ARUP CHATTERJEE
CHIEF INFORMATION
SECURITY OFFICER

ADOPTING A MANAGED SERVICES APPROACH TO SIEM

Extending Your Enterprise

User Admin
Pass

ADOPTING A MANAGED SERVICES APPROACH TO SIEM

ARUP CHATTERJEE
CHIEF INFORMATION SECURITY OFFICER

The year 2016 saw a slew of security incidents, at the receiving end of which were large organizations, government departments and individuals. Sophistication in technologies coupled with security flaws, has enabled cybercriminals to launch audacious attacks which have rendered companies vulnerable to repeated network and data intrusions.

In October 2016, cybercriminals mounted major Distributed Denial of Service (DDOS) attacks, temporarily crippling a host of websites, including the likes of Twitter, Netflix, PayPal, Pinterest and the PlayStation Network, amongst many others[1]. Though the impact of this attack was short-lived, the scale of the attack (involving multiple compromised systems and measuring upto 1 TBPS at one time) is what made it overwhelming. The real implications of this sort of attack are however far reaching, with Gartner predicting that there will be 20.8 billion 'connected' things talking to each other by 2020.

Just a few months earlier, CNN had reported that cyberattackers had released data on 10,000 Department of Homeland Security employees one day, and then released data on 20,000 FBI employees the next day[2].

Indeed, these were just a few of the many well-publicized instances of network attack and data breach that rocked 2016. As much as the inability of organizations to insulate their networks made headlines, the ability of sophisticated cyberattackers to mount such well-orchestrated attacks at will has caused a sense of both surprise and panic. This has again put the spotlight on organizations and their approach to Security Information and Event Management (SIEM), raising pertinent questions about their ability (or the lack of it) to proactively identify, analyze and act during episodes of security violations.

As much as the inability of organizations to insulate their networks made headlines, the ability of sophisticated cyberattackers to mount such well-orchestrated attacks at will has caused a sense of both surprise and panic

[1] http://www.welivesecurity.com/2016/12/30/biggest-security-incidents-2016/
[2] http://www.welivesecurity.com/2016/12/30/biggest-security-incidents-2016/

A Comprehensive SIEM Can't be an Afterthought

SIEM is growing in importance and this can be gauged from the fact the global SIEM market is expected to grow to USD 4.5+ Billion by 2019. According to IDC, a premier global market intelligence firm, the key areas for (cybersecurity market) growth are security analytics / SIEM, threat intelligence, mobile security, and cloud security[3].

Many organizations today are handicapped by legacy SIEM systems, which are merely focused on collecting and managing logs, and meeting basic compliance needs

Understandably, organizations today are fighting a dual battle of thwarting hackers and malware, and contending with the deluge of data from their own networks. Against such a complex backdrop, it is imperative for enterprises to implement a comprehensive SIEM program that will enable real-time monitoring of security events, use of analytics and historical analysis for incident investigation and compliance reporting. However, many organizations today are handicapped by legacy SIEM

[3] http://cybersecurityventures.com/siem-report-2016/

systems, which are merely focused on collecting and managing logs, and meeting basic compliance needs. They simply lack the intelligence and threat-monitoring capabilities that SIEMs need to have in a complex threat landscape. Another significant roadblock that organizations face is the lack of expertise that will help realizing the benefits of SIEM solutions.

These inherent inadequacies have prompted organizations to look at SIEM as part of a managed services setup, which gives them access to the latest technologies (including automation and analytics), security and data experts, and industry best practices. Apart from obvious cost benefits, this approach spares organizations the responsibility of constantly planning, monitoring and bringing in critical technology upgrade.

The WNS SIEM Narrative

WNS Global Services serves more than 200 customers worldwide and is obliged to meet several regulatory and contractual requirements of its clients as well as information protection mandates. WNS embarked on a journey towards implementing a comprehensive SIEM program and a state-of-the-art WNS Global Security Operations Center (WNS GSOC) — from the ground up and on an accelerated path driven by security goals and evolving market opportunities. The diverse and complex nature of WNS operations (multiple geographies and serving a wide range of industries) makes effective IT threat management a critical capability, much beyond simply demonstrating compliance. The WNS SIEM platform was built on the Arcsight ETRM technology which was shortlisted based on extensive research and product evaluations. The key attributes for selection included flexibility of deployment, integration with commercial security products, ease of log collection and visualization, bandwidth optimization for log collection from remote locations over WAN with minimal use of precious bandwidth, capacity and scale to deal with high volumes of data (events per second), and the intelligence for generating humanly-interpretable log information. WNS scope of SIEM deployment at the early stages included consolidation of events from across its 100+ Windows active directory servers, over 500 firewalls and network devices, 40 intrusion prevention sensors, antimalware servers, DLP platforms and custom log collection from application databases and physical security access control systems.
The consolidation of events from all these different sources under one umbrella was necessary for real-time visualization of attacks taking place in our environment and also to enable compliance reporting to ease internal and external audit requirements such as PCI DSS, SOC 1 and SOC 2.
The key was to establish a SIEM platform integrated with active cyber threat intelligence combined with real-life use cases based on the cyber kill chain that provided actionable intelligence from real-time analysis and ability to react to incidents and threats with an orchestrated approach. SIEM integration with Active Directory was intended at discovering user behavior patterns and early warning signs of account misuse and violations across its 33,000+ strong employee workforce distributed across the globe. WNS' GSOC with Arcsight implementation has been immensely successful and is validated under the PCI DSS, SOC and ISO 27001 compliance programs.

Conclusion

The proliferation of digital resources and greater connectivity among devices makes establishments and their network vulnerable to cyber intrusions. Safeguarding against such threats warrants application of SIEM in its most holistic form to drive early detection of targeted attacks and data breaches. Needless to say, the role of automation and analytics becomes extremely critical to the functioning of SIEM and its ability to uncover unknown threats.

From an organization's perspective, it is just not about implementing any SIEM solution but implementing the right solution that is aligned with the existing threat landscape and that can be adapted to meet any change thereafter. For organizations that are attempting to build a SIEM solution from the ground up or re-evaluating the existing SIEM solution, they need to be mindful of the possibility of partial or failed deployment which can jeopardize the state of security. Moreover, SIEM as a domain requires specialized skillsets, including the ability to examine data, knowledge of systems across the IT infrastructure, experience with nearly all security point solutions, and the ability to define and analyze threat correlations.

This necessitates that enterprises tie up with partners who bring the right kind of industry expertise, expert analysts and technological know-how to deliver a highly scalable, intelligent and customized solution. SIEM is an ongoing activity which warrants impeccable scrutiny and monitoring, and by going the managed services way, organizations can bring in sophistication and expertise to heighten security, while saving on costs.

CYBER
SECURITY
CONFIRM
click here for more informati

About WNS

WNS (Holdings) Limited (NYSE: WNS) is a leading global Business Process Management (BPM) company. WNS offers business value to 200+ global clients by combining operational excellence with deep domain expertise in key industry verticals, including banking and financial services, consulting and professional services, healthcare, insurance, manufacturing, media and entertainment, retail & consumer packaged goods, telecom and diversified businesses, shipping and logistics, travel and leisure, and utilities. WNS delivers an entire spectrum of business process management services such as customer care, finance and accounting, human resource solutions, research and analytics, technology solutions, and industry-specific back-office and front-office processes. WNS has delivery centers world-wide, including China, Costa Rica, India, the Philippines, Poland, Romania, South Africa, Sri Lanka, Turkey, UK and US.

To know more, write to us at marketing@wns.com or visit us at www.wns.com

Extending Your Enterprise