CYBER CITADEL TESTING OFFER

No critical finding, no charge

Cyber Citadel are international vulnerability and penetration testing experts – offering the services of highly capable, innovative and accredited security analysts, architects and penetration testers. Instead of automated scans, we take the manual, human-led approach and test for business logic and vulnerabilities that would otherwise be missed.

Cyber Citadel believe that given enough time, we will always uncover a critical finding. We are so confident of this claim, we offer our penetration testing service on a 'no critical finding, no charge' basis.

WE ARE LOGISTICS EXPERTS

Cyber attacks are becoming increasingly well coordinated and extremely sophisticated. During the Covid-19 pandemic, the logistics industry has unfortunately taken centre stage in the world of cybercriminal attacks. With the growing complexity in networks, it is becoming infeasible to protect all parts of a network all the time from within.

Yet continuous network security is paramount, particularly in a real-time business such as logistics. If an attacker decides to encrypt all your files, and destroy or corrupt your backups, then your business will at a minimum suffer a reputational crisis, likely losing customers to competitors, but could also be completely crippled and unable to continue functioning.

> *You need to be right 100% of the time – the attacker just needs one thing to go their way: a simple misconfiguration, a successful phishing email or an unpatched system.*

Cyber Citadel has worked for many years with logistics software and logistics providers and understands the unique problems that the industry has with its complex mix of systems talking to multiple third parties and integration with customers, agents, partners, wholesalers, transport providers, air/sea carriers and Government. Such complexity leaves the potential attack surface much wider than in many other industries. Having direct and frequent experience with these types of issues makes Cyber Citadel faster than other more generalist cybersecurity firms. Our operatives' specialist industry knowledge not only results in more complete results for you, but at a lower cost.

In Cyber Citadel's experience, many companies feel satisfied that they are secure because they have had testing performed and no critical vulnerability was found. Let our specialist team confirm that peace of mind with our 'no critical finding, no charge' offer.

Example Critical Finding Notification

S #	Hostname	Critical	High	Medium	Low/Info
1	cargo.example.com	1	-	-	-

E1 – Arbitrary File Upload Leading to Remote Code Execution (RCE)

Affected Hosts: cargo.example.com

Level: Critical

Impact: Severe **Likelihood: High**

Explanation

It is possible to upload malicious scripts and files on the web server and possible to run remote commands on the web server. This usually means complete compromise of the server and its contents due to insecure web application programming or configuration. [etc]

[Proof of concept/evidence and solution/remedial work required will appear here in the final report]

HOW OUR TESTING OFFER WORKS

▸ Step 1 – Provide some basic network information

Using this background information and some low-level credentials, we will attempt to completely take over your systems, providing a real-world example of what happens if someone actually gets into your network.

▸ Step 2 – Set a start date

We will agree a time period within which the 'first critical' testing will take place. This normally takes 1–4 days and does not interfere with your day-to-day operations.

▸ Step 3 – Receive notification of critical finding

After our initial test, we will provide you with a description of the critical finding(s), along with evidence from your system and an explanation of the risk (see example above).

▸ Step 4 – Agree to a full penetration test

After the first critical finding, we will recommend a full penetration test. This provides you with a full report containing a list of additional findings, evidence of the vulnerabilities, an assessment of the risk of each, and the solution/remedial work required. The full report includes an easy-to-understand Executive Summary that can be shared with boards and key stakeholders. A complete penetration test will generally take around 5–10 days.

LET US FIND YOUR VULNERABILITIES BEFORE THE BAD GUYS DO

FTA FREIGHT & TRADE ALLIANCE

In order to urgently address the heightened risk we are seeing in 2022, **Cyber Citadel have partnered with FTA** to provide security assistance that is measurable and brings results. Even if you are confident in your network cyber security and sure that you have no critical vulnerabilities, you should take up this offer. You will not be charged if we find nothing. But if we do identify vulnerabilities, this will be the most valuable exercise you have undertaken. **The risk is real. Get in touch now.**

www.cybercitadel.com

For more information contact Jonathan Sharrock:
info@cybercitadel.com | +61 2 8318 0290 | +61 466 533 533