Managed Security Services

Bridging the Enterprise Security Skill Gap

By Rishikesh Kamat

Despite a plethora of security and risk mitigation technologies and approaches available today, there has been no respite in the number of major breaches in the last year. Recent data breach incidents indicate that hackers and people with malicious intent have the ability and motivation to penetrate the most secure of businesses, notwithstanding the massive investments these companies make in security tools and processes. We see that security breaches are becoming more frequent, more complex and more difficult to predict, because hackers are becoming more sophisticated.

What makes the security space particularly complex and fast-changing is that cybercriminals, by design, are motivated to seek new vulnerabilities and work out new approaches (DDoS, malware, ransomware, phishing, spoofing, skimming, bots, dark web transactions, day zero threats) to penetrate and impair enterprise security setups. The need for reskilling needs continuous investment and oversight, and can significantly distract business and IT teams. The sheer cost of continuous reskilling and retention of skills makes managing an up-to-date security team unfeasible for many organizations. Consequently, many of the security solutions invested by organisations remain ineffective due to poor configurations, maintenance and monitoring.

Most organisations face the following challenges in terms of security skills development

- Difficulty to hire and retain the right talent
- Inability to provide a strong career growth to the employee
- Lateral hiring leading to higher costs of on-boarding
- Inability to provide a true 24X7 shift coverage
- Inability to develop multi-skilled resources and optimise costs
- Inability to effectively leverage the hired resources

Managed Security Services thus need to become a necessary component of enterprise security strategy. While in-house teams are absolutely necessary for overall program management, day-to-day security operations (policies, tool upgrades / patches, detection, backup and remediation) and threat monitoring can and should be outsourced to Managed Security Services Providers (MSSPs). This helps bridge the skill gap more affectively as compared to developing or upgrading in-house skills. Here are some of the key areas where Managed Security Services can bridge the enterprise security skill gap.

MULTI-CLOUD SECURITY

The growing adoption of multiple cloud vendors and services within the same organization creates challenges around consistency of security processes and policies. The dynamism of a multi-cloud environment makes it difficult to invest in tools and skills. Managing and retaining skills in for multi cloud security tends to become cost prohibitive in the long run. Leading MSSPs like Netmagic have strong partnerships with cloud service providers like AWS, Microsoft Azure and Google, and make it easy and cost-effective to manage multi-cloud security.

THREAT DETECTION

The nature of security threats changes continuously in today's times, and keeping pace with the changing environment is a challenge. Thousands of new vulnerabilities are being discovered in software every year, and it is difficult to predict where the next data breach will occur, until it actually does. It is also very challenging to keep track of and implement hundreds of security vulnerability patches across systems on a regular basis. Since MSSPs are in the business of detecting and mitigating threats for multiple customers, they are generally better invested and better placed to address emerging security threats. MSSPs also offer a wide spectrum of capabilities to ensure strong, proactive threat detection and efficient remediation.

ENDPOINT SECURITY

Integration with systems outside the firewall (e.g., mobile apps, IoT, third party portals, consumer devices) is becoming a necessary aspect of business – something that cannot be avoided. The vulnerabilities that arise are not often in control of enterprise security teams, since they not have enough understanding of external systems and data to deal with them effectively. MSSPs can provide an additional layer of oversight across all endpoints before exposing enterprise systems and data to external applications and devices.

ENTERPRISE DATA GOVERNANCE

As the security landscape evolves, new tools and technologies, e.g. data protection, governance, policy management, encryption, analytics, etc.) are introduced on a regular basis. MSSPs constantly invest in new skill development and can make tools as well as resources available to customers in a scalable and need-based fashion, without needing to make significant investment in training and licenses.

REGULATORY COMPLIANCE

There is an increasing focus on regulatory oversight around data security and data protection, globally as well as in India (e.g., FedRAMP, HIPAA in US, GDPR in Europe and the IT Act in India). With continuous evolution in regulations, data security has become top-of-mind for IT decision makers. Meeting regulatory needs involves a high degree of transparency, auditability and access to large amounts of transactional data (audit logs, drill down reports, etc.). Understanding and implementing evolving regulatory needs thus becomes a new challenge (with new overheads) for IT and infrastructure management teams. MSSPs are very effective in addressing regulatory needs, since they make large scale investments in auditable processes and documentation.

Recent incidents have shown us that data security and protection is not an easy task, and will get even more difficult in the future. The nature of malicious attacks is likely to become more sophisticated over time, with the ability of hackers to use analytics (AI, big data) and behavioural science to take advantage of new vulnerabilities (at system, application, network and even human level). Today's infrastructure management teams are fairly underprepared to deal with the sophisticated nature of malicious attacks in the future. Building new skills on a continuous basis is not only an expensive proposition, but may also become a counter-productive exercise - preventing IT teams from focusing on core business needs.

Strong, global providers of Managed Security Services, that have made a significant investment in security tools, processes and skills, are perhaps the easiest way for companies to bridge the enterprise security skill gap, and create a cost effective, scalable and robust strategy for current and future security needs.