Samsung SDS

Security Architecture Assessment

Assessment and Consulting on Security Monitoring System to Enhance Security Monitoring Capabilities

Background

Needs for the Assessment of Security Monitoring System

Risks of web hacking, web shell, DDoS, malicious code, and APT attacks are constantly rising

Need to establish operational processes such as incident responses

Need to strengthen security monitoring systems and establish improvement models

Service Overview

Assess existing and new security architecture using market-proven architecture assessment framework and support making improvements

Key Features

Samsung SDS's Unique Security Monitoring Process Assessment

- Assess security monitoring architecture based on SMCI[1] consisted of 4 areas (8 domains) including monitoring policy, organizational capability, processes and platforms

Assess Security Level and Identify Problems through On-site Inspection

- Identify weak points in major security monitoring functions through interview with your professionals, log sampling analysis, and inspection on security equipment operations
- Propose improvement points including security monitoring process map and implementation considerations for each area

Define Goals and Propose Guidelines

- Provide detailed goals and action items to execute improvement plan
- Monitor the progress and provide support for improvements

[1] Security Monitoring & Control Index:
A methodology for measuring the level of security monitoring, integrating international standards and Samsung SDS's know-how

Key Services

Assess Security Monitoring Architecture

Understand security policy, organizational capabilities, and operational process in detail

Discover data breaches undetected due to insufficient log analysis

Establish Security Improvement Plan

Identify gaps comparing with best practices and analyze balance across domains

Prioritize improvement projects considering ease of implementation, effectiveness, and correlations

Transplant Security Capabilities

Provide basic training courses for firewall, intrusion prevention, DDoS, and zombie virus

Provide advanced training courses for the role of security monitoring, event log analysis, and other simulation programs

As-Is Analysis	Architecture Assessment	Improvement Measures	Advisory Service
Monitoring Regulations/ Guidelines	Field Inspection and Interview by Area	Improvement Measures • Security solution • Security Monitoring System	Improvement Execution Monitoring
Detection Rules	Analysis of Undetected Hacking Incidents	Improvement Method • Analysis of information flow • Identify possible vulnerabilities • Determine inspection method	Security Operational Guidelines
Security System Log	Simulated Security Training		Security Experts Training

Benefits

Objective Assessment of Current Security Posture

Analyze gaps and balance within and across domains such as policy management, detection rule management, and incident response

Establishment of Optimal Security Architecture

Propose the best suitable to-be models for workforce, capabilities, monitoring processes and platforms

Proactive response against new security threats

Adopt detection rules and response process against the latest attacks