How do organisations in Asia Pacific tackle vulnerability management?

Matthew Tan

July 1, 2024

In 2024, we have seen the impacts of cyberattacks on many organisations largely around data breaches and ransomware. The most recent news being an entertainment company that had over 500 million user data allegedly exposed on the dark web, while several ransomware incidents were targeted at retail, manufacturing and healthcare industries.

Such incidents underscore the relentless threat posed by cyber criminals, who actively exploit vulnerabilities across an increased attack surface. Even the most digitalised companies may overlook hidden vulnerabilities in their systems and infrastructure, leading to substantial damage to their brand and reputation.

This underscores the critical importance of vulnerability management, which involves identifying, assessing, classifying and prioritising security vulnerabilities in software and IT systems. Some companies, particularly those in regulated industries, are required to have vulnerability management in place to meet compliance standards. The objectives of vulnerability management include:

- Reducing business and reputational risks.
- Enhancing security posture.
- Minimising the attack surface.
- Meeting compliance requirements.

A key challenge in addressing vulnerabilities is the dispersed nature of modern enterprise networks and the frequent emergence of new vulnerabilities. Effective vulnerability management requires more than just the use of multiple tools. Cybersecurity teams can enhance the organisation's security

posture by proactively identifying and resolving vulnerabilities before they become exploitable. This approach should be a continuous and automated process involving five seemingly overlapping steps.

1. **Identification**
The identification process revolves around vulnerability assessment. All IT assets of an organisation are assessed for vulnerabilities. An expert service provider can help you automate this process using specific solutions. IT teams can also use periodic assessments such as penetration testing to locate vulnerabilities that might have evaded vulnerability management solutions.

2. **Prioritisation**
Organisations categorise and prioritise identified vulnerabilities based on their severity. This prioritisation helps in assessing the likelihood of each vulnerability being exploited.

3. **Resolution**
Once vulnerabilities are identified and prioritised, IT teams can resolve them in three ways.

- **Remediation:** This involves addressing a vulnerability thoroughly to prevent its exploitation. Most vulnerability management solutions, like those employed by managed security service provider providers, can manage patches and rectify device and network misconfigurations through a risk-based approach.
- **Mitigation:** Mitigation involves reducing the likelihood of an attack from an identified vulnerability without excising the vulnerability entirely. For example, isolating an affected device or system from the rest of the network can mitigate the impact of an attack, should it occur.
- **Acceptance:** Sometimes, vulnerabilities with a low likelihood of attack or minor severity are left unaddressed.

4. **Re-identification**
Resolution is not the final step; IT teams reinitiate the identification process to ensure that remediation and mitigation efforts are effective, and to confirm that vulnerabilities do not pose recurring threats again.

5. **Reporting**
Vulnerability management solutions provide metrics on remediation and mitigation efforts. Advanced solutions offer databases of identified vulnerabilities and analytics-based threat intelligence, which can accelerate vulnerability resolution and benchmark previous efforts. IT teams can use these reports to establish baselines for ongoing vulnerability management and to monitor the effectiveness of their cybersecurity risk management programs over time.

What can companies do to manage vulnerabilities?

Offence is often the best defence. Companies can strengthen their security by initially assessing and then enhancing their security posture. Given the limited resources and the cybersecurity talent crunch in Asia Pacific, this task may seem daunting and costly for many regional companies. Partnering with a cybersecurity expert can help companies understand and address potential vulnerabilities in their systems and network infrastructure.

Do more with Lumen's Advanced MDR

More than vulnerability management, Lumen's Advanced Managed Detection and Response (MDR) service provides a unified and holistic approach that extends beyond the traditional notion of just threat detection and prevention:

- Proactively detecting and hunting vulnerabilities: Beyond just endpoints and network infrastructure, Lumen's Advanced MDR covers cloud-native applications, supply chains, IoT devices, and OT among others. It also drives user and entity behaviour analytics through our 24/7 Security Operations Centres (SOC).
- Elevating the overall security posture: Comprehensive cybersecurity protection by seeing more and stopping more with complete visibility of assets across the attack surface, allowing risk-based continuous vulnerability management, and elevating the overall enterprise security posture.
- Enhancing threat detection effectiveness: Lumen's Advanced MDR goes beyond traditional MDR services by using next-generation threat modelling and detection engineering processes based on the MITRE ATT&CK® framework.

Lumen's Advanced MDR service empowers organisations with the capabilities to identify, protect, detect, respond and recover with proactive threat hunting and intelligence. Learn more about our offerings and contact us to schedule a security discovery session.
