WWW.WIPRO.COM

WIPRO
Applying Thought

ARMING YOUR SECURITY OPERATIONS CENTER WITH THE RIGHT TECHNOLOGY & SERVICES

Gopinathan. K

Table of contents

Arming your security operations center with the right technology & services

This whitepaper discusses the importance of IT security for enterprises especially as they deal with challenging business conditions. The consequences of not having proper IT security measures in place can result in substantial losses – both financial as well as intangibles such as diminishing reputation, credibility and so on. It is imperative for enterprises to embark on a holistic security program in their SOC. At the same time, enterprises need to be aware of which technology and service is relevant for their kind of business to get the maximum returns. This paper throws light on this topic too.

Security - a key requirement

Technology has become the pivot to an organization's success in today's demanding business environment. And within that, IT security has assumed significant importance –to handle the compliance and regulatory demands along with the myriad threats and vulnerabilities that businesses are exposed to continuously. The consequence of not allocating this importance can be quite expensive –the recent Sony PlayStation Network incident resulted in damages of $171 million to Sony. Similarly, Citigroup lost $2.7 million to hackers who accessed information of 200, 000 clients illegally. To appreciate the seriousness, consider this finding from PwC - the cost of information security breaches just in the UK was a whopping £5 - £10 billion in 2011. Clearly, the findings from a survey conducted by the Enterprise Strategy Group is no surprise then which states that IT security is among the top five priorities identified by IT professionals for 2012.

To compound matters, threats and attacks are only becoming more complex and sophisticated and so a well-equipped Security Operations Center (SOC) with the required security technologies and services is the order of the day. Many enterprises plan to increase security budgets to deal with this situation and enhance the capabilities of their SOC.

Challenges abound

No doubt that IT security is gaining much needed attention; however, the road ahead is replete with challenges. Most IT security professionals seldom take a holistic view while securing their organization. Typically, they adopt a siloed approach and secure the entire network without paying attention to individual host systems. It is assumed that access controls implemented across the network will, by extension, be sufficient to protect host systems and associated information. Unfortunately, this approach falls short in protecting business and technology services against attacks, threats and vulnerabilities comprehensively.

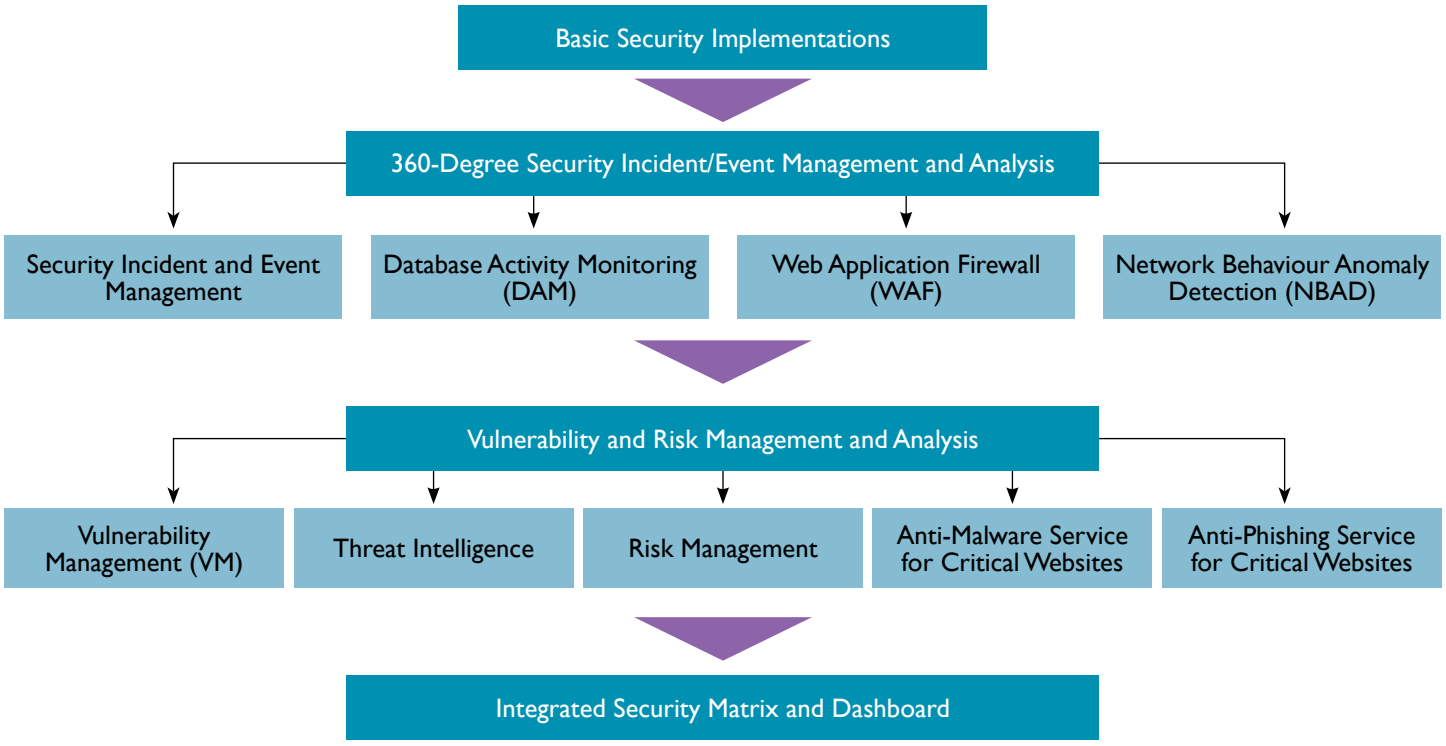
In addition, SOCs today have to contend with not only the physical networks, computers and applications, but extend their purview to the online realm and mobile devices too - no easy task. Verizon's "2011 Data Breach Investigations Report" reports alarming news that the number of online attacks increased by a factor of five between 2005 and 2010. Plus, there is the issue of mobile malware and anti-theft measures especially with the growing popularity and acceptance of the BYOD trend that needs to be addressed.

Some hard facts:

- According to McAfee, there were 8 million new kinds of malware more within the space of a quarter in 2012.
- Mobile vulnerabilities rose by 93% in 2011
- Estimated losses due to phishing attacks was $687 million in the first half of 2012 as per RSA

The way forward

Organizations must view the security portfolio holistically to provide a comprehensive cover enterprise-wide. Consequently, every host whether it is service oriented devices/servers or user oriented workstations, should be considered as a potential target and its vulnerability to attacks assessed. It is therefore essential to consider different technologies and services that can help mitigate these risks. The key technologies and services required in an SOC are as follows:



A practical framework to determine the right mix of security technology and services for enterprises

While the security elements introduced above are essential to protect enterprises and meet compliance requirements successfully, the choice and implementation of these technologies depend both on the industry they belong to and the size of the enterprise. For instance, large enterprises require security of a higher order and have stringent compliance requirements such as ISO 27001, SOX, HIPAA, and SAS 70. Such enterprises typically face a large volume of transactions resulting in terabytes of data which has to be managed securely. In specific cases such as in the financial sector, there is the added complexity of handling sensitive data. Failing to secure critical data can not only result in monetary losses but also lead to intangible consequences such as loss of reputation and credibility which can be equally damaging.

Stringent regulations

- BFSI – Compliance requirements such as ISO 27001, PCI-DSS, SOX, GLBA, HIPAA, SAS 70 and Regulatory compliances such as RBI, SAMA, FRB, FSA
- Telecom – Compliance requirements such as ISO 27001, IEC15408, 3GPP, SAS70, Telecom Regulatory Authorities

However, the same norm is not necessary for mid-size and smaller enterprises or those belonging to other industries such as manufacturing or CPG. Not only is the volume of transactions much lesser, the resources required to manage a comprehensive security portfolio is generally not available warranting a different approach to security. Clearly, a "one-size fits all" approach will not be effective.

The following framework has been conceptualized keeping in mind the specific needs of different kinds of organizations.

Sl.No	Service	Enterprise Category		
		Small	Medium	Large
1	Infra Security Operations	Yes	Yes	Yes
2	Security Incident and Event Management	Optional	Yes	Yes
3	Database Activity Monitoring	Optional	Yes	Yes
4	Web Application Firewall	Optional	Optional	Yes
5	Network Behaviour Anomaly Detection	Optional	Optional	Yes
6	Vulnerability Management	Optional	Yes	Yes
7	Threat Intelligence	Optional	Yes	Yes
8	Risk Management	Yes	Yes	Yes
9	Anti-Phishing	Optional	Optional	Yes
10	Anti-Malware	Optional	Yes	Yes
11	Data Loss Prevention	Optional	Optional	Yes
12	Virtual Infra Security	Optional	Optional	Yes
13	Network Admission Control	Optional	Optional	Yes
14	Wireless IPS	Optional	Optional	Yes
15	Identity and Access Management	Optional	Optional	Yes
16	Fraud, Forensic Analysis & SIRT	Optional	Optional	Yes
17	Security Matrix Dashboard	Optional	Yes	Yes
18	Application Code Review, SSO, 2FA	Optional	Optional	Yes
19	Physical Security Command Center	Optional	Optional	Yes

While this framework can be applied across industries, it becomes particularly critical for the BFSI and telecom owing to the nature of their business. For enterprises belonging to the BFSI industry, all the above services are recommended; however, the Identity and Access Management, Fraud, Forensic Analysis & SIRT and Wireless IPS are optional for smaller banks for obvious reasons. Similarly for enterprises in the telecom industry, other than Wireless IPS service, the rest of the elements are mandatory.

Essential elements for your SOC

Basic Security Implementations

All organizations need to implement a basic list of security technologies for overall protection. This includes a strong firewall, anti-virus and spam software, VPN devices for site-to-site and remote access as well as physical security checkpoints such as CCTVs, security guards etc.

360-Degree Security Incident/Event Management and Analysis

Security Incident and Event Management (SIEM)

The main requirement for SIEM tools is to monitor security incidents in real time and generate reports in case of any lapses. This tool also functions as a centralized security incident management framework as it can be easily integrated with other security technologies and services.

Database Activity Monitoring (DAM)

Often database administrators and other privileged users in organizations can access and modify sensitive information. DAM provides privileged user and application access monitoring, helps improve database security by detecting unusual activities, triggers alarms and meets compliance requirements.

Web Application Firewall (WAF)

WAF is necessary to ensure secure internet based (HTTP) communication and can detect common attacks such as Injection Vulnerability, Cross Site Scripting (XSS), Broken Authentication and so on. It is particularly useful in detecting and blocking out unwanted content when dealing with sensitive HTTP data and the logs generated by WAF can be used for forensic analysis and reporting.

Network Behaviour Anomaly Detection (NBAD)

NBAD is used for monitoring the network traffic behavior in real-time to protect the organization against zero day attacks that are not detected by signature/rule-based security systems like firewalls. It typically detects malwares through traffic analysis in all devices including those not discovered by the OEM vendor products and subscription services.

Vulnerability and Risk Management and Analysis

Vulnerability Management (VM)

To protect the software and hardware systems from attacks and exploiting inherent vulnerabilities, a security team must know what vulnerabilities are present. This means that organizations should have effective vulnerability management tools and processes as part of their IT security.

Threat Intelligence

Threat Intelligence Service is essential for the organizations to track, update and integrate the evolving threats and vulnerabilities for monitoring and mitigation. It would track global threats and vulnerabilities, chart an action plan and notify stakeholders through advisories.

Risk Management

Risk management services would ensure all the identified security incidents, vulnerabilities and threats are tracked and closed. It would also monitor technology related risks like design, configuration, security baselining, etc. These services would also regularly upgrade employee skills in dealing with security challenges, process violations and unauthorized changes/access.

Anti-Malware Service for Critical Websites

This service is to ensure that the websites are proactively monitored and protected from malicious attacks particularly defacements, malwares, etc. Through real time crawling and behavior analysis of a website, this service helps avoid blacklisting of the website in search engines.

Anti-Phishing Service for Critical Websites

Phishing attempts to acquire information like usernames, passwords, credit card details etc., through emails/sms to direct users to fake websites. Anti-phishing services are essential to proactively monitor, identify, detect and protect the user's identity and sensitive data from malicious elements.

Security Matrix & Dashboard

A Security Matrix and Dashboard provides a consolidated security status reporting of all the security technologies and services along with key metrics through a portal. This is very critical in enabling a comprehensive understanding of the security posture of the organization and typically includes dashboards for vulnerabilities, risks, security incidences, compliance, Anti X and patch management reports, and so on.

In addition to the key technologies, enterprises should invest in a SOC customized to their organization's environment for a drill down on business and technology risks, vulnerabilities, trends and comparisons with global practices.

Concluding thoughts

It is evident that enterprises need to implement the right set of security technologies and have a robust Security Monitoring Framework in place in their SOC. By adopting the proposed framework, enterprises stand to gain significantly – they choose the right set of technologies and hence secure their organization effectively. By doing this, they also invest wisely and this is critical in today's tough market conditions. Finally, with the right set of tools and technologies, the SOC becomes easier to manage and services business requirements better.

About the Author

Gopinathan. K. is the Practice Head for Managed Security and Network Services, Global Infrastructure Services (GIS), Wipro Infotech. Managed Services Business is the services arm of Wipro Infotech, focusing on providing Infrastructure Management Services including End User Computing, Cloud and Data Center Services. With 12,000 plus employees, it is one of Wipro's largest divisions and contributes strongly to Wipro's leadership position in the region. Gopinathan's practice responsibilities span across India and Middle East geographies.

Global Infrastructure Services

Wipro's Global Infrastructure Services (GIS) is a pioneer in the Infrastructure Management services space with revenues of 2Bn USD. This division contributes to over 30% of IT revenues of Wipro Ltd, with a headcount of over 26,000+ technical specialists. Our strong domain capabilities and specialized offerings help businesses across the globe transform their vision to results. Backed by our strong network of iGCCs (Integrated Global Command Centers) and 10 owned datacenters spread across US, Europe and India, GIS is enabled to provide cost variabalization, accelerated growth and continuous innovation for global businesses. Few of our industry specific service offerings include Wireless Place, Shoptalk™, Bank-in-a-Box while our traditional offerings include data center management, cloud, managed network, managed security, end user computing and business advisory services.

About Wipro IT Services

Wipro IT Services a part of Wipro Limited (NYSE:WIT) is a leading Information Technology, Consulting and Outsourcing company, that delivers solutions to enable its clients do business better. Wipro delivers winning business outcomes through its deep industry experience and a 360 degree view of "Business through Technology" - helping clients create successful and adaptive businesses. A company recognized globally for its comprehensive portfolio of services, a practitioner's approach to delivering innovation and an organization wide commitment to sustainability, Wipro IT business has 135,000 employees and clients across 54 countries.

For more information, please visit www.wipro.com or contact us at info@wipro.com

DO BUSINESS BETTER

NYSE:WIT | OVER 135,000 EMPLOYEES | 54 COUNTRIES

WIPRO TECHNOLOGIES, DODDAKANNELLI, SARJAPUR ROAD, BANGALORE - 560 035, INDIA TEL : +91 (80) 2844 0011, FAX : +91 (80) 2844 0256

North America South America Canada United Kingdom Germany France Switzerland Poland Austria Sweden Finland Benelux Portugal Romania Japan Philippines Singapore Malaysia Australia