

# Fully Managed SIEM Solution



## Speed Up Your Incident Response & Control Your Organization's Cyber Risk With A Fully Managed SIEM

A tremendous amount of effort goes into deploying and maintaining a SIEM solution, on top of the ongoing training and enablement of your own security team. Let us handle the difficult work for you.

Our dedicated security engineers handle all aspects of a Fully Managed SIEM deployment as well as the monitoring and optimization necessary for effective incident management. We offer a choice of several SIEM solutions tailored to best fit our clients' needs, often eliminating the need for other security tools in your environment.

### What's Included In Our Fully Managed SIEM?



#### Managed SIEM

Utilizing our managed SIEM tool allows your organization to effectively allocate your IT staff, allowing them to focus on core business needs and new projects while providing peace of mind, knowing that your environment is efficiently managed and constantly monitored for any compromise.



#### Compliance Monitoring

Our monitoring tool assesses your adherence to your organization's policies and procedures, governing activities that pose compliance risk to your business and helps the business effectively manage risks on an ongoing, real-time basis.



#### Log Collection

Logs are collected from event sources throughout the IT environment of your organization. The logs are then forwarded to other Security Analytics devices, where they are stored as metadata for use in investigations and reports.



#### Log Retention

Our log retention service provides full lifecycle management of your chosen log retention technology, assuring that your log retention tool will allow you to **Achieve and/or maintain your PCI-DSS, FISMA or HIPAA compliant status.**



#### Incident Response

Our IR Plan encompasses the six key phases that are defined in **NIST-SP 800-61**: Preparation, Detection, Containment, Investigation, Remediation, Recovery



#### Event & Intelligence Correlation

Regardless of whether the events are associated with end-user experience, business processes, application performance or technology performance, effective event correlation will pinpoint the specific cause of any event storm.

### Key Benefits:

Deploying and maintaining a SIEM is time-consuming and requires specialist skills many businesses don't have access to. MegaplanIT's dedicated security engineers ensure your business has a powerful, optimized Fully Managed SIEM running **24/7/365**. Some of the key benefits you will receive with our Fully Managed SIEM Service:

- ✓ Fully Managed Security Stack
- ✓ Real-Time Incident Response
- ✓ Daily Compliance Reviews
- ✓ Early Threat Detection
- ✓ 24/7/365 Staffing & Service Availability
- ✓ Expand Your Existing Resources
- ✓ Deep Environment Visibility
- ✓ Scale For The Future