

LMNTRIX
BE THE HUNTER | NOT THE PREY

Whitepaper

**REAL-TIME AND AUTOMATED
ATTACK VALIDATION PLATFORM**

Table of Contents

Introduction	2
Next Generation Automatic Attack Validation	3
Industry Challenges	4
How LMNTRIX Help Solve Industry Challenges	6
Summarizing LMNTRIX With 6 Questions	8
A Look At Other Cyber Security Services	9
Automated Attack Validation Comparison	10
Conclusion	11
Discover LMNTRIX AAV	12



INTRODUCTION

In a time where news of data breaches are becoming “the new normal,” the need for organizations to evaluate their overall risk and avoid becoming the next victim has become critical. Organizations simply can’t protect themselves from risks they’re unaware of.

Additionally, many organizations are simply unsure where to start. As the demand for cyber security consulting services increases, consulting firms are experiencing many difficulties with filling in the roles to provide these services. Many gaps are introduced in the assessments provided to organizations.

During a time where attackers are becoming more sophisticated and performing these attacks on a regular basis, it is imperative that organizations establish and maintain an information security program that allows them more flexibility on when and how often they can assess their environments.

NEXT GENERATION AUTOMATIC ATTACK VALIDATION

LMNTRIX Automated Attack Validation (AAV) bridges the gap between the increased demand of cyber security services and the lack of resources available and value provided to customers. Our team has developed this platform to combine all the knowledge and methodologies traditionally used during an automated attack validation to offer to organizations.

Essentially, LMNTRIX allows organizations to conduct a full-scale automated attack validation at any time to assess their infrastructure. Given that it is based on multiple frameworks and experience, organizations can be assured they are receiving the best automated attack validation possible, several times a year.

LEARN MORE:

**[AUTOMATED ATTACK
VALIDATION TESTING
ON A NEW LEVEL](#)**

INDUSTRY CHALLENGES

Traditionally, organizations face several challenges when it comes to looking for the next qualified cyber security consulting partner, including some of the following:

1. Scheduling

It can be rather difficult to schedule a penetration test if you need a quick turnaround, especially during Q4. If you need one ASAP, it might cost you a premium just because resources may not necessarily be available. This can also become a problem if you suddenly remembered you need to meet a specific deadline that is shorter than you expected.

2. Communication

Knowing what's going on before, during, and even after an engagement is always a challenge. Some consulting firms send out daily status reports and others don't send out any at all. Having to ask "how'd it go?" and following up should never be necessary.

3. Comprehensiveness

A review of the consulting firm's deliverables is almost a must if you want to ensure high quality results. In many cases after receiving deliverables, organizations are still unsure what exactly the issues are and how the risks affect their specific organization and industry. Vulnerabilities do not affect every organization in the same way - risks should be evaluated based on the organization's compensating controls, probability of exploitation, potential impact, etc.

4. Frequency

Many organizations only perform an annual penetration test of their environment(s) to meet industry regulation requirements. Although it is necessary to schedule multiple automated attack validation engagements per year (e.g., once per quarter), doing so would still be much more expensive, requiring more travel or even multiple resources.

5. Cost


Many smaller businesses can't afford cyber security so they implement best practices based on their own research, sometimes leaving them vulnerable to many high-severity threats. As a result, they are exposed to risks that could ultimately lead to an organization going out of business.

6. Frequency

Many organizations only perform a penetration test of their environment(s) to meet industry regulation requirements. Although it is necessary to schedule multiple penetration testing engagements per year (e.g., once per quarter), doing so would still be much more expensive, requiring more travel or even multiple resources.

7. Activity Tracking

As mentioned in our blog post titled, "Getting the Most Out of Your Automated Attack Validation", many organizations do not receive the data they need to go back and trace activities, which could be extremely valuable for improving security technology in the event of a real data breach.



LMNTRIX AAV bridges the gap between the increased demand for cyber security services and the lack of quality resources available.

HOW LMNTRIX HELP SOLVE INDUSTRY CHALLENGES

A dedicated version of LMNTRIX AAV was developed initially before it was integrated into LMNTRIX XDR. After using it on a number of assessments, we were able to provide a lot more value to our customers by avoiding some of the repeatable tasks. Here's how LMNTRIX can help solve current industry challenges:

1. LMNTRIX AAV can run at any time and any frequency.

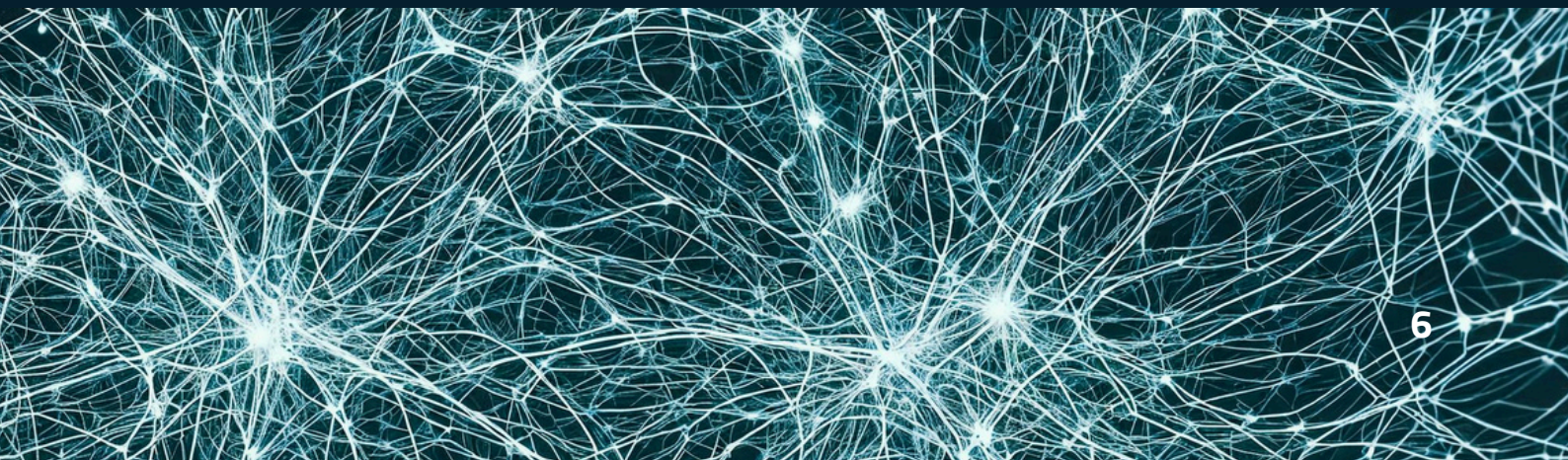
This essentially means you never have to wait on anyone to perform a automated attack validation. Technically, you could have a automated attack validation performed and have the report in your hand by the end of the week, and this is obviously something that cannot happen very easily when it comes to traditional engagements

2. Real-time Notifications

Notifications are always sent out when the automated attack validation starts and stops, keeping important individuals in the know as to when things are going on. This is also helpful in case there are some alerts that get triggered.

3. Reports that Drive Results

Considering LMNTRIX AAV has a reporting framework that is built around quality – the data provided in the reports will always be very informative. How these risks affect your organization, where your organization stands compared to its peers, how this compares to the last assessment, etc. are all examples of data that are included in each report.



4. Cost

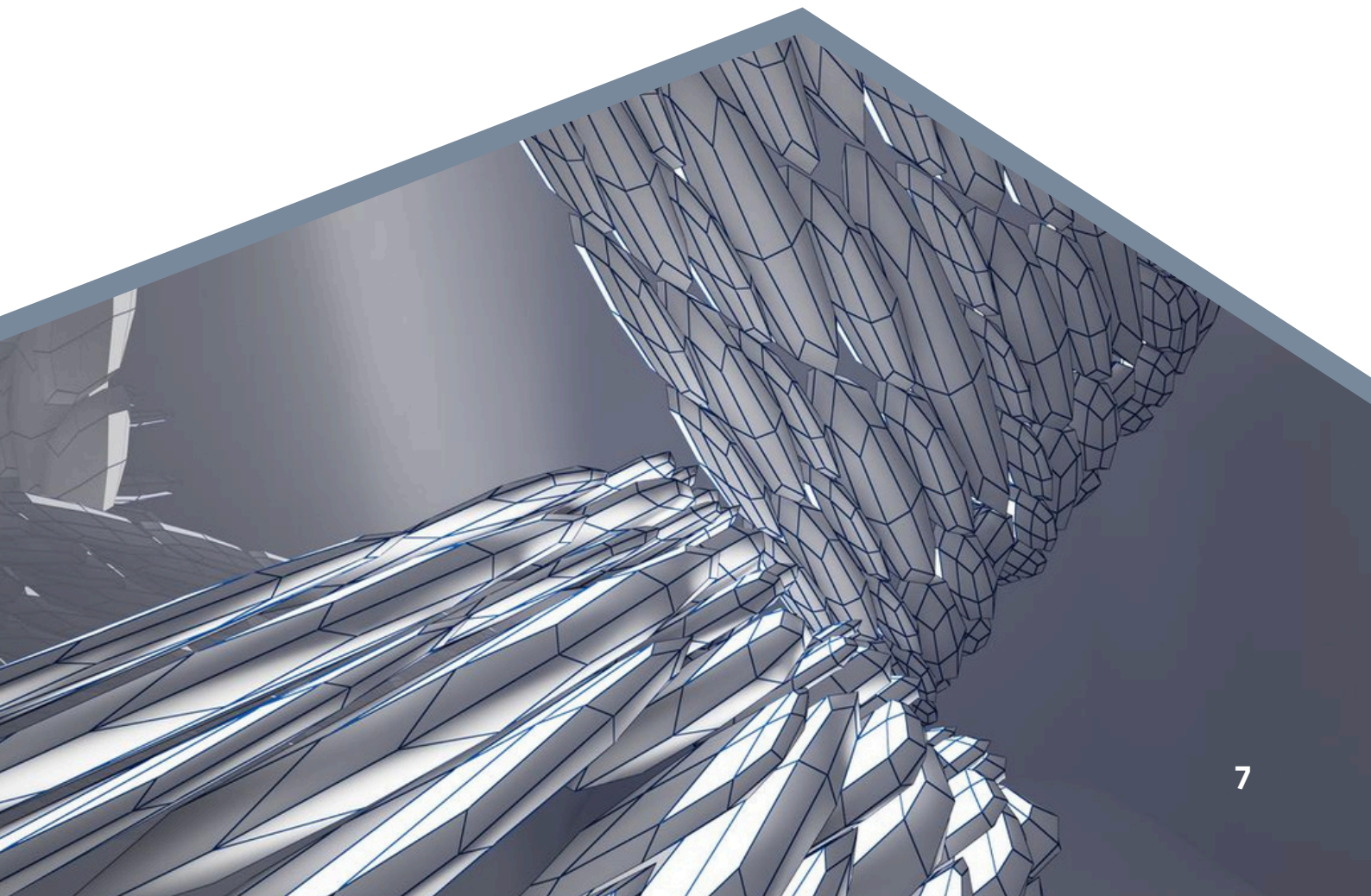
The price of LMNTRIX AAV is very competitive when compared to traditional penetration testing services but provides a lot more value for the same or smaller price point.

5. Transparency at Your Fingertips

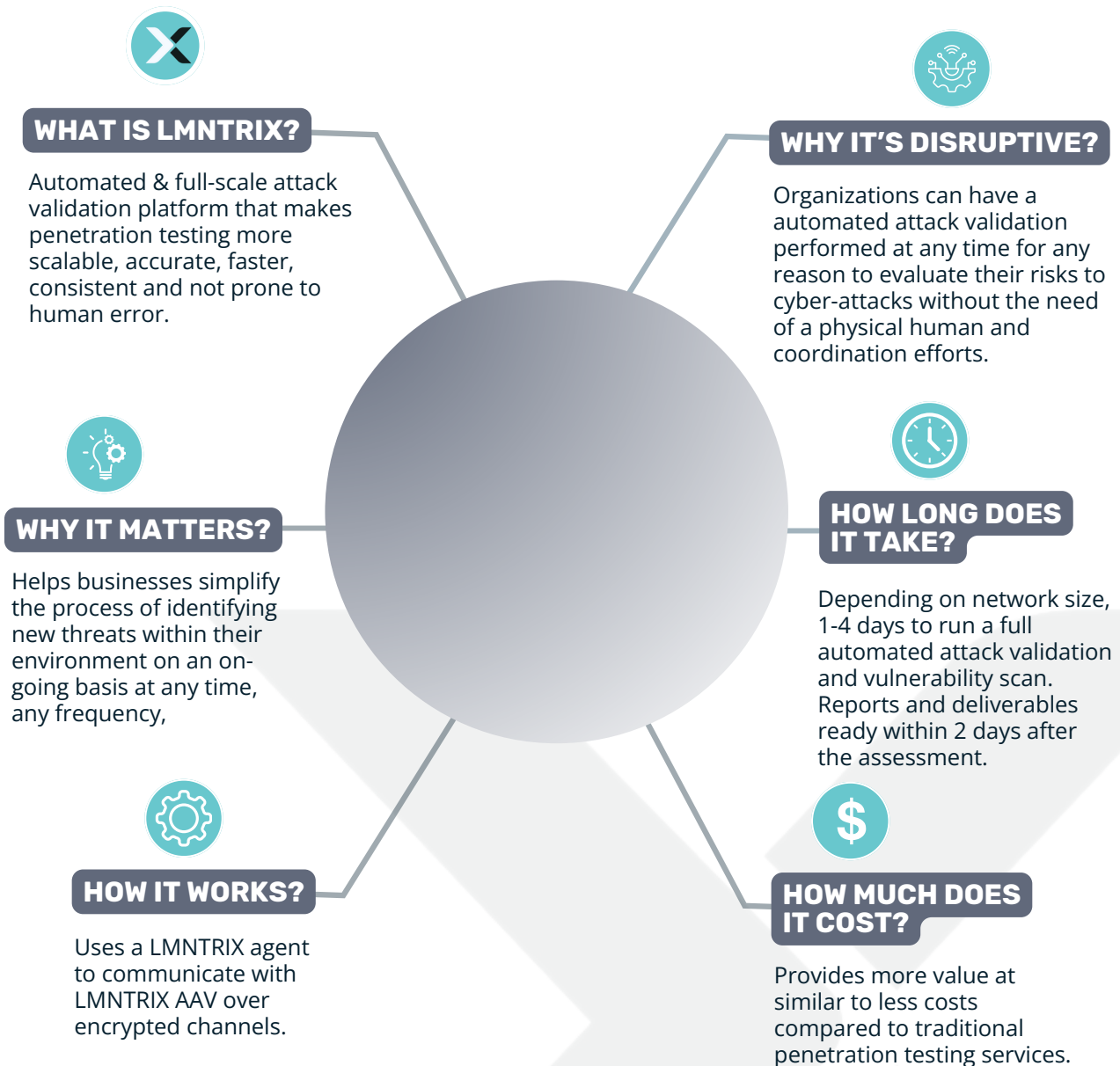
Customers can always log into their portal to get a list of contacts involved in the project, communicate with the consultant, as well as get a progress update that provides preliminary results and expected completion dates.

6. Reduce Turnaround Time for Detection and Response

Because all activities are tracked, including any manual activities conducted by a consultant, organizations can download this activity log and correlate activities with their XDR and incident response procedures. This is extremely useful in helping organizations make adjustments and tweak their controls, reducing the turnaround time for detection and response.



SUMMARIZING LMNTRIX AUTOMATED ATTACK VALIDATION WITH 6 QUESTIONS



A LOOK AT OTHER CYBER SECURITY SERVICES

The cyber security market is anticipated to exceed \$300 billion by 2024 due to the increasing frequency of cyber-attacks. Given the increase of attacks occurring against many organizations of all sizes, some cyber security consulting firms have already adapted to addressing these concerns in a scalable manner, including AI-based user awareness training, implementation of internal reward systems for organizations' employees that detect security threats, and more.

Automation is a very important advantage in cyber security that has been gaining momentum. Furthermore, there are other frameworks available that assist organizations with automating post exploitation (or breach-simulation) activities to help improve detection rates. These have also been extremely effective and help organizations reduce their overall risk in a way that scales with the growth of their organization and technology infrastructure.

A recent Ponemon Institute survey of more than 1,400 IT and IT security practitioners shows that 79% of respondents either currently use (29%) automation tools and platforms within their organization or plan to use them (50%) within the next 6 mo - 3 years.

Using Automation Tools

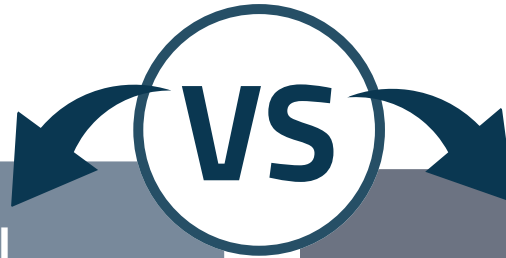


Planning to Use Automation Tools



Similar to other industries where repeatable processes become automated in order to scale and meet new demands with less mistakes, penetration testing should also be adapting to the new increased demand of services and be able to provide the same level of value, if not more.

TRADITIONAL PENETRATION TESTING VS AUTOMATED ATTACK VALIDATION



Traditional Penetration Testing



Executed manually by humans, possibly missing checks and low-hanging fruit



Methodology executed based on memory and experience



May lack consistent communication about assessment status and identified risks



Scheduling assessments may be difficult, depending on available resources



Risks are evaluated and demonstrated at a point-in-time with longer turnaround time on deliverables (approx. 2 weeks average)



Consultant(s) may lack expertise depending on experience

Consultants sometime juggle multiple projects, resulting in less value to your organization and higher costs due to manual labor required.

LMNTRIX: Automated Attack Validation



Consistently performs discovery, enumeration, exploitation, and post-exploitation



Tasks based on MITRE attack framework, experience, and LMNTRIX Automated Attack Validation framework



Real-time status updates and notifications for activities and identified threats



Execute automated attack validation at any time, any day



On-going automated attack validation, allowing for up-to-the-minute identifications of risks



Backed by OSCP, OSCE certified consultants with contributions to Kali Linux, Metasploit, and other frameworks

Combination of red team automated attack validation and developers to offer your organization more value, efficiency, consistency, and convenience.

CONCLUSION

LMNTRIX AAV aims to help organizations simplify the process of identifying new threats within their environment on an on-going basis without the traditional challenges and concerns. Your organization can use LMNTRIX AAV to perform Automated Attack Validation at **any time, any frequency**, receiving real-time reports, preliminary findings, notifications, and more.


[SCHEDULE A DEMO](#)



DISCOVER AUTOMATED ATTACK VALIDATION

LMNTRIX
BE THE HUNTER | NOT THE PREY

 lmntrix.com

 info@lmntrix.com

