Samsung SDS

Malicious Code Monitoring Service

Malicious Code Monitoring Service to Detect the Incoming Malicious Codes into the Internet and Prevent Data Leakage

Background

Needs for 'Detection, Blocking and Action' Service for Malicious Code Detection and Response

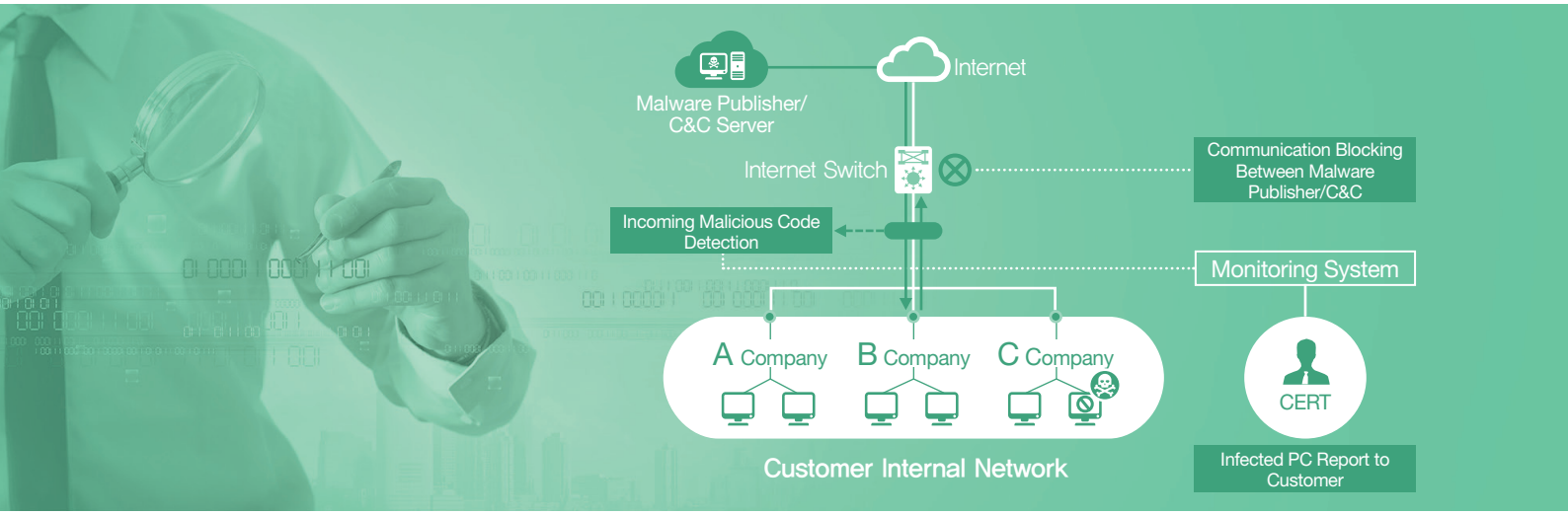
Detection: Detect the incoming malicious code into internal PC as well as malware publisher

Blocking: Block malware publisher and access attempts to C&C

Action: Provide an alert and action guidelines against infected PCs

Service Overview

A security monitoring service that detects the incoming malicious code into internal PC via internet, cuts off communication between malware publisher and C&C server[1] and prevents data leakage



Key Features

Hybrid Analytics Technique

- Combine static analysis with dynamic analysis on malicious code
- Analyze behavioral relations and reputations
- Detect a document-type malicious code utilizing vulnerability

Real-Time Threat Monitoring

- Provide greater visibility to the malignity of every detection and analysis target
- Perform intensive monitoring on interesting events (File, IP, URL)

Malicious code status analysis

- Analyze malicious code detection trend, key malware publisher/C&C server detection status

[1] C&C (Command and Control Server): A server that issues commands to the PC infected with malicious code and is used for data reception

Key Services

Examination and Detection of Widely Known Malicious Code and Suspicious File

Phase 1: Detect the incoming known malicious codes
Signature-based pattern matching technique
Phase 2: Detect new and variant malicious codes
File reputation and behavior analysis

Detection and Blocking of Malware Publisher

Detect the download URL/IP by accessing the site where the malicious code has been uploaded
Block the URL/IP in real time after verifying the malicious code infection route

Blocking of Communication with C&C Server

Block the malicious URL/IP based on new malicious code information announced by multiple sources as well as the C&C server information being collected

Classification and Notification of Risk Level of Detected Malicious Code

Notify the risk level of the incident as either emergency or warning to the customer

Vaccine Engine Update

Request the vaccine company to update the engine whenever new malicious code is detected
Provide the diagnosis title and newest version of vaccine

Service Process

Whenever malicious code 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.