2023

PENTERACON

Pentera's Annual Customer Summit

ROUNDTABLE SESSION SUMMARY

At PenteraCon 2023 we launched our Club Continuous community to help cyber defenders from all over the world share knowledge, exchange opinions and sharpen cybersecurity skills. One of the first opportunities for community interaction was our roundtable session. Thank you to all who contributed to the live discussions.

We are pleased to present you with this summary covering key insights and takeaways from the session. >>

KEY TAKEAWAYS

Cybersecurity performance metrics need to correlate with business impact and value.

Organizations use **different metrics to measure risk impact**. Examples of risk-based metrics used include business damage due to server or application downtime, legal impact, reputation impact, criticality of assets impacted, and cost of recovery. Time-to-remedy was also mentioned as a viable metric if risk impact measurement practices are not in place.

More than getting an accurate estimate of risk in currency terms, it is important to have a continual understanding of where your risk exposure is. If you can prove how you achieve **security posture improvements over time**, thereby reducing risk, this is a reliable benchmark for the effectiveness of your security program.

Communication with executive leadership must be adapted to achieve alignment and support.

Management sponsorship is key to getting the internal collaboration and resources needed for security improvement. **Demonstrating the existence of real-life security gaps** in the organization, for example through security awareness exercises or user password cracking tests, leads executives to action as they realize the risk of attack is not just theoretical.

It is important to **tailor the communication** style and information presented to different audiences, using non-technical language. Backing claims on the scope of security risk with data, such as industry benchmarks, cyber attack volumes and trends, or the cost of breaches, is key to getting buy-in from executive leadership to invest in cybersecurity.

Evolving threats and expanding attack surfaces are creating new security challenges.

Complexities in setting password strength policies and implementing advanced authentication lead to **credential risk exposure**. To validate credential strength, organizations are using a combination of automated password strength testing using cracking techniques, password blacklisting in Active Directory, and guiding users to update their passwords.

Organizations **migrating to the cloud** are adopting security measures, but feel the need to do more. Challenges include threats to the cloud environment originating from on-premises networks, too many alerts from cloud security tools, and lacking cloud penetration testers.

Automation enables continuous security assurance and accelerates remediation, augmenting human expertise.

The security assessment process for cyber-insurance is increasingly challenging and restrictive. **Insurance companies are looking for assurance** of the organization's security posture. The use of automated testing can help in providing such assurance and obtaining a policy with improved terms.

Man and machine need to work together. You can't feel safe, you have to validate and challenge yourself each and every day. Automation allows security teams to identify and solve problems in minutes.

Automated testing is needed not only for new threats and exploits but also for **continually testing existing vulnerabilities**. Automation can be used to routinely validate the security of newly deployed hosts.

Remediation prioritization should be contextual and based on risk.

Extensive vulnerability data coming from multiple security tools can be overwhelming and hard to consolidate. Prioritization of vulnerabilities based on exploitability, assets impacted and/or business risk is important for **determining which remediation actions to focus on.**

A vulnerability in a small segment may look insignificant but may still enable lateral movement as part of a high-impact attack. **Attack maps are very effective** for showing the potential impact.

To invoke change, make security personal, and clarify accountability.

Personal awareness is what builds better interest and care among employees. **It's about changing attitudes**. Relate cybersecurity to personal risk such as the potential consequences of leaving their house key under the mat or not sufficiently protecting their bank account.

Gamification is a very effective method to impact behavior. Employees get the experience without the negative consequence. It is important to enforce positive behavior.

For vulnerability remediation, unclear ownership is a common challenge. **Clarify which group is responsible** for implementing the remediation.

SEE YOU NEXT YEAR

PENTERACON 2024

Pentera's Annual Customer Summit

For more info, visit: **penteracon summit 2023**