Cyber Security Posture Assessment (CSPA)

cloud business

Cyber Security Posture Assessment Overview

Credibility and trust play a critical role in determining how organisations choose their security providers or partners. This is elevated in importance as the costs of failure in the effectiveness of security controls are increasing rapidly, both in terms of lost reputation and damage to productivity and profitability.

As the Global community grapples with the unprecedented events of 2020 and 2021, cyber criminals have remained true to form and capitalised on the chaos that has ensued.

Now, more than ever, organisations need to collaborate with their partners to accelerate the effectiveness of their Cyber Security defences.

As a value-add to our customers, we conduct a Cyber Security Posture Analysis (CSPA) of their ICT infrastructure to determine the current level of threat activity and risk level/vulnerability exposure. This assists us in identifying priority areas that may need to be addressed.

In order to establish trust with our customers, it is imperative that we build our relationship on a foundation of transparency. Therefore, identifying potential gaps in the environment allows us to jointly embark on a path of remediation and continuous improvement, reducing the potential of any breaches going forward.

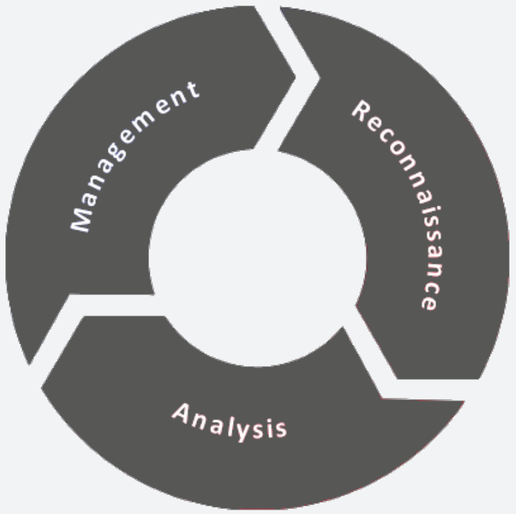
The CSPA is completely independent and provides an overview of the adequacy of the current security controls deployed in the IT environment. We will consider not only the technical controls in the environment, but also the level of compliance required by industry, relevant regulatory authorities & international best practices and evaluate how the organisation compares against these.

The analysis consists of two parts, a physical Technology Controls assessment and a Policies & Processes assessment, and is performed over 10 to 15 days. During the Technology Controls assessment, we will focus on assessing the customer's environment for targeted attacks as well as possible known threats prevalent in the environment, analyse network traffic and identify any possible privileged account security challenges, amongst others. The Policies & Processes assessment is performed in line with the International Organisation for Standards (ISO) 27000 controls and is delivered as an interactive questionnaire.

The combination of these two assessments allows us to create a "perception vs reality" viewpoint, which is then delivered to the customer in both a report and presentation format. This will allow each customer to consider the results of the analysis within the context of their specific business and ultimately allows for a more informed decision-making process when it comes to improving the overall security posture of the organisation.

Phase 1 – Policies & processes assessment

The Policies & Processes assessment will be delivered through an interactive meeting where a questionnaire will be completed. The purpose of this questionnaire is to provide a conceptual view of governance, risk, compliance, people, process and technology towards a view of establishing gaps in the IT security posture. The structure consists of three distinct phases, depicted in the following diagram.



The objective of the first phase (Reconnaissance) is to establish a high-level understanding of the customers' overall business, Information Technology (IT) and security landscape. During the Analysis phase, the findings are mapped against best practice security frameworks and standards, e.g. ISO 27001 and the NIST Cyber Security Framework (CSF).

Finally, the Management phase provides an overall report with high-level recommendations and an improvement plan.

The following topics are covered during the assessment:

- High level business landscape and related objectives and services
- The impact of information confidentiality, integrity and availability compromise of the in scope applications
- Non-technical Cyber Security components:
  - Governance o Risk
  - Compliance o People
  - Processes
- Technical Cyber Security and ICT components:
  - Perimeter Network Infrastructure
  - Internal Network Infrastructure
  - Cloud
  - Critical Applications (x3)
  - Endpoints, including mobile and smart devices
  - Supporting Security Infrastructure & Management

Speak to our team to explore how we can support your organisation.

Call:
+44 (0) 8456 808538
or Email:
hello@cloudbusiness.com
Website:
www.cloudbusiness.com

Phase 2 – Technology controls assessment

The Technology Controls assessment is delivered through the CSPA appliance, which is available for the duration of the assessment. This appliance is preinstalled with all the software needed for the assessment and configured with the necessary network settings, which are provided by the Customer. The software will include an IPS, Vulnerability Scanning software, Big Data database and Privileged User Credential scanning software, amongst other tools. All these appliances are running in Linux containers which are hardened to prevent any unauthorized access.

This phase endeavours to provide a view of the IT security posture from the "inside out", by assessing the current environment on a technical level. The following prerequisites must be met for successful delivery of the assessment:

- A detailed network diagram must be provided to assist with planning the correct placement of the assessment appliance
- A kick-off telephone call must be scheduled between the client and the assigned technical resource performing the assessment. This call will be used to discuss and agree on the placement of the device and make sure all of the client's questions are answered
- A Mirror port on the main switch in the client environment. It is best to see traffic before it gets to the proxy, this will allow us to analyse the network for any anomalous traffic.
- A read-only Active Directory account, which will allow us access to review privileged accounts.
- Up to 5 IP addresses for the different assessment tools, as well as internet access for the device.
- If any change control is required, the client will take responsibility for this process.

The CSPA device consists of various carefully crafted scanning technologies, and some will be discussed here. It will scan assets within predefined maintenance windows for configuration and software installed on the customer assets and look at the Vulnerabilities and Risks associated with these configurations on the assets. The CSPA device will also analyse network traffic (analyser) and provide insights to the metrics generated. The analyser has very powerful analytical capabilities and will give insights to DNS filtration, Bot-net, Ransom-ware and many more activities occurring on the network. We are also able to see what countries and or individuals are showing an interest in your environment and to what extent.

The CSPA device ingests information from the customer site (rich set of plug-ins available) which can be used as a metric or as enrichment to other data. The devices' capability is enhanced through the use of high-speed high-volume reporting technology coupled with workflow integration that allows us to obtain insight to trend over time activities on the network.

With these elements in hand, we are able to look at the true near real-time Risk view of the organisation, as we have the assets identified and we know what their weaknesses are. In addition, we have insight to what is happening on the network at any particular time and where this occurred. This allows us to see where the attack vectors are in the environment. This capability not only shines a light on the exploitable risks in the environment, but can also help to identify prioritising of remediation efforts thus saving time and money as it allows the customer to apply effort where it counts.

The management report will be completed once both phases have been completed. On report completion the hard drive is over written with disk wiping software called disk wipe https://www.diskwipe.org/. No data is removed from the customer site, as all processing activity is conducted on the device.

Contact Cloud Business

Call:
+44 (0) 8456 808538
or Email:
hello@cloudbusiness.com

Or book a discovery call to discuss your requirements:

Website:
www.cloudbusiness.com

cloud business