Introduction

> New security threats are emerging all the time, from new forms of malware and web application exploits that target code vulnerabilities to attacks that rely on social engineering. Defending against these risks is an ongoing battle. In response, the array of security technologies available has also grown. While we are familiar with essential defenses such as network firewalls and antivirus software, more sophisticated solutions are harder to evaluate. Intrusion detection, SIEM, Web application firewalls—which are right for your organization, and how do they work together to prevent data breaches, downtime and the business consequences of a successful attack?

> In this white paper we will discuss how vulnerability assessment, network intrusion detection and log management work together to protect your IT assets. We will do so in the context of the Vulnerability Life Cycle—a model to understand how attackers find and leverage vulnerabilities to attack their targets. In doing so, we will provide insight into how you can use these different technologies to identify attacks, prevent them and recognize and remediate successful attacks.

The Vulnerability Life Cycle

> What is the Vulnerability Life Cycle? This model is a helpful framework to understand how vulnerabilities in systems and applications become points of entry for attackers—when your risks are greatest—and how to appropriately defend yourself.
A vulnerability is simply a weakness in a system or application that can be exploited to gain unauthorized access to resources and data. Typical examples of vulnerabilities include:

- The ability to access a server’s physical environment
- Improper input validation in a Web form, which allows an attacker to inject code into an application
- Misconfigurations that provide an unauthorized user with more privileges than a system designer intended
- Buffer overflows in which an application overruns a memory buffer and overwrites adjacent memory

Vulnerabilities are common—a recent Ponemon Institute survey found that 7 in 10 application developers believe that security is not adequately addressed in their development process, and as many indicated that their applications have been compromised by security breaches. As a result, software and systems developers are constantly identifying and patching vulnerabilities to protect their users.

The Vulnerability Life Cycle provides a view over time of a vulnerability’s origin and correction and the relative risk during each stage of the cycle.

Pre-Discovery

- The pre-discovery period is the period from the origin of vulnerability—when a vulnerable product is released—to the point where it is discovered. Vulnerabilities can be discovered by developers who created the code, by third parties who report the vulnerability to a developer, or in the worst case, by cybercriminals who use this unique time to exploit it (a zero day attack).
- During this period, the number of impacted systems is high, but risk is relatively low. Attackers are probably unaware of the vulnerability, and no automated tools have been created to exploit it.

Discovery Through Correction

- Once a vulnerability is discovered, risk increases. At this point, attackers are likely to develop exploits to take advantage of the vulnerability, in order to compromise target systems during this high-risk stage.
- This stage ends when the vulnerability is corrected, typically by patching. However, even if a patch is quickly released, risk remains until the patch is applied to all vulnerable systems. This points to the importance of patch management—it is a complex process to manage, and typically many systems remain unpatched (and at risk) for some time after a patch is available. While the number of vulnerable systems begins to decrease after universal patch adoption, all users must be on guard for attacks.

Post-Correction

- After a patch has been applied, the risk of compromise drops significantly. However, some systems may be compromised before correction.
- The potential for an existing compromise to continue after vulnerabilities are corrected is significant. For example, an attacker could have already installed a rootkit that phones home before the holes are plugged.
> In its annual *Data Breach Investigation Report*, Verizon provides data on the time between compromise of a system and discovery of the compromise by the business that owns it. For 40 percent of breaches, the gap is measured in months or years—a period during which an attacker has access to data and resources without the owner’s awareness.

> In fact, savvy attackers will try to remain undetected after a breach to maximize the time they can use their victims’ systems.

> During each stage of the Vulnerability Life Cycle, different technologies can help you protect yourself and identify attacks. Let’s understand what those technologies are.

### Alert Logic Threat Management

> Alert Logic’s threat management solution is a fully managed intrusion detection system (IDS) with vulnerability assessment (VA) via integrated scanning. It is a combination of technology and services.

> Alert Logic Threat Manager is a software-as-a-service IDS/VA product that monitors all network traffic and analyzes it through a signature-based expert system. Threat Manager appliances in your environment monitor traffic and use intelligent multi-factor correlation based on a database of known threat signatures to identify attackers.

> ActiveWatch for Threat Manager provides the intelligence to identify real risks and escalate them appropriately. Alert Logic GIAC-certified security analysts respond to all incidents identified by Threat Manager and evaluate their severity. Analysts then escalate incidents appropriately. For serious risks, you are notified immediately via phone, and are provided with recommendations for protecting yourself from the attack. For less severe incidents, an email notification is sent.

> This approach removes the biggest challenge of effectively using IDS by itself—identifying the significant incidents out of a vast number of network events and disregarding the false positives. The combination of Alert Logic’s expert system and analysts provides top security expertise and 24x7 monitoring that are difficult to replicate in-house without a significant investment in a large team and technology resources.

> Integrated into the threat management solution is a vulnerability scanning service. This provides unlimited internal and external scans of your networks to identify uncorrected vulnerabilities. These scans are similar to those that attackers will use to find vulnerabilities to exploit, and will allow you to correct problems before they become paths to compromise. Vulnerabilities are identified but not exploited, as they would be a more invasive approach, such as a penetration test.
Alert Logic Log Management

- Alert Logic’s log management solution enables you to collect, normalize and analyze the vast volumes of log data created by your devices, systems and applications. Audit logs contain valuable data that can reveal the fingerprints of attempts to compromise systems or the results of an existing breach; however, the volume of data and the complexity of parsing it for analysis across different systems makes using that data a challenge.
- Alert Logic’s Log Manager provides analysis and alerts through a Web-based interface. You can access reports on log data and set threshold alerts for warnings of suspicious activity. For example, log data indicating hundreds of unsuccessful attempts to log into an administrator account within two minutes suggest that an automated brute force attack is underway.
- LogReview provides additional assistance in managing log data by providing a daily report prepared by one of Alert Logic’s security analysts. LogReview reports provide insight into any unusual patterns in log data that help identify attacks.
- In addition, all log data is securely stored for one year (or longer, if required), to assist with compliance requirements. Archived log data can be easily retrieved for the Department of Justice or other law enforcement agencies.

Pre-Discovery Awareness and Defense

- During this stage, vulnerability assessment (with Alert Logic Threat Manager) and log analysis (with Alert Logic Log Manager) are important tools.
- Vulnerability scanning helps you identify unknown vulnerabilities in your infrastructure, such as unpatched software or misconfigured systems with default passwords. Threat Manager relies on a database containing thousands of known vulnerability signatures to scan every system in your environment, testing for problems and presenting them in consolidated reports to guide remediation efforts. The database is constantly updated with the creation of new signatures for new vulnerabilities, Trojans and malware discovered by Alert Logic’s security research team as well as other security teams.
- Analysis of log data provides further insight into problems in your environments. Log data provides a trail of evidence of attempts at network compromises or improper application behavior.
Defense After Discovery

> Once a vulnerability is known but before it is corrected or mitigated, vigilance against exploit attempts is critical. Alert Logic Threat Manager with ActiveWatch provides 24x7 intrusion detection, analyzing millions of security events through its expert system’s intelligent multifactor correlation capabilities. The expert system is able to identify almost 95 percent of the traffic; the remaining 5 percent is flagged as either a threat or a false positive depending on the data. That remaining 5 percent of traffic is analyzed by Alert Logic’s security analysts who validate incidents, alert you to them and provide guidance on recommended responses and mitigation strategies.

Post-Correction Incident Identification

> After a vulnerability has been corrected, risk of a compromise based on that vulnerability is mitigated. However, the possibility of a breach related to other, still unknown vulnerabilities remains. Zero day attacks on unknown vulnerabilities also fall in the 5 percent of false positives and alerts that the system generates. Suspicious traffic patterns cause alerts and are reviewed by analysts.
> Log analysis with Alert Logic Log Manager can help you identify unauthorized activity, and if a breach is known to have occurred, provide important post-incident forensic data to guide your investigation and analysis.

Conclusion

> The Vulnerability Life Cycle illustrates the risk for a single vulnerability, from its introduction to correction and beyond. It is important to remember that this cycle repeats for every vulnerability, and at any single moment, different vulnerabilities are at different points in the cycle. Since vulnerabilities live and die with the product, some just get antiquated or become non-threats if the product is discontinued or changed dramatically.
> Regular vulnerability assessment, consistent review of log data, and 24x7 intrusion detection monitoring are powerful tools to help you protect yourself at all points in the Vulnerability Life Cycle. In addition, these tools provide valuable insight into real attack vectors within your environment, offering important guidance when setting priorities for other security technologies.

About Alert Logic

> Alert Logic, the leading provider of Security-as-a-Service solutions for the cloud, provides solutions to secure the application and infrastructure stack. By integrating advanced security tools with 24x7 Security Operations Center expertise, customers can defend against security threats and address compliance mandates. By leveraging an “as-a-Service” delivery model, Alert Logic solutions include day-to-day management of security infrastructure, security experts translating complex data into actionable insight, and flexible deployment options to address customer security needs in any computing environment. Built from the ground up to address the unique challenges of public and private cloud environments, Alert Logic partners with over half of the largest cloud and hosting service providers to provide Security-as-a-Service solutions for business application deployments for over 1,800 enterprises. Alert Logic is based in Houston, Texas, and was founded in 2002. For more information, please visit www.alertlogic.com.