Samsung SDS

Homepage Monitoring Service

Homepage Monitoring Service to Detect and Block Web Hacking[1] Attacks while Performing Preventive Actions

Background

Needs for an Integrated Prevention, Detection and Response Service in preparation against Web Hacking

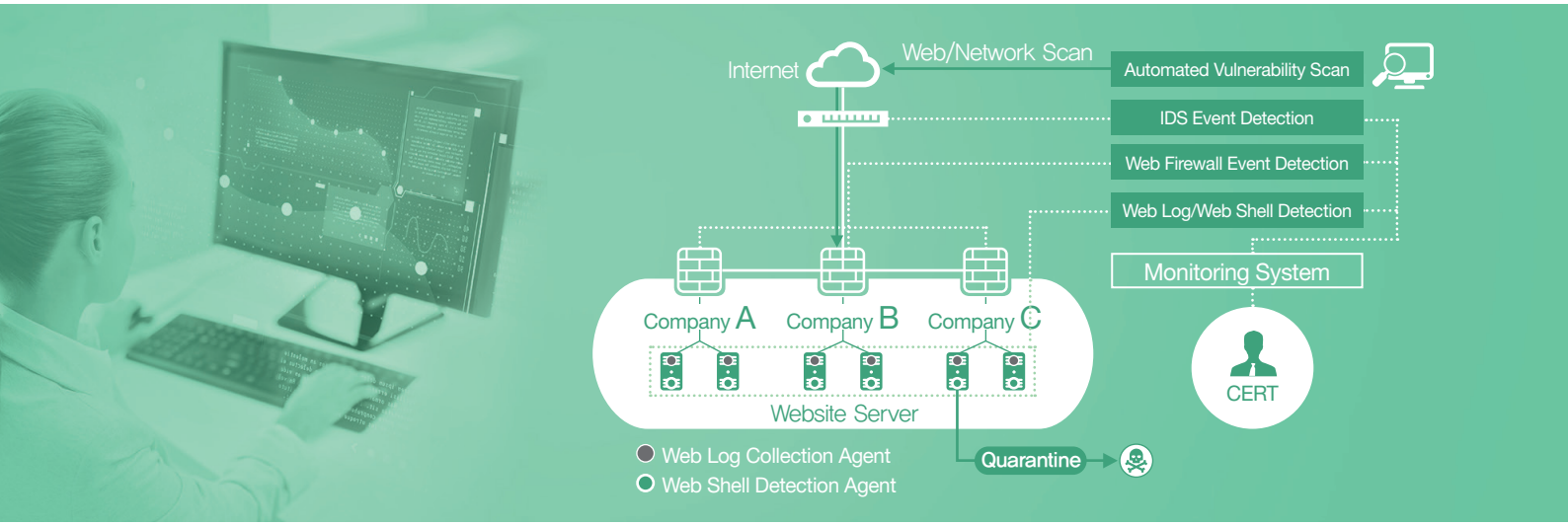
Prevention: Conduct regular diagnosis of web/network vulnerability based on up-to-date vulnerability information

Detection: Conduct an integrated analysis through IDS, web firewall, web shell, weblog agent, etc.

Response: Conduct detailed analysis and remaining vulnerability assessment by CERT for hacking detection

Service Overview

A service that supports precautionary measures and detection as well as response and post management to protect your homepage from external threats such as homepage forgery or information theft



Key Features

Automatic Web Hacking Detection at All Times

- Detect homepage hacking attempts, homepage forgery, malicious URL insertion into the web source, etc.
- Detect all new cyber threats such as zero-day exploit by the collection, analysis, ruleset development, monitoring process
- Respond to hacker attacks according to the risk level

Hacking Prevention through Automated Vulnerability Scan Regularly

- Automated network vulnerability scan
  (Detect outdated settings and OS vulnerabilities)
- Automated web vulnerability scan
  (Detect web application vulnerabilities such as unverified input value, etc.)

[1] Web hacking : An act of exploiting vulnerabilities to make unauthorized access to a webpage, leak or destroy data

Key Services

Web Traffic Analysis

Collect and analyze in real time the web traffics through web firewall and IDS whenever there is external access to the client's website

Detect attack pattern using OWASP Top 10[1]

Detailed Analysis of Infringed Website Vulnerabilities

Expert analyst provides a detailed manual assessment and response guideline to most recent targets

Google Data Leakage Detection

Detect leakage of confidential customer data such as designs, contracts or personal information by utilizing Google search

Web Log Analysis

Collect and analyze in real time the web logs within the web server whenever there is external access to the client's website

Web Shell Detection

Detect in real time any malicious web shell being uploaded within the web server home directory

Detect and quarantine any file that includes a commercial web shell[2] or a script that can be utilized maliciously

Website Screen Forgery Detection

Collect the forged and falsified information and check if the client's website is forged or not. If so, analyze the root cause

Detect forgery as a result of the stored website screen images

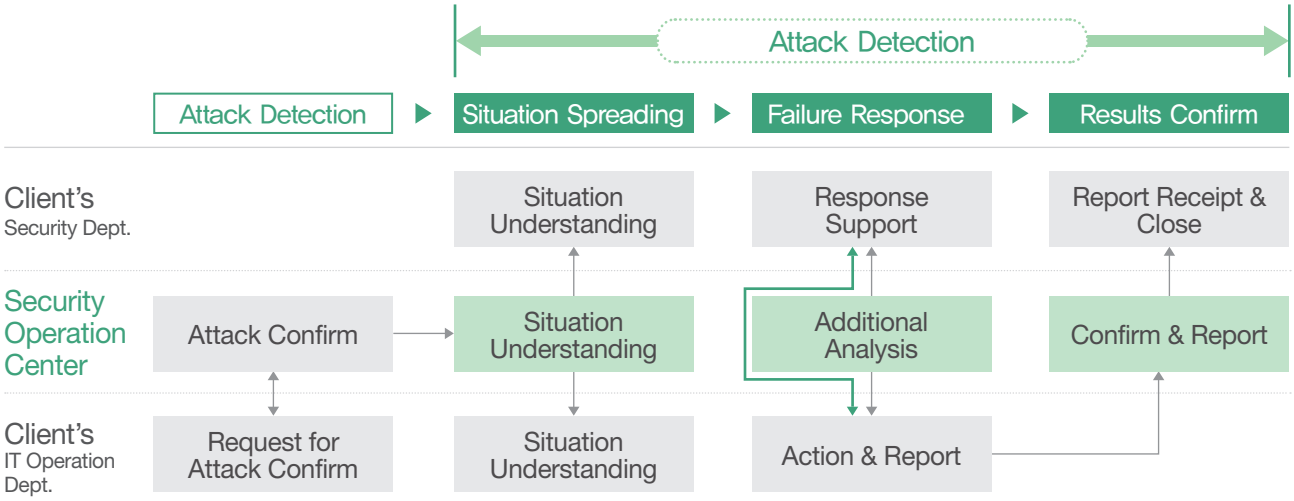
If a forgery is encountered by the screen-level comparison, detect the falsified source or malicious URL insertion through HTML web source analysis

[1] OWASP Top 10 : An open source web application security project that represents top ten web application vulnerabilities such as data exposure, malicious file, script and security vulnerabilities, etc.

[2] Commercial web shell: A malicious file created for hackers or a widely known web shell disseminated through Google search or traded in the black market

Service Process

Once a web hacking attack is identified, the Security Operation Center and the relevant client's Department run a phased response system quickly and accurately based on a standardized process.



SAMSUNG SDS SAMSUNG