Your Guide to Penetration Testing as a Service (PTaaS)

TROLL EYE SECURITY

Table of Content

TROLLEYE SECURITY

What is Penetration Testing as a Service?

PTaaS is a methodology for conducting continuous penetration testing of your IT systems and applications by mimicking the actions of hackers. We test your systems weekly to find their faults, so you can quickly identify and remediate vulnerabilities before they can be exploited by attackers.

TROLLEYE SECURITY

Our Process

Our process four PTaaS follows five steps, Pen Testers Assess, Pen Testers Prioritize, Client Acts, Pen Testers Re-Assess, and Processes Improve. This is a continuous process, with our pen test being performed on a weekly basis, drastically improving your organization's security posture.

Pen Testers Assess

- **Identify Assets**: Recognizing and categorizing valuable digital assets within an organization, ranging from databases to applications, is the initial critical step. This ensures that the most vital components are given the attention they warrant.
- **Scan**: Using advanced tools, the digital landscape is thoroughly scanned to find vulnerabilities or potential weak spots that could be exploited.
- **Test**: After vulnerabilities are spotted, rigorous testing is done to confirm them. This could involve attempting to exploit those vulnerabilities to determine their severity.
- **Analyze**: Post-testing, the results are analyzed in-depth, determining the nature of each vulnerability, its potential impact, and the risk associated with it.
- **Report**: An exhaustive report is written, presenting all findings, insights, and recommendations to the client, ensuring they are well-informed on their cybersecurity posture.

TROLLEYE SECURITY

Pen Testers Act & Prioritize

- **Assign Value**: To each identified vulnerability or threat, a specific value is assigned. This could be based on potential financial impact, data sensitivity, or other pertinent factors.
- **Gauge Exposure**: The exposure level of each vulnerability is evaluated, determining how accessible or exposed the vulnerability is to potential external threats.
- **Add Threat Context**: A broader context is provided by understanding the current threat landscape, recognizing the most imminent threats, and correlating them with the identified vulnerabilities.

TROLLEYE SECURITY

Client Acts

- **Accept Risk**: After a thorough analysis, some risks might be deemed acceptable based on their low impact or the high cost of remediation.
- **Mitigate**: For vulnerabilities deemed too risky, measures are taken to lessen their impact or likelihood.
- **Remediate**: Actions are implemented to correct or resolve identified vulnerabilities, ensuring they can't be exploited in the future.

Pen Testers Re-Assess & Processes Improve

- **Rescan**: After remediation measures are in place, a rescan is conducted to ensure that vulnerabilities have been adequately addressed.
- **Retest**: Similar to the initial test, a retest is done to validate that the vulnerabilities have indeed been fixed.
- **Validate**: A validation process ensures that all remediation actions are effective and have not introduced new issues.
- **Eliminate Issues**: Any lingering or new issues detected during the re-assessment are dealt with promptly.
- **Evolve Processes**: The overall cybersecurity process is evolved and enhanced, incorporating learnings from the assessment.
- **Evaluate Metrics**: Key performance and risk metrics are evaluated to track the effectiveness of the cybersecurity measures over time.

TROLLEYE SECURITY

Dark Web Analysis Included

Included in our PTaaS offering, we run your domain name every month, meticulously scanning the web for any stolen credentials associated with it. Once this data is amassed, our dedicated team determines the immediate threat level, gauging whether these credentials can indeed be acted upon by cybercriminals. In addition to this our Dark Web Analysis offering have several other use cases, including:

- Scan the dark web monthly, identifying your organization's stolen and compromised credentials.
- Vet third-party vendors before your organization engages with them.
- Gain a better understanding of your organization's password practices.
- Increase compliance with cyber regulations like PCI-DSS 4.0, which places a larger emphasis on continuous security.
- Know when your organization's data is being sold on the dark web, notifying you of a data breach.
- Monitor your organization's executives, to make sure that their data is not being sold on the dark web.

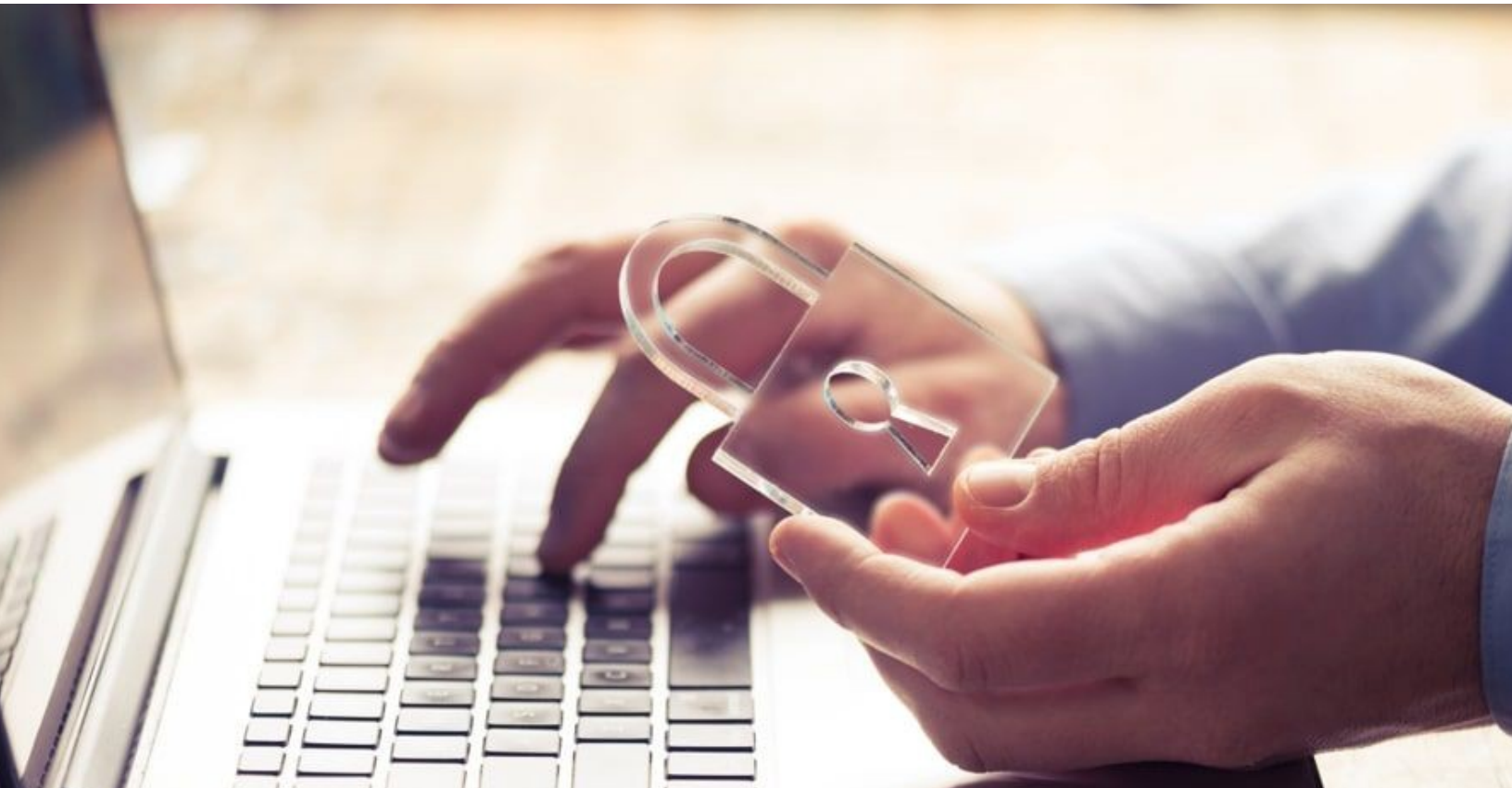
Quarterly Phishing Campaigns Included

As a part of our PTaaS offering we conduct quarterly phishing campaigns where we work closely with your organization to develop targeted phishing simulations. The process begins with an in-depth consultation to understand your unique business environment and industry-specific challenges. This insight informs the creation of customized phishing emails that are both relevant and convincing to your organizational context.

These crafted emails are then deployed as part of a campaign using our Command Center platform. The platform tracks and records the interactions of your staff with the simulated phishing attempts, capturing valuable data on their responses and susceptibility to such threats.

We also take the additional step of validating any credentials obtained during the campaign to assess potential vulnerabilities and the extent of access that could be gained. This approach not only tests the reaction to phishing attempts but also the potential impact on your systems.

The campaign concludes with a comprehensive debriefing session. In this meeting, we present a detailed analysis of the campaign results, offering insights and actionable recommendations to bolster your cybersecurity posture and improve your team's awareness and response to phishing threats.



Attack Surface Management Included

Using our platform, Command Center, we identify, catalog, and manage the risk associated with every point of exposure within your network. From on-premises infrastructure to cloud environments and remote endpoints, our platform ensures continuous visibility into your assets, enabling us to proactively detect vulnerabilities before they can be exploited.

Execution of ASM involves an iterative cycle of mapping, testing, analysis, and fortification. We begin with a thorough mapping of the existing attack surface, followed by simulated attacks and vulnerability assessments to identify weak points. Subsequent analysis of these findings leads to strategic recommendations for fortification, which are then implemented to enhance the overall security posture. Continuous monitoring ensures that as the attack surface evolves, our defenses evolve with it, maintaining the integrity of our clients' systems and data.

Command Center (SaaS)

Command Center is our cybersecurity platform that enables your IT staff to manage cybersecurity risk. When you use TrollEye Security for penetration testing, your team will get access to the platform. With role-based access and views, your IT staff will only see the findings related to their role.

In addition to that, we are constantly adding new futures to Command Center, with our product also having both Managed SIEM and Attack Surface Management capabilities, allowing us to perform Purple Teaming engagements.

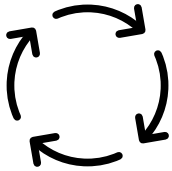
Role Based Findings

User Friendly

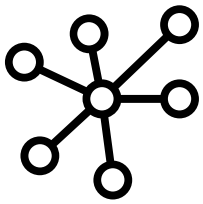
New Features Constantly Added

Purple Teaming Engagements

Why Should Companies Use PTaaS?

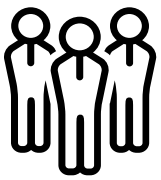


Continuous Security Testing: Traditional penetration testing provides a point-in-time assessment of vulnerabilities. PTaaS offers continuous monitoring, ensuring that new vulnerabilities are detected and addressed promptly.



Scalability: PTaaS solutions can easily scale to meet the demands of businesses, whether they're assessing a single application or an entire enterprise environment.

Cost-Effective: Companies can save costs associated with hiring full-time penetration testers or paying for one-off tests by opting for a subscription-based model.



Expertise: PTaaS providers often have a team of experts who are updated with the latest threats and vulnerabilities, ensuring a high standard of testing.

Compliance: Regular penetration testing can help businesses meet certain regulatory and compliance requirements.

TROLLEYE SECURITY

How Is Our PTaaS Offering Different?

At TrolleyEye Security, we understand that navigating the multitude of cybersecurity offerings can be daunting. That's why we've meticulously crafted our Penetration Testing as a Service (PTaaS) to stand out in a crowded market. To help you make an informed decision, we present a transparent, feature-by-feature comparison of our services against other leading providers. Whether it's our ability to initiate testing within 24 hours, distribute findings tailored to specific roles, or offer dark web analysis and executive monitoring, our comprehensive PTaaS solution is designed to deliver unparalleled security assurance and support for your organization. Compare us with Cobalt, NetSPI, Bug Crowd, Breachlock, and Astra, and see why TrolleyEye Security is the preferred choice for businesses seeking robust and responsive cybersecurity defenses.

Features	TROLLEYE SECURITY	Cobalt	NetSPI	Bug Crowd	Breachlock	Astra
Weekly Testing	✓	✗ (On Demand)	✗ (On Demand)	? (Not Specified)	? (Not Specified)	? (Not Specified)
Actionable Recommendations	✓	✓	✓	✓	✓	✓
Testing Can Start in 24 Hours or Less	✓	✗ (48 Hours)	? (Not Specified)	? (Not Specified)	? (Not Specified)	? (Not Specified)
Findings Distributed Based on Role	✓	✗	✗	✗	✗	✗
Monthly Cadence Meetings	✓	? (Not Specified)	? (Not Specified)	? (Not Specified)	? (Not Specified)	? (Not Specified)
Easily Request Retesting	✓	✓	✓	✓	✓	✓
User Friendly Platform	✓	✓	✓	✓	✓	✓
Immediate Notification of Findings	✓	✓	✓	✓	✓	✓
Dark Web Analysis	✓	✗	✗	✗	✗	✗
Third-Party Vendor Monitoring	✓	✗	✗	✗	✗	✗
Executive Monitoring	✓	✗	✗	✗	✗	✗
Attack Surface Management	✓	✗	✗	✗	✗	✗
Quarterly Phishing	✓	✗	✗	✗	✗	✗

Take It From Our Clients!

Mario Andino

★★★★★

Security Analyst at SMC3

"I am pleased with all the services we are receiving from the team at TrollEye Security. Being able to actively view our dashboard from Command Center gives our information security team the insight we need to ensure our security posture across the organization."

John Andrew

★★★★★

Security Compliance Manager at Flight Schedule Pro

"TrollEye is a trusted partner in our cybersecurity efforts, and I highly recommend them for their technical expertise and client-focused approach!"

Cyrus Yazdanpanah

★★★★★

IT Manager at FSLSO

"PTaaS has been a wonderful addition to our Development Lifecycle. And Command Center provides a unique experience with excellent value!"

Find Out How We Can Help Your Organization

Schedule a Free Demo Today

(833) 901-0971

trolleyesecurity.com/contact/

TROLLEYE SECURITY