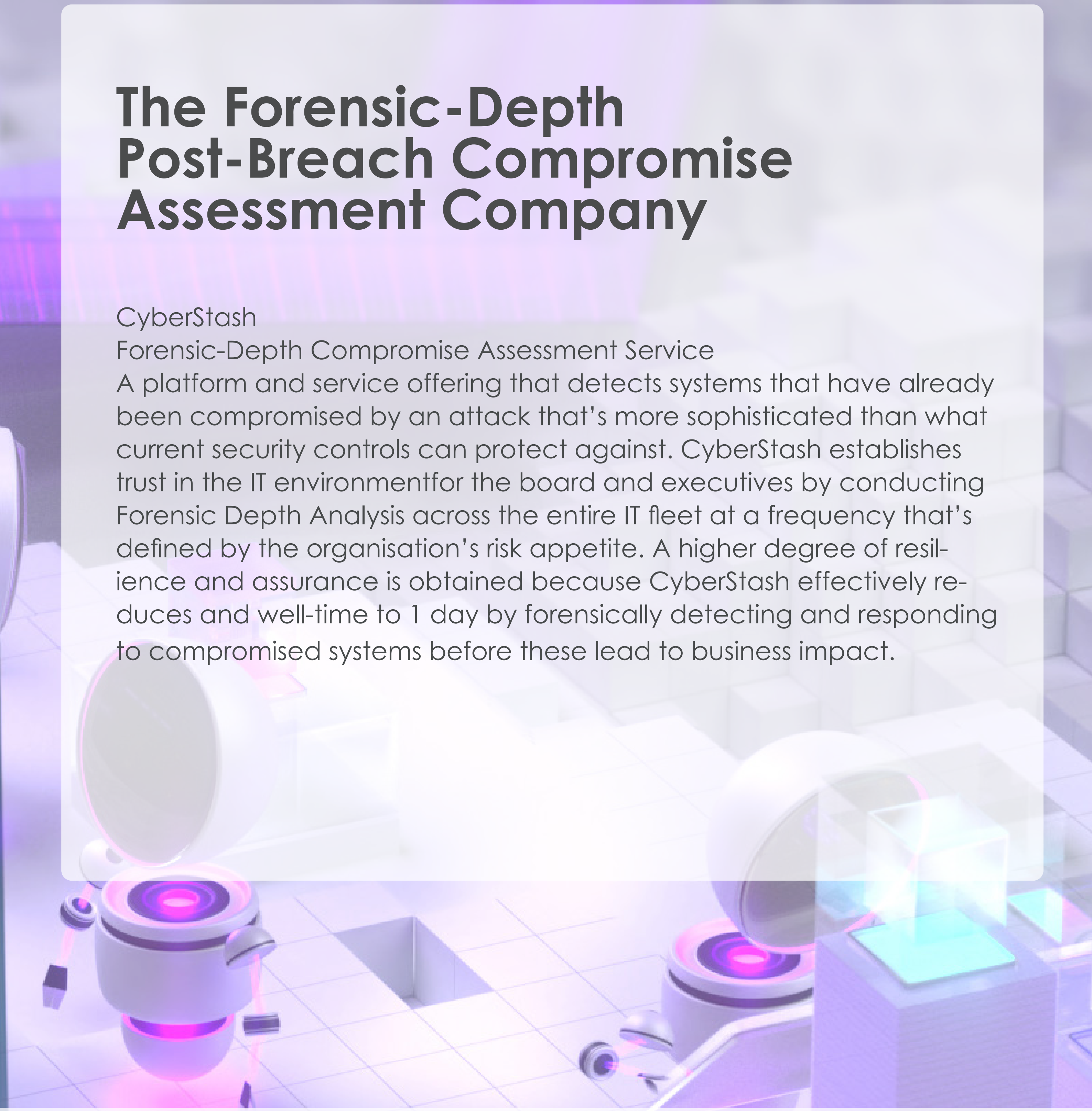
- What would be the total cost to conclusively detect and respond to attacks capable of evading defensive controls to control dwell-time to 1-day? What’s required to achieve this outcome?

- What would be the total cost to conclusively detect compromised hosts to control dwell-time to 1-day? What’s required to achieve this outcome?

Avoid the mistake of not focusing on dwell-time as this is a key performance indicator for any threat detection and incident response capability. Ensure capability exists to measure dwell-time and to costeffectively adjust it to what is necessary to meet your business risk appetite.

CyberStash provides organisations the ability to cost-effectively control dwell-time to 1-day. If you would like to learn how, simple email us at info@cyberstash.com and ask to speak to one of our consultant.

The Forensic-Depth Post-Breach Compromise Assessment Company



CyberStash
Forensic-Depth Compromise Assessment Service
A platform and service offering that detects systems that have already been compromised by an attack that's more sophisticated than what current security controls can protect against. CyberStash establishes trust in the IT environmentfor the board and executives by conducting Forensic Depth Analysis across the entire IT fleet at a frequency that's defined by the organisation's risk appetite. A higher degree of resilience and assurance is obtained because CyberStash effectively reduces and well-time to 1 day by forensically detecting and responding to compromised systems before these lead to business impact.

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

Want to run a trial?
Reach Out To Cyberstash
For More information.