Security Information and Event Management: How do I implement SIEM on a budget?

Z&Z Insurance Brokerage*, an insurance company with 200 employees spread over 5 offices, faced regular critical system outages and malware attacks that threatened business operations, reputation, employee morale and required significant costs outside of budget.

After a full assessment, Z&Z* decided that implementing a solution for logging network activity and monitoring user access across the enterprise would help them deal with their challenges. Kalki worked with Z&Z* to evaluate their biggest monitoring challenges, assess their needs from a logging solution and select and implement a tool.

Challenges

Issues

- Lack of audit trail
- Network Interruptions and access issues
- Risk of un-noticed malicious activity
- Inability to diagnose and prevent future network issues
- Lack of budget for a full-scale enterprise logging and monitoring solution

Impact

- Regular network outages and downtime
- Compliance issues
- Lost revenues

Solution

Kalki worked with Z&Z* to balance the needs of the business with the cost of implmenting a logging solution. Kalki provided a full breakdown and comparison of various solutions and worked with the client to select the best fit.

Prior to solution implementation, Kalki restructured the network elements as required and prepared the environment for the addition. An ArcSight Logger appliance was installed, configured and fully tested in Z&Z's* network.

Key Facts

Challenge-

- Industry: Insurance
- Regulations: Financial Services & HIPAA
- Network outages and downtime
- Inability to diagnose network issues and track user access

Solution

- Needs review and assessment
- Solution comparison and breakdown
- Network restructuring
- ArcSight Logger installation
- Logging and monitoring ruleset creation and implementation

Results

- Measurement and monitoring of all network and infrastructure elements
- Monitoring for malicious activity
- Regular real-time alerting for high risk issues

17 State Street / 40th floor / New York, NY / 10004 / KalkiConsulting.com / 855.GO.KALKI / 855.465.2554 / DOC.NUM.001.2015

KALKI

Services

Kalki's provided the following services to Z&Z Insurance Brokerage*:

- Logging and monitoring environment needs review and assessment
- Full review of current tools
- Solution comparison and breakdown by feature-set and cost
- Network architecture redesign and restructuring
- ArcSight Logger installation
- ArcSight Logger configuration and implementation
- Logging and monitoring ruleset creation and implementation

Results

Z&Z* is now actively able to measure and monitor:

- Total failed logins on perimeter devices
- Antivirus tool policy breaches
- Policy breaches by specific user (any possibly malicious downloads)
- Potential cryptolocker variant oubreaks
- Consolidated updates from business critical applications

Z&Z* now regularly receives alerts regarding:

- ArcSight configuration changes to environment or setup to prevent unauthorized changes
- Alerts for 3 failed logins on across all network and infrastructure within 60 seconds
- Antivirus poilcy breaches (pulled from the antivirus tool)

> *Having SIEM capability, even limited, allows an organization to derive meaningful and actionable information from the their latent event log data. Prior to implementation, these logs were not stored or managed properly and were scattered across various disparate systems. The addition of the logging and monitoring appliance has allowed Z&Z* to more effectively manage their exposure to risk.*
> *- Kalki Technical Lead*

The Road Ahead

Z&Z* is now in a place where they are able to track and maintain an audit trail of user activity as well as proactively monitor network activity and prevent network issues. All major devices and systems within Z&Z's* network send event log data to the Logger for aggregation and alerting, bringing all the information to a centralized location and allowing for intelligent real-time analysis of network and user activity.

The ArcSight Logger implementation has the ability to recognize many attack types and prevent issues before they begin. Z&Z* is now armed with alerts to notify them of malicious activity in addition to the network monitoring capabilities of other tools. Z&Z* has been provided with the tools and processes by which to handle and escalate any issues found by the logging system.

About Kalki

Kalki was founded specifically to serve the needs of the 'underserved', by offering effective, affordable, expert security-focused IT advice to small-to-medium sized businesses (SMBs) who want to protect their futures. Our SecurITy Services help **A.R.M.** our customers with the right tools, processes and skills to ensure that their future is protected.

Assess
Regain control of your technology

Respond
Maintain control and proactively manage risk

Monitor
Focus on what you do best

*Disclaimer: Client names withheld to ensure confidentiality

17 State Street / 40th floor / New York, NY / 10004 / KalkiConsulting.com / 855.GO.KALKI / 855.465.2554 / DOC.NUM.001.2015

KALKI