March 21st, 2023

Ensuring that security is proactive and preventative – Q&A with Arik Liberzon, Co-Founder and CTO of Pentera

Arik Liberzon

#Automated Security Validation #Q&A

PENTERA
ARIK LIBERZON, PENTERA: "WE MUST ENSURE THAT SECURITY IS PROACTIVE AND PREVENTATIVE AND NOT SIMPLY RESPONSIVE"

Despite major investments in their security suites, organizations continue to be breached. Our Co-founder and CTO, Arik Liberzon, recently sat down with CyberNews to discuss the value of the adversarial perspective and where his inspiration from Pentera came from.

1. **Let's go back to the very beginning of Pentera. What has the journey been like over the years?**

Starting out, I arrived at the idea for Pentera and Automated Security Validation in a pretty organic way. After leading the pentesting operations in the IDF, the value that the hacker's perspective provided security teams was unquestionable to me. In the army I had teams dedicated to the purpose of pentesting and red-teaming, but despite the manpower we still wanted more. After I retired from the army, I was thinking about what to do next and realized that if that very perspective could be automated it would be like handing every security to a team of 1000 dedicated pentesters. The scale of the work would provide security teams with an unprecedented view of their exploitability, and I was confident the demand would be there.

The good part about the journey was that, like me, from the start nobody questioned the immense value automation could have on the industry. Instead, what everyone questioned was if the product I was proposing was even possible. Could you make an automated solution that was as dynamic as a real-world hacker without impacting business continuity? Could an automated solution be as sophisticated as the human hacker's brain? I knew it could be done. It's interesting to look back on the days where I struggled to find a single VC willing to fund the venture to where we are now as a Unicorn and category leader.

2. **Can you introduce us to your Automated Security Validation approach? What are its key principles?**

The concept of Automated Security Validation is an entirely new way of validating the effectiveness of your existing cybersecurity controls and reducing your cybersecurity exposure based on real-world attack emulation.

The key principles to our approach are:

- **Continuous Validation** – Our deployments are constantly changing and our security must be able to keep up. Instead of waiting for a report from their annual pentests to understand the effectiveness of their existing security, users can call on a virtual, automated team of pentesters to validate their security at the push of a button.

- **Emulate the Real Hacker –** To effectively validate the security of your organization, your testing must get as close to the real threat as possible. Automated Security Validation relies on an agentless solution that safely exploits your in-production environment, without the use of playbooks, to provide the most accurate emulation of actual attacks across the entire attack surface.

- **The Full Kill-Chain** – The testing must progress every scenario until it's completion so that security teams have an accurate assessment of how impactful each attack can be and where along the attack kill-chain is the most effective for mitigation.

- **Safe by Design** – Our Security Validation approach showcases exactly how hackers can exploit your network, what attacks they can execute, the potential for lateral movement, and what payloads they can use, all without any impact to your business continuity.

- **Actionable Insights** – Security validation cuts through the phenomenon of vulnerability fatigue, to reveal your true risk and provide a risk-based remediation roadmap with actionable insights that you can immediately execute to reduce exposure.

3. **Even though penetration testing is already ubiquitous, why is automated penetration testing not widely adopted?**

I believe the process for wide-scale adoption is already underway, but as in all aspects of life, traditional methods have their own inertia. While regulatory requirements mandate that many industries pentest, the frequency of tests is generally every six months or even once a year (industry dependent). Security benefits from more frequent pentesting. Companies realize already that securing the perimeter isn't enough and that they need to test their entire networks/systems altogether (EDR's, SOC, SIEM, etc.), however, the regulatory mandates have become the norm, and industries have gotten used to "ticking the box" as often as required.

The good news is that every security professional we meet understands the value of testing more often, and is enthusiastic about what continuous validation can provide their organizations. As more companies become aware of the option, we will see more large-scale adoption.

4. **Have the recent global events altered your field of work in any way? Were there any new challenges you had to adapt to?**

The truth is that while the economic slowdown has changed the way companies are structuring themselves, and how they approach hiring and expansion, it has not impacted the need for cybersecurity. In fact, quite the opposite.

Today everyone is under attack, and with the economic downturn, hackers are looking to capitalize on companies who may not have resources to expand security teams or add security solutions. This makes cybersecurity even more crucial, but without additional resources on the horizon, companies need to focus on efficiency and getting more out of what they already have.

Our security validation solution can help organizations optimize the effectiveness of their security, highlighting where it is working well, and where hackers are still able to exploit them. The constant attacks, and evolution of attacker techniques requires us to keep evolving alongside them.

We've already introduced two major modules to validate our customers against two of the most prevalent and growing attack vectors. Pentera is able to test our customers against the latest ransomware strains and the growing threat of leaked credentials, and is the first to automate these capabilities in the market. We are constantly adjusting our roadmap based on the greatest threats, adding new modules, features and capabilities to ensure that our customers are validated against the latest threats across their entire attack surface.

5. **In this age of frequent cyberattacks, what do you think are the key security practices both businesses and individuals should adopt?**

Gartner recently predicted that one of the keys for security in 2023 will be the shift from threat management to exposure management. I believe that adding the hacker's perspective to your security practices is crucial to making this strategy work and a must for security teams moving forward.

While it has traditionally been used in the context of DevSecOps, Shift-Left is a concept that the rest of security needs to adopt as well. We must ensure that our security is proactive and preventative and not simply responsive. Security teams can't close every threat vector, and must be efficient with how they allocate their time and resources, surgically remediating the exploitable issues across their extended attack surfaces. We need to be able to effectively prioritize our remediations, and not only according to CVEs and CVSS scores but according to critical kill-chains. The ability to distinguish the actually exploitable from the theoretically vulnerable relies on understanding the hacker's perspective and how they can attack your environment.

6. **What are the most common vulnerabilities nowadays, that if overlooked, can lead to serious problems for a business?**

It’s not the classic software deficiencies and CVEs that spring to mind when you say “vulnerabilities.” Instead, the most common vulnerabilities of companies today are more centered around misconfigurations and identity threats.

While ransomware continues to be a major problem that companies are faced with, it is hardly overlooked by security teams. There are so many other issues that can impact your organization that companies have no solution for. For instance, according to the 2022 Data Breach Investigations Report (DBIR), over 80% of Web Application breaches involve compromised credentials, yet most companies don’t have a protocol or solution in place to find out if they could be impacted. Hackers are always looking for ways to breach our organizations without notice, and utilizing leaked credentials allows them to enter under the guise of a legitimate user. With billions of leaked credentials already available on the dark web and paste sites, leaked credentials are a major concern and could lead to more breaches in the future if companies don’t adapt.

The other factor that companies should never disregard is mastering the basics. While they sound cliche, the common answers of setting minimum privileges for users, configuring proper segmentation, patching appropriately, avoiding end-of-life software, and investing in employee cyber awareness are actually among the most critical. Each is a small piece of the larger cybersecurity posture that ensures you are a less attractive target for hackers.

7. **Which industries do you think should take penetration testing more seriously?**

The short answer is that anyone who wants to maintain a robust cyber security posture needs to take their pentesting seriously.

Every industry is a target, so nobody has the luxury of not taking their cybersecurity seriously. What we’ve seen from our experience with customers across 20 industries is that the majority of security teams already know the value of penetration testing, so at this point it’s about improving the efficiency of the process, increasing the cadence of testing, and ensuring that your efforts are actionable. If you pentest frequently, but don’t take advantage of the reports to improve your security posture, then you need to re-examine your processes.

8**. In your opinion, what kind of tests and checkups should every company conduct regularly?**

Our networks today are not only larger, but more complex than they’ve ever been. Today, deployments change so frequently that it’s honestly not a stretch to say that just because you secured something a few days ago, doesn’t mean that it can’t be vulnerable today.

Companies are using so many different solutions to stay on top of their security, and they must have a way to verify that they are working in unison to deliver on their promises to prevent breaches. Every organization is a target, and every attack surface is a potential entry point, so there is no room for blind trust.

The other checkup you should never skip should be testing the human factor. People remain one of the largest and most consistent attack surfaces that companies have to contend with. Employees open malicious emails all the time and IT professionals may make simple misconfiguration errors that could be costly. All of your efforts to patch vulnerabilities, segment your network and implement new security tools can be undone if your staff makes simple mistakes, so it's crucial to invest in their cyber-awareness education.

9. **Would you like to share what's next for Pentera?**

First and foremost Pentera is committed to ensuring that our customers are secured against the latest attack techniques and are able to validate their security controls. To meet the challenges of the ever-evolving threat landscape we constantly add relevant capabilities, attack surfaces and techniques to our platform.

In addition to our recently announced Credential Exposure module, which combats the rising threat of leaked credentials, over the past year we launched Pentera Surface, becoming the first company on the market to validate security across the entire kill-chain from external assets all the way to the core of your enterprise. This enables IT security teams to see not only how adversaries may breach their organization, but also how they can escalate the attack and move laterally once inside.

On the business level, Pentera will continue its expansion to new markets. We recently expanded to APAC, and will continue to expand to new markets around the world to ensure that organizations everywhere have access to the latest in security validation.
You can read the original interview on Cybernews.

> Written by: Arik Liberzon