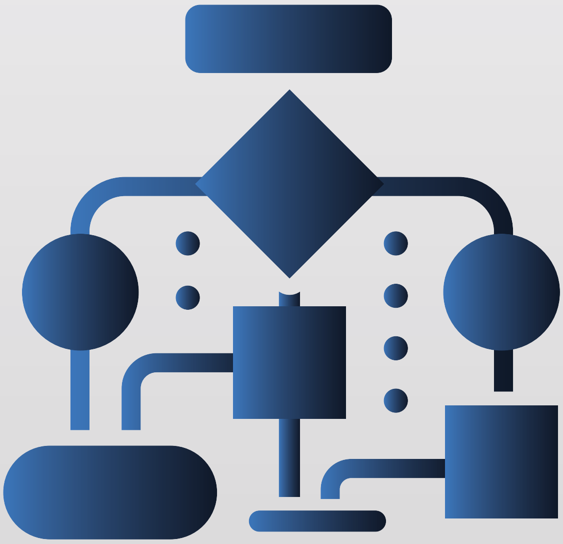
CASE STUDY

ENDIDA
NEXT GENERATION CYBER DEFENCE

VULNERABLE DOES NOT ALWAYS MEAN EXPLOITABLE

AN INSIGHT INTO CYBERSECURITY PRIORITISATION



GET IN TOUCH TO FIND OUT HOW WE CAN HELP YOU TODAY

endida.com | 0238 2180 428 | info@endida.com

THE TYPICAL APPROACH

Ever wondered how much of your time and effort is being wasted fixing things that don't actually matter?

Vulnerability scanners, and installed agents will alert you of potential vulnerabilities and breaches. You receive a list, or a notification, and you respond – correct?

You may be surprised to hear that a large majority of all vulnerabilities are unexploitable. According to data compiled by Kenna in 2020, only 2.7% of the vulnerabilities found appeared to be exploitable and only 0.4% of those vulnerabilities were actually observed to be exploited at all.[1]

The prioritisation of these low-risk or no-risk vulnerabilities alongside, or even above the truly exploitable vulnerabilities can actually cause an organisation's security posture to suffer. It takes significant time and co-ordination to find the asset owners, bring them up to speed on the issue, prepare downtime for the asset, remediate the issue and then confirm that the issue is remediated. Meanwhile, more critical vulnerabilities are waiting in line for their turn to be remediated.

If you can't properly prioritise, you will never secure your network.

A client came with the goal of validating an outsourced company they were using for manual Pen Testing. The outsourced company had sold them an annual test for the organisation's network environment. Endida's AI, Autonomous Pen Test was then used to assess the network and compare the results, to ensure it was a real Pen Test.

We found that proposed manual Pen Test they paid for was in fact just a vulnerability scan. Overleaf find out how our results compared to the outsource, so called Pen Test company.

[1] https://www.kennaresearch.com/a-decade-of-insights/

GET IN TOUCH TO FIND OUT HOW WE CAN HELP YOU TODAY

endida.com | 0238 2180 428 | info@endida.com

VULNERABILITY SCAN VS ENDIDA PEN TEST

Comparison	Vulnerability Scan	Endida Pen Test
Coverage	Assessed only -600 hosts	✓ Assessed 3,644 hosts
Accuracy	Nearly 80% (22 of 28) of critical findings are either not exploitable, or are extremely impractical to exploit Several critical/high vulnerabilities not detected (IPMI, guessable root access to databases, credentials/ keys stored in an open share.... all of which Endida's Pen Test found)	✓ Critical/High exploitable findings discovered on many more hosts (BlueKeep, Eternal Blue, etc.) ✓ Several additional critical/high exploitable findings found (IPMI, GhostCat, Cisco Smart Install, etc.) ✓ Surfaced contents of several large SMB/NFS shares
Valid critical findings	5 of 28 issues marked critical are exploitable 1 of 28 (VMware) may be a false positive	✓ Automatically identified 4 of 5 exploitable issues found by the MSSP ✓ VMWare issue appears to be a false positive or was remediated between ops
BlueKeep (leads to RCE)	Found on 1 host	✓ Found on 12 hosts
External Blue (leads to RCE)	Found on 2 hosts	✓ Found on 14 hosts
'Guest' access to CIFS shares	Found 4 file shares	✓ Found 14 file shares, over 2 million files surfaced, likely containing sensitive data (multiple SSH/AWS keys found)
Additional critical/high weaknesses	NONE	✓ Achieved root-access to 3 database servers, pilfered hashes from 9 hosts with vulnerable IPMI configurations

GET IN TOUCH TO FIND OUT HOW WE CAN HELP YOU TODAY

endida.com | 0238 2180 428 | info@endida.com

WHY COVERAGE AND ACCURACY MATTER

The hardest part of cyber security is deciding what NOT to fix because of limited time and resources

VULNERABILITY SCANS CREATE AN INCOMPLETE SNAPHOT

Fixing 79% of the critical issues highlighted in the vulnerability report would have been an inefficient use of time and effort. These so-called 'critical issues' did not have exploits, were blindly assumed due to poor enumeration, or the conditions for exploitability were extremely unlikely.

Meanwhile, only one host was identified to be vulnerable to BlueKeep, while the Endida Pen Test found an additional 11. We also proved three additional critical/high weaknesses, including easily guessable root access to a database server.

- ⊗ No exploits exist, or conditions to exploit are extremely unlikely, for 22 out of 28 of the vulnerabilty scan's critical findings
- ⊗ Partial coverage leads to missed critical findings
- ⊗ Poor enumeration leads to blind spots and incomplete fingerprinting – port scans are not enough!

When the noise is removed, the critical findings are revealed.

GET IN TOUCH TO FIND OUT HOW WE CAN HELP YOU TODAY

endida.com | 0238 2180 428 | info@endida.com

THE ENDIDA DIFFERENCE

Thinking like an attacker gives you a distinct advantage as you devise a defensive strategy

The attacker's perspective asks:

- What is an attacker interested in doing or achieving?
- What methods are realistically at their disposal?
- What things about your environment makes achieving their intentions possible, or even easy?

We believe that these questions can only be answered by an 'attacker-mindset' pen test, which should be performed frequently on your entire environment so risks do not accrue, and should produce findings that guide your remediation actions with a heavy bias towards efficiency and return on investment.

Endida delivers these outcomes through an autonomous penetration testing-as-a-service platform. Endida's on-demand, self-service platform is safe to run in production and requires no persistent or credentialed agents.

Within our Portal, we provide the following supporting information for every weakness found:

- ✓ Path followed to identify/discover the weakness.
- ✓ Proof of exploitability of the weakness.
- ✓ Context and severity of the finding, which can be used to determine business impact.
- ✓ Fix action report you can follow to remediate the weaknesses.

"For me, the biggest benefit is the attack path identification and actual prioritisation of the vulnerabilities. Other tools simply pull the CVE value, and we get hundreds of criticals and highs."

GET IN TOUCH TO FIND OUT HOW WE CAN HELP YOU TODAY

endida.com | 0238 2180 428 | info@endida.com

THE FUTURE STATE

Overall, the comparison between the client's original report and the Endida report shows that our Pen Test provides broader coverage, proves exploitability, contextualises weaknesses, and provides the defensive team with the information they need to fix what matters.

Work with this client exemplifies the need for a proactive security posture that includes continuous assessment, so you can catch up, keep up and even stay ahead.

CONTINUOUS, AUTONOMOUS PEN TESTING WITH ENDIDA

- Identify new exploitable attack vectors.
- Auto open/track/close tickets with proof.
- Prioritise remediations based on impact and effort.
- Verify problems have been fixed.
- Validate security controls are effective.
- Benchmark posture against best practices.
- Report posture to board and regulators.

PROACTIVE SECURITY

- Detect beacons, lateral movements and exfil
- Disrupt kill chain and conduct forensics

REACTIVE SECURITY

✓ CATCH UP

Identify exploitable attack paths that must be fixed immediately, significantly reducing the opportunities for exploitation, sensitive data exposure, elevated privileges or remote code execution.

Your first Pen Test will provide this insight and minimise the time spent dealing with false positives.

✓ KEEP UP

Establish a purple team culture to find exploitable problems, fix them and then verify that the problems no longer exist.

You can run multiple Pen Tests per week – our licences give you unlimited access.

Use the compare feature to power your security standups.

✓ STAY AHEAD

Continuously verify your security controls tools, processes and policies by measuring and optimising your detection, remediation and compliance response times.

Use our reports to show your leadership where you stand. Not just a compliance checkbox; this is effective security.

GET IN TOUCH TO FIND OUT HOW WE CAN HELP YOU TODAY

endida.com | 0238 2180 428 | info@endida.com