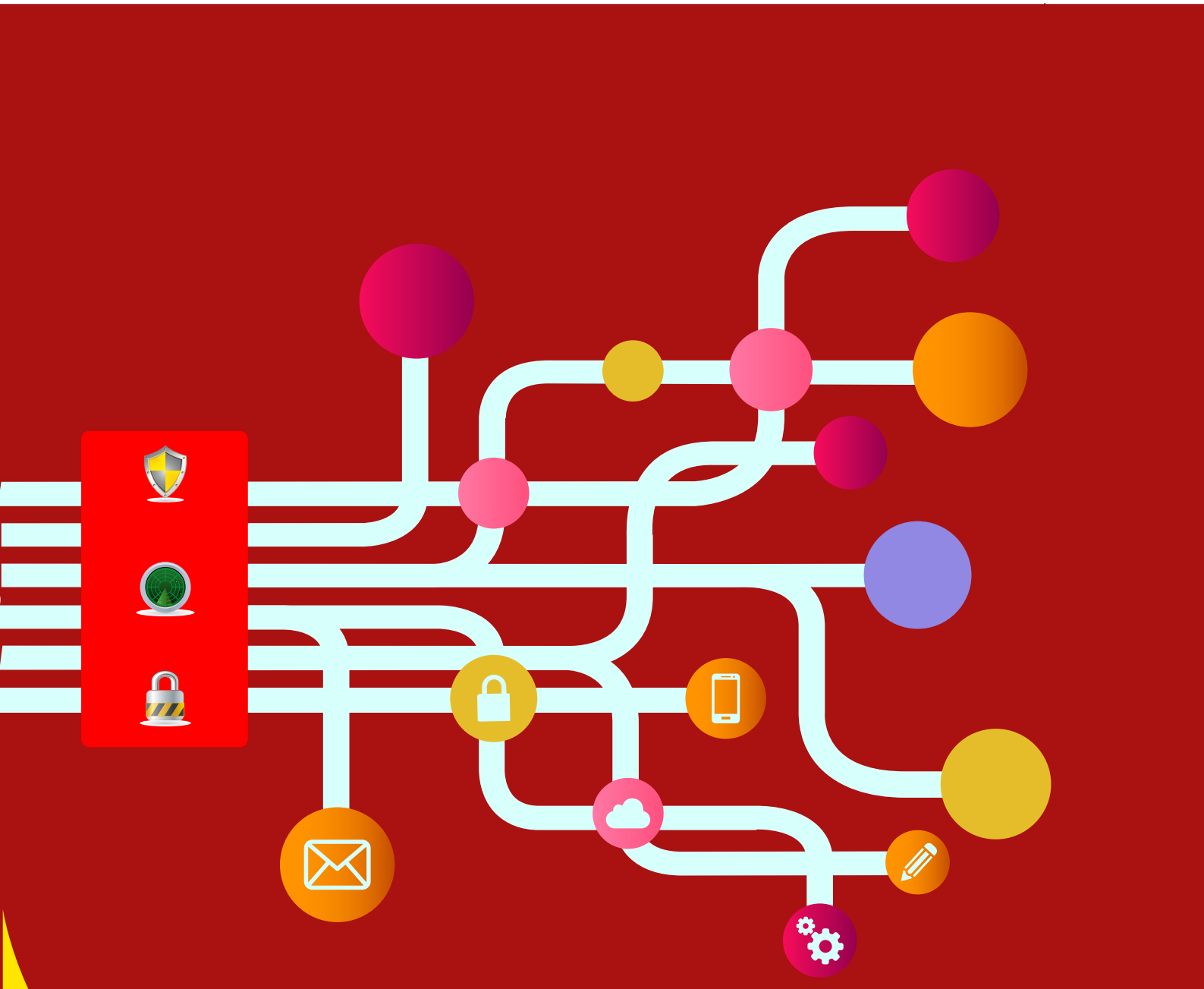
happiest minds

Integrated Security Services



Happiest People Happiest Customers

Contents

Introduction

Internet of things is slowly making sure that anything that can be inter-connected is getting connected. Technology, these days, form the foundation of most business functions; multiple business functions getting integrated through network devices has resulted in a catch phrase 'integrated security services' The phrase 'integrated security' in its most basic format refers to assimilation of security across functions and devices.

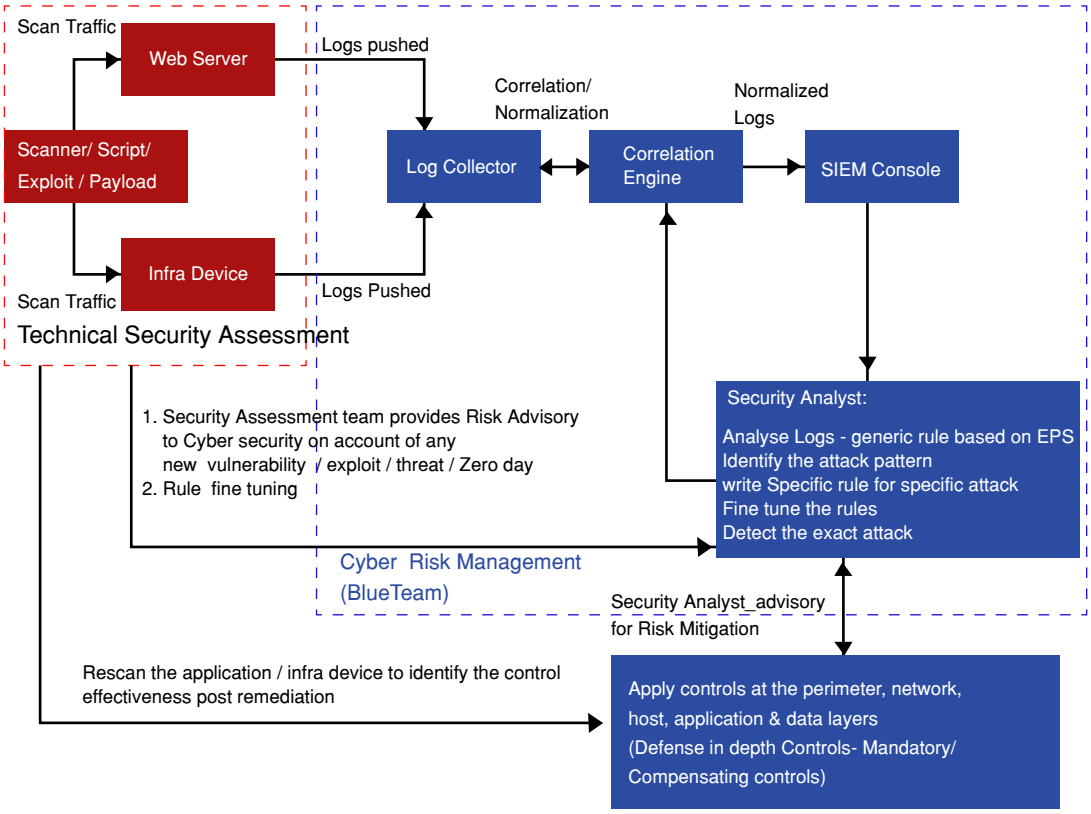
Organizations cannot manage security on an ad-hoc basis anymore. The nature of business environment these days compel organizations to allow access of information to various users -employees, customers, partners, vendors and other stakeholders. The Chief Security Officer is in today's dynamic and connected business environment has to look much beyond a basic anti-virus since there are possibilities of targeted sophisticated attacks besides already existing traditional threat landscape. As people become more dependent on mobile devices, cloud based services and a work culture that thrives on BYOD, the threat attack surface has just spread wider. In such a connected threat scenario, the security solutions should be robust, fully integrated solutions that can prevent, detect, analyze and respond in helping mitigate attacks. Advanced features like URL filtering, behaviour monitoring, firewall. POP3 scanning can add value to the existing point solutions. Given the changing technology landscape, integrated security solutions that can protect devices that an employee brings to work, whether Mac or Android, along with traditional Windows workstations and servers that are of paramount importance.

There are instances where integrated security solutions have worked only on laptops/desktops and not on servers which have resulted in using a separate security solution adding to the cost and resources. For instance, if the servers are not integrated with SIEM solutions then there might be a need to install monitoring solutions on the servers which can increase the cost to the organization. Also, if integrating the servers and all other devices in the network is mandatory as per regulatory and compliance requirements of a particular organization.

It is also important to discuss the pitfalls if integrated security is not in place:

- Without integrated security solutions, it is difficult to identify the source of scanned traffic - whether it is from the legitimate internal security team or from the illegitimate internet channels such as command & control server, blacklisted IPs etc. Without integrated solution, manual intervention is required which besides being time consuming, increases the possibility of errors. With the use of SIEM, one can write correlation rules to detect real time attacks.
- With the absence of integrated solutions, the SOC team cannot write the necessary signatures required to detect specific attack patterns that targets internal network.
- Integrated solutions used to determine the compensating controls for the application or infrastructure vulnerabilities helps control costs.
- The integration of security solutions keeps a check on the security assessment activity going on in the current network. It allows analysts to monitor the specific host undergoing scan activity ensuring that the host is verified and trusted.

The security assessment team can help the SIEM team in determining the threats an organization is facing based on the detailed analysis of the existing controls in the client environment. The logic pertaining to a certain attack can be converted to a specific rule in the SIEM system to detect the attacks more accurately. Mentioned below are the areas where the security assessment team can extend their hands in helping cyber risk management teams under the following circumstances.



Identify the attack pattern based on the EPS

Once the scan is initiated against the specific target, the scanner generates huge traffic to find vulnerabilities in the target. The target device generates the logs and scrutinizing them based on the EPS (events per second) helps identify the attack patterns.

Assist SIEM admin in understanding the logic of specific attack

Red team can assist the Blue team in understanding the root cause of a specific attack. Besides, the technical security assessment team would assist the SIEM team in understanding the logic of a specific attack and assist them in writing the rule to detect the attack.

Fine tune the existing rules

Default rules provided by OEM can be fine-tuned according to the existing technological environment of the client.

Detect the exact attack

Security assessment team should provide Risk Advisory services to Cyber Security team on account of any new vulnerability, threat, zero day, APT, malware, etc. specific to the domain of client (For ex : Telecom, BFSI, Healthcare, etc.).

Assist in risk mitigation and follow defense in depth strategy

Jointly review the detailed recommendation to mitigate or reduce the security exposure and likelihood that would help the business owner to manage the technology risk in accordance with the organization's business policy.

Help the business owner in mitigating the risks in cost effective manner by adopting the Defense in Depth strategy. This includes leveraging the existing controls such as fine tuning the rules of Firewall, IDS, IPS, WAF, etc. For application specific attacks the recommended controls should be adopted at the source code level.

Reassessment for all reported security findings within the application assessment scope, post vulnerability remediation from the respective teams at the client organization. This involves evaluating the control effectiveness post risk mitigation.

-

About the Author

Karthik Palanisamy

Karthik Palanisamy, Technical Security Assessment Professional with 4 plus years of consulting experi-encein network & web application vulnerability assessment and penetration testing, thick client security, database security, mobile application security, SAP application penetration testing, source code audit, configuration review of devices and security architecture review (Applications and Infrastructures). Currently holding a position with Happiest Minds Technologies to deliver technical security assessment and penetration testing services covering application security, infrastructures security, mobile application security and source code review.

Happiest Minds

Happiest Minds enables Digital Transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights through an integrated set of disruptive technologies: Big Data analytics, internet of things, mobility, cloud, security, unified communications, etc. Happiest Minds offers domain centric solutions applying skills, IPs and functional expertise in IT Services, Product Engineering, Infrastructure Management and Security. These services have applicability across industry sectors such as retail, consumer packaged goods, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality. Headquartered in Bangalore, India, Happiest Minds has operations in the US, UK, Singapore, Australia and has secured $ 52.5 million Series-A funding. Its investors are JPMorgan Private Equity Group, Intel Capital and Ashok Soota.

E-mail: Business@happiestminds.com
Visit us: www.happiestminds.com

Follow us on