resillion

Quality: Engineered. Tested. Assured.

Datasheet

Security Assessment

Mitigating cyber attacks

The range of cyber attacks keeps growing and getting more complex. Consequently, the need for good cyber hygiene has never been more important. Although technology can be a critical defence tool, psychology and emotions are of equal importance.

Humans are often the weakest link in any defence strategy and require intensive training and encouragement to avoid criminal penetration, especially in cases of phishing. Many organisations conduct regular tests to identify which members of staff might open an unauthorised email with a view to equip staff as an army of cyber warriors. In addition, most employ external agencies to conduct penetration tests on a periodic basis. **Ethical hacking enables** management to assess possible **areas of vulnerability** and take appropriate mitigating actions.

There is a strong debate about the value of penetration testing versus red teaming, where the latter focuses on contextual risks relating to a specific attack landscape. However, it is widely agreed that automated testing alone is not enough to avoid cyber-attacks. Human intervention and training have proven to be the most effective means of managing cyber risk.

Next steps

The ingenuity of cybercriminals combined with the aggressive motivations of state actors demonstrates that increasing attention is required to minimise potential risks. Consider these actions to improve your overall cyber security posture:

- **Assess** the motivation of potential cyber actors, both state and private – gain a better understanding of the context in which attacks take place
- **Develop** scenarios that illustrate the potential damage caused by such attacks and assess the financial impact – set against cyber insurance policies and enhanced with a cyber incident response retainer
- **Conduct** regular penetration testing and red teaming to identify and resolve areas of cyber vulnerability
- **Engage** the board in cyber matters well ahead of any potential attack, learning from the experiences of previous incidents

The price of getting this wrong is evident in the fines and profit losses imposed on organisations across the globe, not forgetting data and operational loss, as well as reputational damage.

Realising the value of cyber security

Resillion sees and treats cyber security differently. Fast enough to keep up with dynamic threats. Intelligent enough to learn from them. Constantly evolving to keep the upper hand. Resillion brings you a cyber security architecture that adapts at the speed of threat actors and delivers advanced cyber threat intelligence. Partnering with best-in-class vendors, Resillion offers a range of services, and cyber hygiene tools, that add value by consolidating multiple security strategies and inputs into a cohesive, unified security solution.

Resillion aligns with your organisation's objectives, business imperatives, and technology blueprints for cloud, hybrid, and on-premises environments. We help CXOs build and manage resilient cyber and IT programs supported by the necessary tools and technologies to withstand and recover from disasters or adverse events.

Reduced risk and better intervention

Ensuring that the security measures you have in place are behaving in the way you would expect is vitally important, just as responding to an incident quickly will minimise losses, mitigate exploited vulnerabilities, restore services and processes, and reduce the risks that future incidents pose.

So many things in the cyber security landscape are changing rapidly notwithstanding your own environment. Ask yourself:

1. Are my defences working as I expect?
2. Has environmental or configuration drift changed over time?
3. Is my change management process effective?
4. Do I have the processes in place to deal with an incident?
5. When was the last time I tested any part of my cyber security defences?

A penetration test will identify weaknesses and vulnerabilities within your organisation via a combination of manual and automated techniques. The best assessments include remediation of threats. Techniques include:

- Threat intelligence specific to your vertical market, geography, and organisational size
- Identification of known/unknown and exploited vulnerabilities
- Correlation of possible indicators of compromise
- Deep forensic analysis of actions by the attack
- Analysis of network lateral movement
- Analysis of endpoints
- Analysis of email boxes
- Analysis of critical assets
- Analysis of critical data

Expose threats, risks, vulnerabilities, and put yourself in a position where, when the attack takes place, you can close the loop on open threats, or even avoid them entirely. Resillion currently offers:

- **Adversarial Attack Simulation**
  Improve your detection and response capability. Stop attackers gaining access to your data. Understand and measure your resilience to cyber-attacks.

- **Cloud Security Assurance**
  Assess your cloud infrastructure for exploitable risks and vulnerabilities that allow a hacker unauthorised access to your organisation.

- **Operational Technology Testing**
  Maximise the expertise of our consultants and protect the integrity and availability of your network-connected systems with regular testing.

- **Application Security Testing**
  Applications, web, mobile, and APIs, are an integral part of daily life. Ahead of production, understand your level of business risk and ensure your apps are built correctly and integrate with their intended operating system, without leaving you vulnerable.

- **Security Hardening**
  Be confident that you are compliant, in line with industry best practice, and know you're resilient to any attacks.

- **API Security Testing**
  There's an API for everything – identify and prevent any vulnerabilities before anyone else and mitigate your organisational risk.

- **Secure Code Review**
  Resillion examines your source code to identify any inconsistencies and weaknesses that make you susceptible to an attack, assuring your application's logic and business code is secure.

- **Network Security Testing**
  One vulnerability is all it takes to compromise your systems – Resillion uses real-world methodology, tools, and techniques to look for weaknesses in services, poor configuration, and weak credentials that lead to compromise. Protecting your network is your first line of defence.

- **Device Security Testing**
  Secure your (IoT) devices, identifying any exploitable vulnerabilities that allow hackers access to and manipulation of your network and data.

- **Remote Access and Mobile Device Management Security**
  Regularly review your device policies to keep up with the changing threat landscape and maintain your corporate security. Use tools and features that centrally manage devices, automatically patching vulnerabilities and upgrading software, tracking and govern installed software, adjusting a device's configuration to a setting dictated by a particular standard policy, as well as forcing users to change their passwords at regular intervals.

Basic defences, countermeasures and best practices detect and respond

Preventative measures only go so far; detection and response are equally critical. Vital to your awareness and ability to respond in a timely fashion, is having adequate intrusion detection capabilities, delivered through a series of triggers to initiate alerts to suspicious activity. **Actively** monitor networks and systems activity for unusual behaviour, such as users logging in at random times of day, from new or unknown systems, or multiple failed password attempts.

Security policies must be devised, applied consistently, and regularly reviewed to ensure their continued relevance – authorised personnel must be trained, kept aware and incentivised to prioritise security. Where you identify gaps in your capabilities or layers of defence, employ cyber security professionals to safeguard your local environment, sanitise and defend with the latest methodologies and applications.

We empower you with the tools and knowledge to protect your local and cloud environments, ensuring that our ongoing security engagements counter the very latest tactics, evolving threats, and build greater resilience, providing greater protection and security.

Protect, detect, respond, recover. Stay ahead of evolving threats and safeguard your organisation.