PROFICIO

SIEM Services Capabilities Review

The Proficio Team

- Multiple Master Solution Architects each with over 5 years experience as ArcSight senior SIEM services professionals
- Experienced SOC and NOC Analysts, and Security Engineers
- Certified security professionals
- Senior SOC Managers previously from high profile industry-leading companies
- Hundreds of successful SIEM implementations
- Extensive use case experience

Architecture Review and Design: Project based

- Expert review and consulting of existing architecture, policies and procedures
- Operational assessment and consulting
- Performance evaluation and tuning

SIEM Fast Start Implementation: 5-15 Days On-Site

- SIEM implementation over server and up to 8 log source types
- Default content tuning
- Network modeling
- Asset modeling
- Custom content and use case development
- Ad-hoc training

Compliance Management Package Consulting: Project based

- PCI
- SOX
- FISMA
- ISO
- HIPAA
- NIST

VSOC: Virtual Security Operations Center

- Uses your SIEM and Proficio SOC Analysts to monitor events
- Proficio experts and experienced Security Analysts monitor events and provide Tier 1 through Tier 4 alert and response based on SLA's

FlexConnector Development and Maintenance for custom applications: Project Based

- Develop FlexConnectors for integrating customer log sources into SIEM
- Add or modify correlation rules and reports as necessary
- Maintain FlexConnector as log source is updated during lifecycle

Operationalization and Advanced SIEM/SOC Consulting and Staffing:

- Complete roll-out of SIEM connectors to all applications and devices
- Review all security operations, policies, & procedures to integrate security functions into SIEM capabilities.
- Develop new procedures when necessary.
- Review all log policies & configurations for supported devices to ensure log alerting for complete incident investigation activities. Establish policies as necessary
- Develop notification and workflow policies and procedures
- Review all metric requirements and create / automate report and dashboard generation and delivery
- Build new security capabilities based on SIEM features.
- Provide advanced solutions to satisfy various security and compliance objectives
- Provide a series of advanced workshops for core security staff and data consumers

Operations and Maintenance of SIEM – Managed Services: Annual Subscription

- Proficio Operation & Maintenance (O&M) service provides comprehensive administrative support with qualified resources in a secure co-manage 'partial FTE' delivery model.
- Proficio O&M allows customers to focus on ArcSight solutions instead of ArcSight maintenance

- **Regular Maintenance**
  - Maintain covered ArcSight software and appliances with the latest software releases, patches, hotfixes and other updates
  - Quarterly and annual performance evaluations, architecture reviews, and operational reviews
  - Robust reporting on all maintenance activities

- **Health & Performance Monitoring Services**
  - Monitor covered ArcSight software and appliances for availability, performance and other issues
  - Triage and handle all ArcSight tickets on behalf of customer
  - Robust reporting on all monitoring activities

- **Expert-on-Call**
  - On-Call block hours for extended repair situations
  - Time may be used for authoring new rules & reports

Advanced SIEM Rule/Application Development: Project Based

- Proficio has developed Reference Architectures for several advanced use cases that are operationally proven in the field
  - Cloud application monitoring
  - SaaS application monitoring
  - Fraud analysis
  - Smart grid monitoring

Cloud Application Monitoring:

- Monitor your applications in Amazon or Microsoft Cloud environments
- We have experience in, and proven reference architectures to monitor services and applications

SaaS Application Monitoring:

- Custom FlexConnector development and advanced correlation rule authoring
- Monitor application and transactions for miss-use, and account take-over

Fraud Monitoring for your applications and services:

- Real-time advanced correlation rules are capable of discovering, alerting and preventing many forms of fraudulent transactions
- We have experience in developing advanced fraud monitoring with SIEM

Smart Grid Monitoring:

- SIEM tools are capable of monitoring utility Smart Grid environments
- We have experience with this advanced use case at major utilities

Synchronization Tool and Consulting for Syncing Multiple SIEM Instances:

- Proficio has created a tool using ArcSight supported API's to sync content
- Project Based Consulting Services in addition to tool license

Health Check and Tune-Up: 3-5 Day On-Site

- All SIEM's require a semi-annual review of the system set-up, rule changes, process, and performance.
- Our SIEM experts will review your SIEM for optimum performance and accuracy of data

Use Case Workshop: 3-5 Day On-Site

- Our SIEM experts lead business discussion to evaluate your SIEM can automate new or existing security or intelligent data analysis
- During the course we will develop new correlation rules and process for creating up to 3 new Use Cases

Proficio Inc.
17551 Gillette Ave
Irvine, CA 92614

800-779-5042 – Phone
408-904-4905 – Fax
info@proficio.com – Email
www.proficio.com – Web

PROFICIO
SECURITY AND NETWORKING SOLUTIONS