Candor
www.candor.cloud

AI Penetration Testing as a Service

Frequently Asked Questions: FAQs

With an expanded remote workforce and a rise in cyber-attacks over the past year, validating organizational resilience is at the top of the enterprise agenda.

By utilizing security validation tools, CISOs can shore up operational defenses, retire ineffective tools and processes, and get a more accurate grasp of the gap between where you *think* you are, and what your *real* resiliency levels are like.

However, not all security validation tools are created equal. Here are 5 must-have capabilities of the most effective validation tools:

- **What is Continuous Applicability and how does it benefit my organization?**
  - **What is it?**
    - **Continuous Applicability** is a term regarding standard method/s and toolset/s that perform predefined functions in a repeatable and consistent fashion.
  - **How does this benefit me?**
    - New threat vectors are discovered all the time, so a periodic check of your vulnerabilities is out of date almost immediately. 40% of organizations are worried that they aren't testing their security controls *enough*. Continuous validation means exactly that: at any given moment, you have real-time, up-to-date confidence in your security program.

- **What is Adversarial Validation and how does it benefit my organization?**
  - **What is it?**
    - **Adversarial Validation** is a term regarding standard method/s and toolset/s that perform validation of vulnerabilities/threats and ethical hacking techniques that can be achieved within your environment.
  - **How does this benefit me?**
    - Yes, it's important to know where your crown jewel assets are, but that knowledge is just the first step in the process. Don't be left wondering how to keep them secure and base your protection on assumptions. Instead, get into the mindset of the attacker, and emulate what *they* do, from privilege escalation to lateral movement through the network. What do you find that you might have otherwise missed?

- **What is AI for Security Validation and how does it benefit my organization?**
  - **What is it?**
    - By leveraging **AI for Security Validation,** we can automate and execute tasks with exponentially greater efficiency and effectiveness than that of a human. This results in improved efficiencies, reduction in cost, and ultimately provides a clear pathway for remediation of inherent risks
  - **How does this benefit me?**
    - When it comes to testing your network for security validation, humans just don't come close to machines. Consistency, speed, cost-effectiveness, and accuracy – that's what you want from a validation platform. An added benefit? Your team can hit play and go add value elsewhere. Machines don't blink, don't sleep, and don't take coffee breaks. That's how your security validation should operate.

- **What is Risk-based Prioritization and how does it benefit my organization?**
  - **What is it?**
    - **Risk-Based Prioritization** is a term for automated prioritization of inherent risks, to ensure that planned remediation efforts provide the maximum efficiency. This provides exponentially increased efficiencies by ensuring your staff spends time in the areas that require the greatest focus in a fact-based easy to understand fashion.
  - **How does this benefit me?**
    - Alert fatigue happens when security teams are given warnings and long lists of vulnerabilities without context, leaving them to make judgment calls or even skip steps. Smart validation tools will help you assess risk alongside the business context, and show you what needs your attention, right now.

- **What are Re-testing Capabilities and how does it benefit my organization?**
  - **What is it?**
    - **Re-testing Capabilities** is a term regarding standard method/s and toolset/s that allow you to re-test and validate that remediation effort executed have reduced your attack surface.
  - **How does this benefit me?**
    - Once you've put changes into place, have you made a difference? It's notoriously difficult to know whether the changes you've made have had the intended effect and haven't caused any collateral damage. Your security validation tool should allow you to test again immediately. Security isn't something you can gauge at a glance to see whether you're on the path to readiness or not. Make sure you can test again immediately, plus after any significant changes, to compare against the baseline.