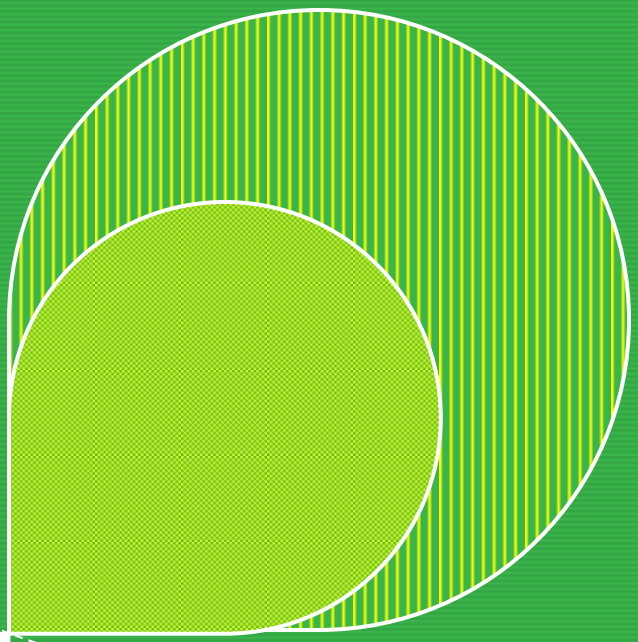
Unified Cyber Security Monitoring and Management Framework

By Vijay Bharti
Happiest Minds, Security Services Practice



Introduction

There are numerous statistics published by security vendors, Government and private agencies, research analysts etc in terms of the number and type of cyber-attacks, money lost due to cyber-attacks, data exposure and litigations. Though most of these estimates and surveys deploy different methodologies and vary to quite a degree, there are a few facts which cannot be ignored i.e. Cyber-attacks are becoming:

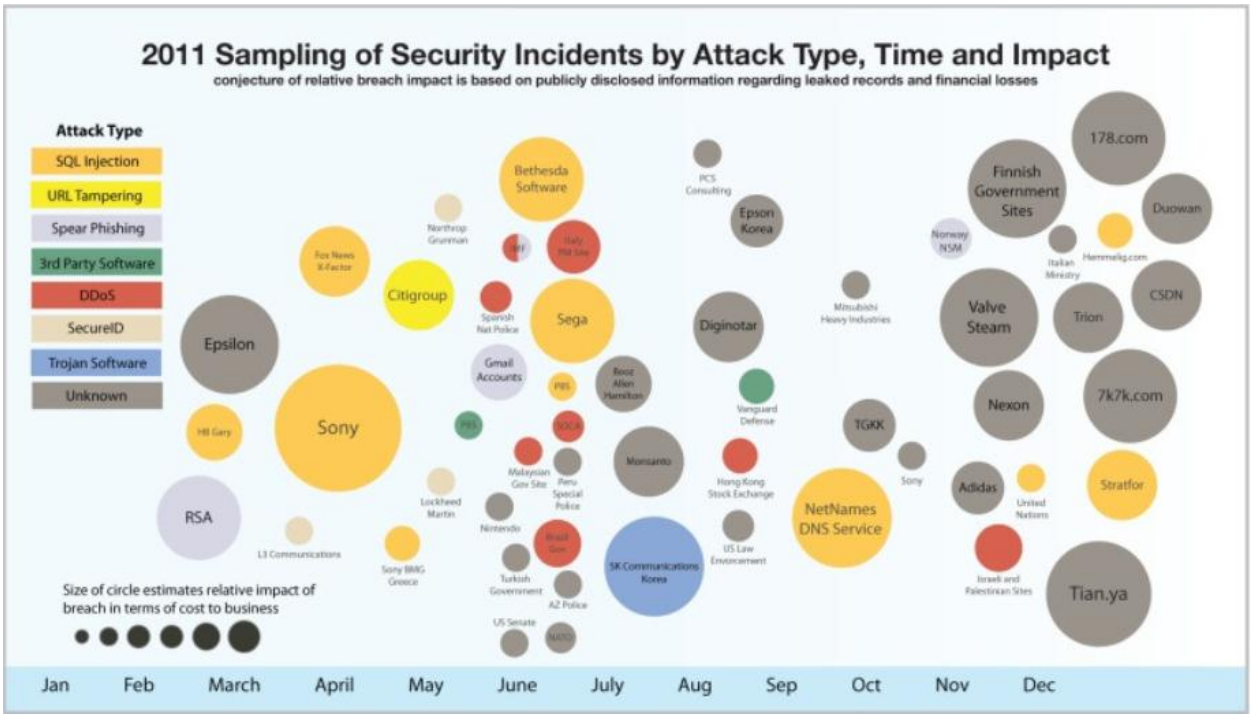
More advanced….

- sKyWIper (Flame) is one of the most sophisticated and complex malware ever found
- Stuxnet was designed to exploit more than 4 zero-days vulnerabilities (not publically known).

More focused and targeted, especially at financial institutions, political, military establishments and intellectual property….

- Stuxnet includes a highly specialized malware payload that is designed to target only Siemens supervisory control and data acquisition (SCADA) systems.
- RSA Advanced persistent attack which focuses on getting confidential data from internal servers.
- Zeus Botnet primarily focuses on financial frauds
- Attacks from Hacktivists like anonymous and lulzsec.

The overall risk would still be low if these attacks continue to remain targeted. However, given the ubiquitous nature of the internet, many of these advanced attacks proliferate into the public domain and become a very potent weapon in the hands of even a novice attacker e.g. most of the malware generation toolkits like Zeus, SpyEye etc are currently available in the hackers' market for a few hundred to a few thousand dollars.



Source – IBM Security X-Force 2012 Cyber Security Threat Landscape

Current cyber security challenges

Today, organizations rely heavily on cyber space to reach out to new customers and geographies, drive new business models and enhance operational efficiencies. However, given the increase in the number and sophistication of cyber threats and attacks, it's very critical for them to understand the risk involved and the counter measures required to derive the desired benefits of cyber space adoption.

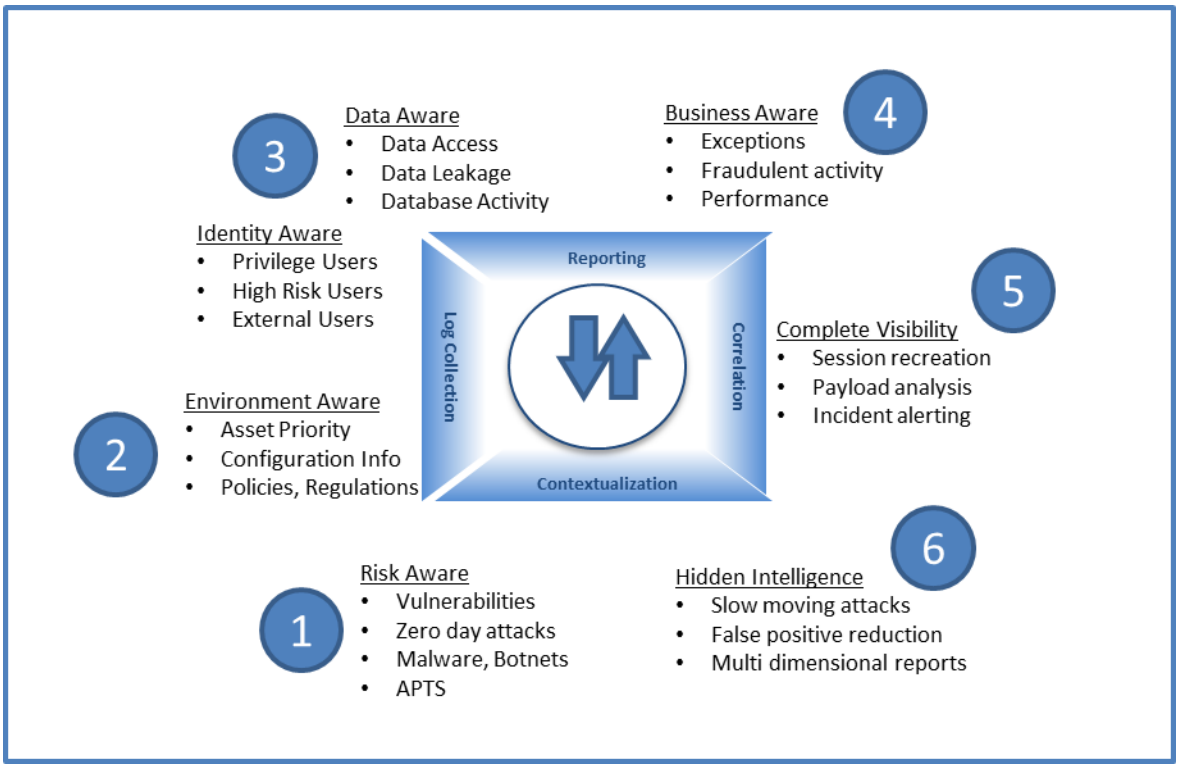
Though there has been tremendous increase in awareness, technology capabilities, market and vendor focus on cyber security, some key challenges still remain

- ✓ Evolving risk and attacks – Cyber space has evolved as the backbone for the survival of entire organizations and even entire countries and is now the basic channel for covert warfare and focused attacks.
- ✓ Increase in complexity and evolving technology landscape – With the introduction of mobility, de-parameterization and cloud adoption , new threat vectors are constantly evolving
- ✓ Dynamic business environment – IT security is still regarded as a cost center and more effort is required for it to be perceived as a business need and work in collaboration with business.
- ✓ Point solution approach – Various security solutions provide good protection against a specific security problem, however, interoperability between the various solutions is still an issue
- ✓ Significant effort and expertise – Significant effort and expertise is required in deployment, management and fine-tuning of cyber security solutions.

A unified approach to cyber security monitoring and management

Despite reasonable investment in security tools and technologies, several successful attacks have proved that something more needs to be done to effectively detect and manage the growing numbers of threats.

One of the major causes is the lack of synergy between various functions and tools within the security domain itself and across layers including physical, network, user, data and application security. Hence, in order to evolve a successful response strategy for cyber security, it is important to look at all these layers holistically and leverage the information available at every layer to develop an overall threat and response model.



Unified approach to Cyber Security

In order to ensure a unified and holistic approach to cyber security, it's important to convert data (logs, packets, policies, activities, configurations etc) available across various layers and across different functions/tools into real actionable intelligence. Some of the latest tools such as SIEM (security information and event management) have evolved on this premise and can serve as a basic building block for a unified framework.

The critical steps involved in building a unified cyber security monitoring and management framework include:

Step 1 - Risk Awareness

The most critical aspect of cyber security is to understand existing and emerging risks and threats to the business. A risk based approach will not only ensure the optimum use of investments but will also provide clear and accurate visibility of current posture. Being risk aware broadly means:

- Visibility of the existing risks – leveraging vulnerability assessment, penetration testing, configuration audits, data, applications and identity handling policies and processes etc.
- Intelligence on emerging threats – leveraging threat intelligence related to emerging attacks, known sources and patterns of attacks, targeted attacks on the industry segments etc in which the organization is operating.

Risk assessment should form the basis of all ongoing and new investments. It is also important to design all the management and monitoring processes in accordance with the identified risk to ensure correct categorization, prioritization and response to any potential security threat.

Step 2: - Environment Awareness

Environment details serve as a fundamental element for the overall cyber security monitoring and management program. Asset information and software/application details from CMDB (configuration management data base), patch level details for patch management database, IP addressing schemes and network topology, business assets by priority, allowed software and applications, applicable policies and compliance regulations not only determine the level of security required and use cases (in terms of determining the rules, access control lists, thresholds, prioritization of security events etc) but also help in responding quickly to any suspicious/confirmed incidents.

Step 3: - Identity and Data Awareness

The two most critical assets of any organization are its users and data. It's imperative for any cyber security framework to leverage and utilize the data and identity information to be able to protect against cyber threats.

- Identity and access management (IAM) solutions deployed in most organizations not only manage the entire lifecycle of users but can also provide information related to different categories of users including administrators, super users, contractors etc.
- Various data security solutions like data leakage protection (DLP) and database activity monitoring (DAM) can help track and monitor any unauthorized and suspicious use or leakage of data.

The integration of identity and data information in the framework will help to define the right level of data access levels, track and monitor privileged and disgruntled user activities, identify unauthorized entitlement changes and unauthorized data access/loss.

Step 4: - Business Awareness

Most of the current efforts in cyber security monitoring and management focus more on the infrastructure, host layers and security products. While these are critical elements, they exist solely to support business and business applications. It is important for the security team to understand the business context and build capabilities to detect and respond to any threats that can impact business applications (including packaged apps, web apps and custom apps).

The traditional security tools do not have the integration and inspection capabilities for business contexts (though they can still carry out traffic inspection for protocol level anomalies and code level anomalies). In order to extract and use the information relevant to security, a separate intelligence engine is required. Such an engine should have the ability to look at transactions logs and audit logs to determine fraudulent activities and anomalous patterns and correlate this information with other layers to identify relevant threats and attacks. Tools like Splunk and Apache Lucene can be used to build such inspection engines.

Step 5: - Content Visibility

Security tools operate at different levels when it comes to the logging of actual content. While a SIEM solution typically works at the audit log level, an Intrusion Detection and Prevention Systems solution actually logs the entire packet detail at the network level. Many times, working only at the log level or isolated packet level does not provide the complete context for getting the desired level of visibility.

In order to build complete visibility across the network, details of actual data traversing the network can answer most of the requirements including identification of threats and anomalous behavior, faster incident response and forensic and legal analysis. Such a solution has the ability to capture all the traffic traversing the network across the desired segments, create alerts on suspicious behaviors and recreate the complete session details to pin point the exact issue.

Step 6: Hidden Intelligence

Though SIEM tools and packet capturing tools have solved the issue of collecting and storing data for purposes of reporting, investigation etc, the amount of data generated in today's organizations can easily overload these tools and prevent any intelligence from being generated. Big Data platforms are evolving as very useful tools to address a lot of business intelligence and data mining applications and it is also possible to use these platforms for the purpose of security intelligence.

Using Big Data platforms and tools, it is now possible to generate trends and carry out pattern analysis over a very large set of data, which can help in identification of slow moving attacks, building statistical

machine learning models for predictive behavior analysis, identify any bottlenecks with regard to capacity, performance, availability etc.

Most importantly, for any cyber security solution to work, it must be managed effectively and evolve continuously. Deployment of point solution products and security technologies do not serve the purpose if they are not continuously updated and fine-tuned. Similarly, the overall cyber security framework should be capable of being upgraded and flexible enough to add new innovations, scale to meet new technology architecture like cloud, mobility and evolve to counter the latest emerging threats.

Conclusion

Countering focused and targeted attacks requires a focused cyber security strategy. Organizations need to take a proactive approach to ensure that they stay secure in cyber space and adopt a robust cyber security strategy which should be:

- Risk driven: To ensure continuous awareness and mitigation of existing and emerging threats and risks
- Holistic: To cover all the layers including infrastructure, applications, data and users
- Adaptable: To address new business models and threats
- Efficient: To support business dynamics, utilize existing investments and maximize return on investment
- Collaborative: To leverage the expert knowledge and experience

Credits and References

- IBM X-Force 2012 Cyber Security Threat landscape
- Content Aware SIEM Defined – by Dr. Anton Chuvakin and Eric D. Knapp
- Oracle Information Architecture: An Architect's Guide to Big Data
- Splunk for Application Management – Splunk
- The Business case for a Next-Generation SIEM – IBM(Q1 Labs)
- Apache Hadoop and Sub-projects

About Happiest Minds

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Cyber Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

To know more about our offerings. Please write to us at **business@happiestminds.com**

About the author

Vijay Bharti (Vijay.bharti@hapiestminds.com) heads the infrastructure security practice at Happiest Minds Technologies Pvt.Limited. He brings in more than 15 years of experience in the area of IT Security across multiple domains like Identity and Access Management, Data Security, Cloud Security and infrastructure Security. His recent work includes building Security operation center frameworks (including people, processes and various SIEM technologies) where he is working on building an i nw teogf seeratecud rivity and ways of leveraging advance analytics and big data innovations for cyber security.

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**