# An Integrated Approach to Enterprise Security – The Bluedog Proprietary Method

A bluedog Whitepaper

bluedog
SECURITY MONITORING

## Executive Summary

What vulnerability did you deploy today? Can you be sure that everything you and your staff clicked on, installed or browsed was 100% safe? No one can.

90% of data breaches[1] are caused by human factors. This doesn't mean that 90% of employees are set to expose company data to attackers. Most often (78% of cases[2]) they do it unwittingly – employees and remote sellers alike. Cyber security training for employees is a scarce commodity[3]. Even when it happens, it's basic and it doesn't even begin to cover all the facets of online threats.

To be fair, it couldn't. The cyber threats landscape is evolving continuously at an alarming pace[4]. The rise of remote working fueled by the COVID-19 pandemic prompted a sudden move to the cloud for companies of all sizes[5]. But this move was done hastily, with little time to vet cloud providers and cloud solution providers.

Remember the Zoom security incident? More than half a million credentials were exposed to attackers. And that was just the beginning of the storm[6].

All in all, online security is murky and threats continue to diversify and grow. This is why companies of all sizes need both a proactive and a reactive approach to them. Some industries already have strict regulations for tackling cyber security.

This whitepaper will explore one of the most common cybersecurity tools: penetration testing. It will reveal its pros, cons, and limitation. Proper security can't rely on a single solution, though, so this whitepaper will emphasize why a fake sense of security is very dangerous and what you can do to avoid

---

[1] https://www.techradar.com/news/90-percent-of-data-breaches-are-caused-by-human-error, retrieved February 2021

[2] https://www.securitymagazine.com/articles/91758-of-it-leaders-say-insider-data-breaches-are-a-major-concern, retrieved February 2021

[3] https://www.statista.com/statistics/949179/united-states-training-frequency-security-awareness/, retrieved February 2021

[4] https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/, retrieved February 2021

[5] https://www.forbes.com/sites/forbestechcouncil/2020/06/16/the-cloud-is-the-backbone-of-remote-work/?sh=79f58fc4dc99, retrieved February 2021

[6] https://www.tomsguide.com/news/zoom-security-privacy-woes, retrieved February 2021

falling into this trap. Finally, you will learn how Bluedog Security Monitoring tackles enterprise security in an integrated and affordable manner.

# Contents

# Penetration Testing: Automated, Manual, or Both?

Things move *fast* in cybersecurity. There is no other way if you want to survive the perfect storms of attacks that get more and more sophisticated by the minute.

A couple of years ago, the rule of thumb for security surveys was pretty clear: do automated vulnerability assessment to get the best-known issues out of the way. Then move on to penetration testing to "catch" the more complicated issues. And, ideally, do this manually.

The conclusion of these recommendations was pretty clear: you can automate a part of the process (vulnerability assessment) but you need human-led penetration testing techniques to ensure a satisfactory level of security.

However, manual penetration testing was a bit of a misnomer in this context: yes, there was a "human factor" involved. But their involvement wasn't as comprehensive as service descriptions led you to believe. In most cases, manual penetration testing consisted of testers manually verifying the issues revealed by the automated vulnerability scanners, with a focus on false positives and false negatives.

Was this a necessary phase? Absolutely! But the technology has evolved. Today, automated pen testing can take care of that, though artificial intelligence and machine learning. In a nutshell, this means that automated pen testing tools can be "trained" to spot issues that required human testers not so long ago. But we'll get to that in a while.

Does this mean that there is no more use for manual penetration testing in today's cybersecurity industry? Not really.

Manual testing is still a necessary phase that helps you:

- Validate your issues and
- Do business logic bypasses
- Do authorization bypasses
- Do authentication bypasses

These are just a few examples of issues that are very hard to find and exploit with automated pen testing.

Thus, you need both automated and manual penetration testing to have a comprehensive overview of your vulnerabilities and of your security priorities.

But a once-a-year pen test is by no means enough. Quite the opposite. We'll discuss this in the following chapter.

## The "False Security Trap"

At Bluedog, we generally applaud the increasing compliance regulations in sensitive industries, like the financial or the health industry. HIPAA[7], and PCI DSS[8] have compliance regulations that require extra attention to security.

While not all these explicitly ask for manual penetration testing (save for PCI DSS, which explicitly requires it every 180 days), a close read of their guidebook makes it clear than pen testing is the fastest, easiest, and safest way to achieve compliance.

But does compliance always mean better security?

Not quite.

This is one of the pet peeves of the cybersecurity industry: a company in a sensitive field will do the mandated yearly pen test and consider their network or their applications secure. But this is a trap.

A yearly pen test isn't enough. Cyber criminals move much faster than this. Wait a year between testing your digital assets and you will have given attackers thousands of widely open gateways to breach your applications or your network.

In a way, this is perfectly understandable: penetration testing is expensive. In fact, penetration testing *was* expensive. Hiring a team of security specialists to do manual checks on your assets is bound to cost an arm and a leg. So you couldn't possibly do it every month.

Thus, companies (especially SMEs) would do an annual pen test and hope for the best. In some of the more fortunate cases, vulnerability scans happened more often – once a month.

But again, this is nowhere near enough. In the current cybersecurity landscape a monthly vulnerability scan and a monthly pen test are mandatory to reach security maturity.

Are they enough, though?

---

[7] https://www.hhs.gov/hipaa/index.html, retrieved February 2021
[8] https://www.pcisecuritystandards.org/pci_security/, retrieved February 2021

Not at all! At Bluedog, we have a mantra: “security is about people”. While we love automation and automated security tools, we know that they all have their limits. Vulnerability scans and pen tests are a great first step towards security maturity. But they are just a piece of the puzzle.

The following chapter details our integrated approach to security and how we combine automation with human-led techniques to achieve security maturity.

## The Bluedog Security Monitoring Approach to Integrated and Affordable Security

In the previous chapter we spoke about false security and about how monthly pen tests are hard to perform because of their prohibitive costs. Our integrated approach takes care of the cost issue and helps mitigate risks faster (a crucial attribute in security!) and more efficiently.

Let's talk about it in detail.

# Automated VAPT – The Solution for Keeping Costs and Vulnerabilities under Control

Integrating vulnerability assessment and penetration testing into a single solution – VAPT – offers the best of both worlds. Through this service, you can easily get to know all your business logic vulnerabilities.

The major benefits of VAPT include:

- It's a fast solution, so you don't have to wait for months just to get a report that might be obsolete by the time you analyze it.
- It's very cost effective solution, thus countering the main drawback of pen testing – its steep price. Cost effectiveness also means that:
- It allows you to perform regular VAPT (once a month). In turn, this means that you can achieve security maturity and that you can stay on top of new vulnerabilities.
- It's better for achieving compliance.

Briefly put, our automated VAPT approach offers 12 times the data a manual approach can obtain and costs one tenth of a manual test.

Why is this such an efficient tactic? It's all about the methodology.

# The Bluedog Penetration Testing Methodology

Before conducting the actual tests, there are two initial steps that have to be made:

- Prerequisites: everything we need to get the testing started.
- Scope setting

The latter is a very important stage. The pen testing team and the customer need to agree on what *exactly* they will be testing. You can end up testing too many assets (which will inherently lead to budget and deadline issues) or you can test fewer assets than you should (which will lead to undiscovered vulnerabilities).

The actual pen testing is comprised of five major steps:

1. **Passive and Active Reconnaissance**

Reconnaissance is the stage in which we gather all the information we need. The result is a bird's-eye-view of the company, the infrastructure, their applications, their employees, and more.

There are two major types of recon you can do during a pen test:

- Passive recon: an attempt to gain information about targeted computers and networks without actively engaging with the systems. In this stage, we typically use information that's freely available online. This phase can be referred to as *blueprinting,* since we're looking to get a map of the company's assets. Passive recon simulates what a real attacker might do. For instance, they may start by a trying to find devices within the IP address range belonging to a company. This indicates that they have the device deployed on their network. Since many IoT devices are vulnerable by default, identifying one or more on the network may give a hacker a good starting point for a future attack.
- Active recon: a way of finding out information that *does* leave a footprint. Things like the operating system used on a computer or the number of open ports may be uncovered during this attempt. While active recon is faster and more accurate than passive recon, it also leaves traces behind and, typically, the target can find out that an attack attempt happened. These tests are usually conducted through a proxy.

2. **Issue Validation**

After the first issues have been uncovered in the previous step, they must be validated. In other words, the blue team is responsible for making sure that the issues are not:

- False positives: certain vulnerabilities have been identified but they are not present in the scanned asset. If the false positives aren't identified as soon as possible, the result is unnecessary remediation work.
- False negatives: these are biggest peril of the entire process. A false negative is a vulnerability that *is* present in the scanned asset, but has not been identified. This risk can be mitigated by running multiple programs on the same asset or by doing regular VAPT with an ML-powered solution that has the ability to learn and adapt.

**3. Proof of Concept**

Our approach provides a proof of concept for each vulnerability. This eliminates the time needed to perform tedious manual testing.

Proof of concept attacks are the ultimate vulnerability validation. They prove that the vulnerability is real, which paves the way to finding the proper way to mitigate it.

**4. Stakeholder Management**

There are several types of stakeholders that may be interested in the findings of a penetration testing. The security team, the engineering team, the product team, and top and middle managers are just a few examples.

However, you may want to share only specific details of the report with each of them. Stakeholder management is the phase that ensures that everyone gets access to the information they need. More importantly, it ensures that no information is leaked to stakeholders who might pose a risk.

**5. Reporting**

The final report outlines the vulnerabilities discovered along with recommended remedial steps. This report acts as a roadmap for the security team. Its findings fuel the cybersecurity strategy of the entire company.

When regular tests are performed, these reports become even more important. You can follow the progress of the company and see how its security evolved from month to month.

What makes the Bluedog methodology highly effective are the built-in reiterations. Our tests rely on the premises that every new thing you learn helps you. If we compromise the network, we start from scratch.

The automated pen testing software picks up on failure and keeps on learning. The ML-powered algorithms help make it better and better with each iteration.

This is why frequent and regular testing is important. And this is why we've made it our mission to create an affordable solution to help all companies stay on top of their security issues, even if their budget is not huge.

As comprehensive as it gets, pen testing has its limitations too. The biggest one of all: it doesn't really account for the human factor. As industry reports show, 90% of attacks have a human-led cause.

This is where the last piece of our integrated approach to security comes into play:

# Red Teaming – the Human-Centric Approach to Cybersecurity

We tend to think about cyber-attacks as impersonal operations. The iconic image of the hacker in the black hoodie is what most of us have in mind.

And while successful attacks are nameless and faceless (no attacker wants their identity revealed), they are as human-led as it gets. This is why it's crucial to have a human-centric approach to cybersecurity.

Red teaming is also known as ethical hacking because it offers a way for independent security teams to test how well an organization would fare during a real-life attack. In other words, red teaming is a multi-layered, full-scope attack simulation designed to measure how well a company's people and networks, applications, and physical security controls can withstand an attack from a real-life adversary.

The VAPT approach mirrors the first steps a real attacker would take: scanning for open ports and other vulnerabilities to find an entry point into the network. But as soon as that open door is found, things tend to get more personal.

Red teaming is a "carte blanche" approach where everything goes. Social engineering, blackmail, asset seizing with the promise of the attack being revoked after a reward is paid – everything goes. A

thorough red teaming approach involves some of the most common tactics a real-life attackers would use.

There are three main directions that are followed (tested for vulnerabilities):

- People
- Processes
- Technology

Of course, red teaming doesn't have to happen as often as VAPT. But it is a crucial step to making sure that your security is up to par. Red teaming doesn't just reveal the vulnerabilities. It also offers remedial recommendations and a "playbook" on fixing the issues in the future.

All in all, it's important to note that there is no one-size-fits-all when it comes to cybersecurity. Every company has different needs and faces different types of attacks. This is why it's important to find a cybersecurity partner that can offer an adaptive approach and a methodology based on machine learning.

## About BlueDog Security Monitoring

Our goal is to provide businesses with a level of network protection typically only afforded by large corporations. We aim to bring high-quality technology, support, and service to the small to medium business, helping protect their business from cyber threats.

Our company is ISO27001 certified and growing quickly, through our simple and affordable end-to-end network monitoring solution. Recently voted one of the Top 10 cybersecurity start-ups of 2019 by Enterprise Security Magazine. Whether you are a small business, or an MSP or IT services reseller or distributor, get in touch and have a chat with us.

**20-22 Wenlock Road, London, N1 7GU**

**info@bluedogsec.com**

**+44 20 8819 6254**