AhnLab
SiteGuard Security Center

사용설명서

세상에서 가장 안전한 이름 Ahn 안철수연구소

일러두기

2009년 6월 22일 제 1판 발행

표기 규칙	표기 규칙 내용
SiteGuard Security Center	AhnLab SiteGuard Security Center의 약칭입니다.
< >	창의 이름입니다.(예: <설치 확인>)
->	메뉴 실행 순서입니다.(예: **시작->프로그램**)
굵은 글꼴	버튼 이름, 창에 나오는 메시지입니다.(예: **확인**)
참고	프로그램을 사용할 때 참고할 사항입니다.
주의	프로그램을 사용할 때 주의해야 할 사항입니다.

고객지원

(주)안철수연구소에서는 고객만족센터와 홈페이지를 통해 정품 등록 사용자가 프로그램을 사용하면서 느끼는 의문 사항이나 사용 방법, 프로그램 오류에 대하여 상담 서비스를 제공하고 있습니다. 상담을 요청하기 전에 다음과 같은 내용을 미리 확인하면 더 빠르고 정확하게 문제를 해결할 수 있습니다.

고객 지원을 요청하기 전에 확인할 사항

- ❖ 온라인 도움말이나 사용설명서를 확인하십시오. 온라인 도움말과 사용설명서는 SiteGuard Security Center의 사용과 관련하여 많은 정보를 담고 있으니 상담 전에 먼저 확인해보시기 바랍니다.
- ❖ 사용하고 있는 제품이 정식으로 등록된 제품인지 확인하십시오. 제품 번호를 정식으로 등록하지 않고 사용할 경우에는 상담 서비스를 이용할 수 없습니다.

고객만족센터 연락처

- ❖ 안철수연구소 홈페이지: http://www.ahnlab.com
- ❖ SiteGuard Security Center 홈페이지: http://sc.siteguard.co.kr
- ❖ 기업고객 핫라인: 02-2186-3082
- ❖ 1:1 메일 상담: http://www.ahnlab.com의 고객지원->1:1 메일 상담
- ❖ 주소: 150-869 서울시 영등포구 여의도동 12번지 CCMM빌딩 6층 (주)안철수연구소 고객만족센터 담당자앞

목차

1장
시작하기

1

SiteGuard Security Center 소개

SiteGuard Security Center는 사용자 PC에 설치되어 있는 SiteGuard의 설치 현황, 인터넷 변조 현황, 위험 웹페이지 접속 현황을 파악하고 차단할 웹페이지 목록을 설정하여 중앙에서 일관된 보안 정책을 수립하고 적용하도록 도와줍니다. 보안 사고는 내부 사용자들이 무분별하게 접속하는 웹사이트나 파일 다운로드를 통해 발생하는 경우가 많습니다. SiteGuard Security Center의 정책 관리를 이용하면, 자사의 보안 정책에 따라 위험하다고 알려진 웹사이트를 차단하도록 설정할 수 있습니다. 차단 정책을 적용하면 사용자 PC에서 위험한 웹사이트에 접속하는 것을 예방할 수 있습니다.

또한 지속적으로 위험 요소를 모니터링하여 긴급한 상황이 발생하면 긴급 경보 알림 기능을 통해 신속한 대응을 지원합니다. SiteGuard Security Center는 사용자 PC에 설치된 SiteGuard에서 수집한 정보를 이용해 보고서 작성도 지원합니다. 각종 보안 위험에 대한 보고서는 내부 보안 사고의 취약점을 파악하거나 대응 방안을 마련하는데 활용할 수 있습니다.

제품 구성물

AhnLab SiteGuard Security Center 구입 후 제품 구성물을 확인하여 주시기 바랍니다. 제품 구성물에 이상이 있는 경우, 제품 구입처나 안철수연구소 고객만족센터 기업 고객 핫라인(02-2186-3082)으로 연락하여 주시기 바랍니다.

- ❖ AhnLab SiteGuard 사용권 증서와 제품 번호
- ❖ AhnLab SiteGuard Security Center 사용권 증서와 제품 번호
- ❖ 사용자 안내문

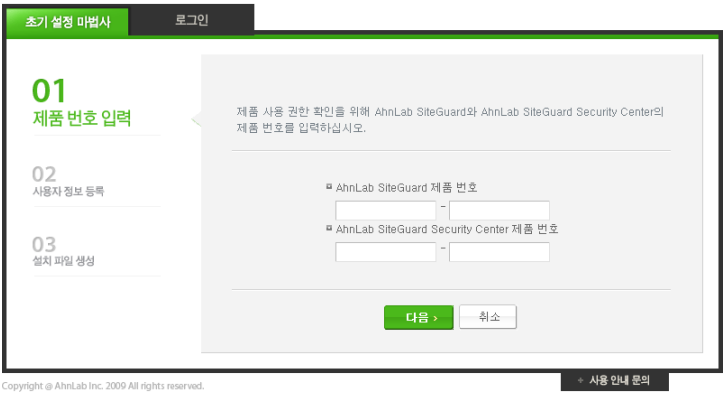
사용자 등록하기

SiteGuard Security Center에 접속하기 위해서는 아이디와 비밀번호가 필요합니다. 처음 접속한 경우에는 **사용자 등록하기**에서 아이디와 비밀번호를 등록해야 합니다. 사용자 등록에 대한 자세한 내용은 로그인 페이지의 아래에 있는 **등록 방법 보기**를 눌러 확인할 수 있습니다.

1 SiteGuard Security Center 홈페이지(http://sc.siteguard.co.kr)에 접속합니다.

2 로그인 화면에서 **사용자 등록하기**를 누릅니다.

3 <초기 설정 마법사>가 나타납니다.



- 제품 번호 입력: 제품 사용 권한 확인을 위해 AhnLab SiteGuard 제품 번호와 AhnLab SiteGuard Security Center 제품 번호를 정확하게 입력합니다.
- 사용자 정보 등록: 입력된 고객 정보(회사 이름, 제품 구매일, 제품 수)를 확인한 후 관리자 등록 화면에 아이디와 비밀번호를 입력합니다. 아이디는 SiteGuard Security Center를 총괄하여 관리할 관리자 아이디를 등록하시기 바랍니다.
- 설치 파일 생성: 사용자 PC에 배포할 SiteGuard 설치 파일을 만듭니다. 설치 과정 모두 보이기와 설치 과정 모두 숨기기 중에서 설치 과정에 대한 방법을 선택한 후 **다음**을 누릅니다. 설치 파일을 만드는 작업은 최대 몇 분이 소요될 수 있습니다. 설치 파일 다운로드 주소가 만들어지면 **마침**을 누릅니다.

- 설치 과정 모두 보이기(권장): 설치 파일을 실행했을 때 설치에 필요한 모든 단계가 화면에 나타납니다.
- 설치 과정 모두 숨기기: 설치 파일을 실행했을 때 사용자 컴퓨터 화면에 표시되는 내용없이 설치를 마칩니다.

참고

설치 파일은 다운로드 주소를 이메일로 전송하거나 공지하여 배포할 수 있습니다.

4 설정한 관리자 아이디와 비밀번호를 로그인 화면에 입력하고 **로그인**을 누릅니다.

그룹 설정

그룹 설정을 하면 조직도와 같은 특정 기준에 따라 그룹을 지정하여 그룹별로 보안 위험 현황을 파악하고 관리할 수 있습니다. SiteGuard 설치 파일을 배포하기 전에 그룹을 지정해 놓으면, 사용자 PC에서 SiteGuard를 설치함과 동시에 자동으로 그룹이 적용되어 편리합니다. 그룹은 CVS 형식의 서식 파일을 등록하거나 자동 그룹핑을 이용해 설정할 수 있습니다.

⚠ 주의

관리자가 그룹 설정을 하기 전에 사용자 PC에서 SiteGuard를 설치하면 해당 PC는 그룹 미등록 PC로 자동 등록됩니다. **그룹 미등록 PC** 화면에서는 삭제만 되고, 그룹 이동이나 그룹 지정을 지원하지 않습니다. 따라서 그룹은 설치 파일 주소를 배포하기 전에 미리 설정해 두는 것이 편리합니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center의 **환경 설정->그룹 설정**을 누릅니다.

3 그룹을 등록할 방법을 선택합니다.

- 그룹 목록 가져오기: CVS 형식으로 구성된 서식 파일에 맞춰 그룹 목록 파일을 등록하면 관리자가 설정한 상태로 그룹을 관리할 수 있습니다.
  - PC 정보 설정: 사용자 PC의 정보를 보여줄 때 기준이 되는 대표 정보를 설정합니다. PC 정보는 모니터링이나 보고서의 표시 기준이 되며 IP 주소, 컴퓨터 이름, MAC 주소 중에서 선택할 수 있습니다.
- 자동 그룹 만들기: IP 주소의 클래스나 네트워크 도메인/워크 그룹 등으로 자동 그룹을 설정합니다.
  - 자동 그룹화 방법: 개별 PC가 서버에 등록될 때의 방법에 따라 자동으로 그룹화합니다.
    - C 클래스 IP 주소: IP 주소의 C 클래스에서 배분한 그룹을 자동으로 등록합니다. 그룹 이름은 3개 단위의 IP 주소와 마지막 번호인 0으로 구성합니다(예: 123.45.678.0). 이 그룹에는 해당 IP의 0에서 254까지 포함한 C 클래스 주소의 모든 PC가 포함됩니다.

- B 클래스 IP 주소: IP 주소의 B 클래스에서 배분한 그룹을 자동으로 등록합니다. 그룹 이름은 2개 단위의 IP 주소와 마지막 번호인 0으로 구성합니다(예: 123.45.0.0). 이 그룹에는 해당 IP의 0에서 254까지 포함한 B 클래스 주소의 모든 PC를 포함합니다.
- NT 도메인/워크 그룹: NT 도메인이나 시스템 등록 정보의 워크 그룹을 자동으로 등록합니다.

▪ 내부 IP 주소 범위: 내부에서 사용하는 IP 주소의 범위를 구분하여 그룹을 설정합니다. 최대 5개의 그룹 범위를 지정할 수 있습니다.

⚠ 주의

내부 IP 주소를 이용해 그룹을 등록할 경우, 해당 IP 주소 외의 모든 PC는 그룹 미등록 PC로 설정됩니다.

4 **저장**을 누릅니다.

계정 관리

SiteGuard Security Center에 로그인할 수 있는 관리자의 계정을 추가, 삭제할 수 있습니다. 관리자 계정은 모든 영역을 관리할 수 있는 계정과 모니터링 업무만 수행할 수 있는 계정으로 구분되어 있습니다. 관리자 계정의 추가나 수정은 모든 권한을 갖는 아이디만 할 수 있습니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center의 **환경 설정->계정 관리**를 누릅니다.

계정 추가하기

새로운 관리자 계정을 만듭니다. 관리자는 모든 권한을 갖는 관리자와 모니터링만 할 수 있는 관리자로 구분합니다. 관리자는 초기 설정 관리자를 포함하여 최대 10개까지 만들 수 있습니다.

1 계정 관리 화면의 오른쪽 아래에 있는 **계정 만들기**를 누릅니다.

2 <관리자 계정 추가>가 나타납니다. 추가할 아이디와 관리권한, 비밀번호를 입력하고 로그인 환경을 설정합니다.

- 아이디: 각 관리자 계정의 고유한 아이디를 입력합니다. 중복된 아이디는 사용할 수 없으며, 등록 후에는 수정할 수 없습니다. 아이디는 초기 설정 관리자 아이디에서 파생된 아이디만을 만들 수 있습니다. 예를 들어, 초기 설정 아이디가 'admin'이라면 이후 관리자 아이디는 'admin.1', 'admin.2'와 같은 형태가 됩니다.
- 관리 권한: 해당 아이디의 관리 권한을 선택합니다. **모든 영역**의 권한을 갖는 관리자는 정책을 적용하거나 그룹을 등록하는 등의 모든 관리를 총괄할 수 있는 권한이 주어집니다. **모니터링** 권한을 갖는 관리자는 모니터링에만 접근할 수 있으며, 모니터링 외에 정책 관리, 환경 설정, 보고서의 내용에는 접근할 수 없습니다.
- 비밀번호: 8자리 이상의 비밀번호를 입력합니다. 비밀번호는 영문자나 숫자만 이용할 수 있습니다.
- 비밀번호 확인: 입력한 비밀번호를 다시 입력하십시오.

- 로그인 환경 설정: SiteGuard Security Center에 로그인할 수 있는 사용자의 IP 주소 범위를 설정합니다. 관리자가 IP 주소 범위를 설정하면 해당 IP 주소 범위 안에 있는 컴퓨터에서만 SiteGuard Security Center에 로그인할 수 있습니다. 기본 설정은 모든 IP 주소에서 로그인할 수 있도록 부여되어 있습니다.

3 **확인**을 누르면 새 계정이 추가된 목록이 나타납니다. **취소**를 누르면 <관리자 계정 목록>으로 이동합니다.

계정 삭제하기

관리자 계정을 삭제합니다. 모든 영역에 관리 권한이 있는 관리자만 계정을 삭제할 수 있습니다. 단, 초기 설정 관리자는 삭제할 수 없습니다.

1 <관리자 계정 목록>에서 삭제할 계정을 선택합니다.

2 **삭제**를 누릅니다.

3 해당 계정이 삭제된 목록이 나타납니다.

긴급 경보 알림

SiteGuard가 설치된 사용자 PC를 실시간으로 모니터링하여 인터넷 변조 등의 보안 위험 현상을 발견하면 관리자에게 문자메시지나 이메일로 긴급 경보를 알려줍니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center의 **환경 설정->긴급 경보 알림**을 누릅니다.

3 긴급 경보 알림 메시지를 전달 받을 방법을 선택합니다. 문자메시지 전송과 이메일 발송을 모두 선택할 수 있습니다.

- 문자메시지로 알리기: 긴급한 보안 위협이 발생하면 저장된 휴대전화로 문자메시지를 전송합니다.
  - 휴대전화: 문자메시지를 전송할 휴대전화 번호를 입력합니다. 공백없이 10~11자리의 숫자를 입력하고, 필요한 경우 '-'도 사용할 수 있습니다. 최대 3개의 번호를 저장할 수 있습니다.
  - 알림 주기: 문자메시지 전송 주기를 선택할 수 있습니다. 시간 간격은 5분, 15분, 30분으로 구분되어 있으며 1~3회의 전송 횟수를 선택할 수 있습니다.
- 이메일로 알리기: 긴급한 보안 위협이 발생하면 저장된 메일 주소로 이메일을 발송합니다.
  - 이메일: 긴급 경보를 받을 사람의 이메일 주소를 입력합니다. admin@example.com과 같은 형태로 입력하십시오. 이메일은 최대 3개까지 저장할 수 있습니다.

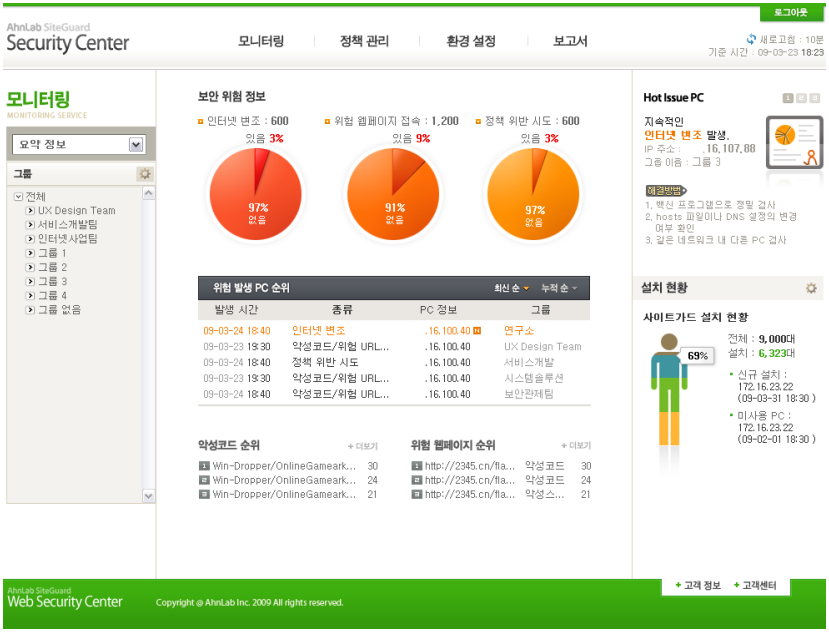
4 **저장**을 누릅니다.

2장
모니터링

요약 정보

2

요약 정보에서는 관리 그룹 및 그룹 내 개별 PC의 보안 상태를 실시간으로 확인할 수 있습니다. 인터넷 변조 현황, 위험 웹페이지 접속 현황, 정책 위반 시도 현황에 대한 그래프 정보를 한 눈에 확인할 수 있으며 발견된 악성코드나 접속한 위험 웹페이지의 순위를 보여줍니다. 사용자 PC 중에서 현재 가장 위험한 상태인 PC 정보는 **Hot Issue PC**에서 확인할 수 있습니다. **설치현황**에서는 SiteGuard가 설치된 현황 정보를 확인할 수 있습니다.



1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center에 처음 접속하면 **모니터링->요약 정보**가 나타납니다. 그룹별 요약 정보를 확인하려면 화면 왼쪽의 **그룹 선택**에서 원하는 그룹 이름을 누릅니다. 특정 그룹의 이름을 누르면 전체 정보에 대한 요약 정보가 해당 그룹의 요약 정보로 변경됩니다.

참고

기본 설정은 내부 PC의 전체 정보를 보는 것입니다. 화면 왼쪽의 **그룹 선택**에서 특정 그룹을 선택하면, 오른쪽 화면이 해당 그룹의 정보로 변경됩니다.

- 보안 위험 정보: 인터넷 변조, 위험 웹페이지 접속, 정책 위반 시도가 일어난 PC의 수치 현황을 보여줍니다.
- 위험 발생 PC 순위: 위험 요소가 가장 많이 발생한 PC의 정보를 보여줍니다. 최신 순이나 누적 순으로 확인할 수 있습니다.
- 악성코드 순위: 가장 많이 발견한 악성코드의 정보를 보여줍니다.
- 위험 웹페이지 순위: 가장 많이 접속한 위험 웹페이지의 정보를 보여줍니다.
- Hot Issue PC: 관리 대상 PC 중에서 현재 가장 위험한 상태인 3대의 PC 정보가 나타납니다. 해당 PC의 IP 주소와 그룹 이름을 보여주고 위험하다고 판단한 이유와 해결 방법도 함께 보여줍니다.
- 설치 현황: SiteGuard가 설치된 현황을 보고서를 작성합니다.

주의

관리자가 그룹 설정을 하기 전에 사용자 PC에서 SiteGuard를 설치하면 해당 PC는 그룹 미등록 PC로 자동 등록됩니다. 그룹 미등록 PC 화면에서는 삭제만 되고, 그룹 이동이나 그룹 지정을 지원하지 않습니다. 따라서 그룹은 설치 파일 주소를 배포하기 전에 미리 설정해 두는 것이 편리합니다.

인터넷 변조 현황

2

사용자 PC에 설치된 SiteGuard에서 인터넷 변조를 탐지하고 차단한 기록을 보여줍니다.

참고

인터넷 변조는 내부 네트워크(LAN)에 있는 PC가 악성코드에 감염되거나 ARP 스푸핑(Spoofing)공격을 받아 인터넷 통신 프로토콜(HTTP)에 악의적인 스크립트가 삽입되는 경우를 말합니다. SiteGuard는 Hosts 파일이나 DNS 서버 주소, Proxy 서버 주소 등에 변조가 발생하는 것을 탐지하고 차단합니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center에 접속하면 **모니터링** 화면의 왼쪽에서 을 눌러 **인터넷 변조 현황**을 선택합니다.

- 인터넷 변조 현황: 그룹 정보를 나타내는 영역과 인터넷 변조의 발생 현황을 보여주는 그래프로 구성되어 있습니다. **그룹**에서는 그룹 이름과 그룹의 설정 방법, 그룹 내 PC 수를 보여주는 그룹 정보가 나타납니다. 그리고 SiteGuard가 설치된 PC 중에서 총 몇 대의 PC에서 인터넷 변조가 발생했는지 보여주는 그래프 및 수치가 나타납니다.
- Hot Issue PC: 관리 대상 PC 중에서 현재 가장 위험한 상태인 3대의 PC 정보가 나타납니다. 해당 PC의 IP 주소와 그룹 이름을 보여주고 위험하다고 판단한 이유와 해결 방법도 함께 보여줍니다.
- 검색: 검색할 기준 정보를 입력한 후 **검색**을 누릅니다.
  - 검색 기간: 기간을 설정하여 해당 기간 내 발생한 인터넷 변조를 확인합니다. 달력 모양을 눌러 날짜를 지정할 수 있으며, **최근 한주**나 **최근 한달**을 누르면 해당 기간의 정보를 볼 수 있습니다.
  - 정렬 기준: 인터넷 변조가 일어난 PC 목록을 정렬하는 기준을 정합니다. 발생한 시간을 기준으로 정렬하려면 **최신 순**을 선택하고, 변조 발생의 횟수를 기준으로 정렬하려면 **누적 순**을 선택합니다. 기본 값은 **최신 순**으로 설정되어 있습니다.
  - 검색 내용: **PC 정보**와 **상세 내용** 중에서 선택하여 검색어를 입력합니다.

- 엑셀로 저장: 인터넷 변조 현황에 대한 검색 결과를 엑셀 파일로 저장합니다. **엑셀로 저장**을 누르면 <파일 다운로드> 창이 나타납니다. **저장**을 선택하면
  <다른 이름으로 저장>이 나타납니다. 이 파일을 저장할 위치를 지정한 후 **저장**을 누릅니다.

참고

기본 설정은 내부 PC의 전체 정보를 보는 것입니다. 화면 왼쪽의 **그룹 선택**에서 특정 그룹을 선택하면, 오른쪽 화면이 해당 그룹의 정보로 변경됩니다.

위험 웹페이지 접속 현황

2

사기 사이트나 피싱 사이트와 같이 위험하다고 알려진 웹페이지에 접속한 정보를 보여줍니다. SiteGuard는 악성코드를 포함한 웹페이지, 악성 ActiveX, 악성 스크립트, 사기 사이트, 피싱 사이트, 웹기반 비정상 프로세스 등을 감지하여 차단합니다. 위험 웹페이지에 접속했던 정보는 그룹별, 기간별로 확인할 수 있습니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center에 접속하면 **모니터링** 화면의 왼쪽에서 을 눌러 **위험 웹페이지 접속 현황**을 선택합니다.

- 위험 웹페이지 접속 현황: 그룹 정보를 나타내는 영역과 위험 웹페이지에 접속한 상태를 보여주는 그래프로 구성되어 있습니다. **그룹**에서는 그룹 이름과 그룹의 설정 방법, 그룹 내 PC 수를 보여주는 그룹 정보가 나타납니다. 그리고 SiteGuard가 설치된 PC 중에서 총 몇 대의 PC에서 위험 웹페이지에 접속했는지 보여주는 그래프 및 수치가 나타납니다.
- Hot Issue PC: 관리 대상 PC 중에서 현재 가장 위험한 상태인 3대의 PC 정보가 나타납니다. 해당 PC의 IP 주소와 그룹 이름을 보여주고 위험하다고 판단한 이유와 해결 방법도 함께 보여줍니다.
- 검색: 검색할 기준 정보를 입력한 후 **검색**을 누릅니다.
  - 검색 기간: 기간을 설정하여 해당 기간 내 위험 웹페이지에 접속한 정보를 확인합니다. 달력 모양을 눌러 날짜를 지정할 수 있으며, **최근 한주**나 **최근 한달**을 누르면 해당 기간의 정보를 볼 수 있습니다.
  - 정렬 기준: 위험 웹페이지에 접속한 PC 목록을 정렬하는 기준을 정합니다. 발생한 시간을 기준으로 정렬하려면 **최신순**을 선택하고, 접속 횟수를 기준으로 정렬하려면 **누적 순**을 선택합니다. 기본 값은 **최신순**으로 설정되어 있습니다.
  - 위험 요소 종류: 위험으로 판단한 기준 요소를 보여줍니다.
    - 악성 파일 다운로드: 악성코드를 포함한 웹페이지에 접속했을 때 악성 파일이 다운로드되는 것을 진단하여 차단합니다.
    - 악성 ActiveX: 악의적인 목적으로 작성된 ActiveX를 진단하여 차단합니다.

- 악성 스크립트: SiteGuard의 자체 휴리스틱 진단 기법으로 해킹에 사용하는 주된 기법과 행위를 감지하여 차단합니다. 백신 프로그램에는 반영되지 않은 새로운 악성코드나 변종 악성코드까지 차단할 수 있습니다.
- 사기 사이트: 서울특별시전자상거래센터에 사기 사이트로 등록된 웹사이트입니다.
- 피싱 사이트: 국제 안티피싱 단체인 Anti-Phishing Working Group에서 제공하는 정보를 기반으로 피싱 사이트라고 알려진 웹사이트입니다.
- 웹기반 비정상 프로세스: 웹브라우저의 취약점을 이용하여 비정상 프로세스가 일어나는 경우를 감시합니다. 백신 프로그램에는 반영되지 않은 새로운 악성코드나 변종 악성코드까지 차단할 수 있습니다.

▪ 검색 내용: **PC 정보**와 **상세 내용** 중에서 선택하여 검색어를 입력합니다.

▪ 엑셀로 저장: 위험 웹페이지 접속 현황에 대한 검색 결과를 엑셀 파일로 저장합니다. **엑셀로 저장**을 누르면 <파일 다운로드>가 나타납니다. **저장**을 선택하면 <다른 이름으로 저장>이 나타납니다. 이 파일을 저장할 위치를 지정한 후 **저장**을 누릅니다.

참고

기본 설정은 내부 PC의 전체 정보를 보는 것입니다. 화면 왼쪽의 **그룹 선택**에서 특정 그룹을 선택하면, 오른쪽 화면이 해당 그룹의 정보로 변경됩니다.

정책 위반 시도 현황

2

정책 위반 시도 현황은 차단 정책이 적용된 웹페이지에 접속을 시도한 PC 정보를 보여줍니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center에 접속하면 **모니터링** 화면의 왼쪽에서 을 눌러 **정책 위반 시도 현황**을 선택합니다.

- 정책 위반 시도 현황: 그룹 정보를 나타내는 영역과 정책 위반을 시도한 PC 정보를 보여주는 그래프로 구성되어 있습니다. **그룹**에서는 그룹 이름과 그룹의 설정 방법, 그룹 내 PC 수를 보여주는 그룹 정보가 나타납니다. 그리고 SiteGuard가 설치된 PC 중에서 총 몇 대의 PC에서 정책 위반을 시도했는지 보여주는 그래프 및 수치가 나타납니다.
- Hot Issue PC: 관리 대상 PC 중에서 현재 가장 위험한 상태인 3대의 PC 정보가 나타납니다. 해당 PC의 IP 주소와 그룹 이름을 보여주고 위험하다고 판단한 이유와 해결 방법도 함께 보여줍니다.
- 검색: 검색할 기준 정보를 입력한 후 **검색**을 누릅니다.
  - 검색 기간: 기간을 설정하여 해당 기간 내 정책 위반을 시도한 정보를 확인합니다. 달력 모양을 눌러 날짜를 지정할 수 있으며, **최근 한주**나 **최근 한달**을 누르면 해당 기간의 정보를 볼 수 있습니다.
  - 정렬 기준: 정책 위반을 시도한 PC 목록을 정렬하는 기준을 정합니다. 발생한 시간을 기준으로 정렬하려면 **최신 순**을 선택하고, 시도 횟수를 기준으로 정렬하려면 **누적 순**을 선택합니다. 기본 값은 **최신 순**으로 설정되어 있습니다.
  - 검색 내용: **PC 정보**와 **상세 내용** 중에서 선택하여 검색어를 입력합니다.
  - 엑셀로 저장: 위험 웹페이지 접속 현황에 대한 검색 결과를 엑셀 파일로 저장합니다. **엑셀로 저장**을 누르면 <파일 다운로드> 창이 나타납니다. **저장**을 선택하면 <다른 이름으로 저장>이 나타납니다. 이 파일을 저장할 위치를 지정한 후 **저장**을 누릅니다.

참고

기본 설정은 내부 PC의 전체 정보를 보는 것입니다. 화면 왼쪽의 **그룹 선택**에서 특정 그룹을 선택하면, 오른쪽 화면이 해당 그룹의 정보로 변경됩니다.

악성코드 및 위험 웹페이지 정보

발견된 악성코드나 위험 웹페이지에 대한 정보를 보여줍니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center에 접속하면 **모니터링** 화면의 왼쪽에서 을 눌러 **악성코드 및 위험 웹페이지 정보**를 선택합니다.

- 그룹: 그룹 이름과 그룹의 설정 방법, 그룹 내 PC 수를 보여주는 그룹 정보가 나타납니다.
- 검색: 검색할 기준 정보를 입력한 후 **검색**을 누릅니다.
  - 검색 기간: 기간을 설정하여 해당 기간 내 발견한 악성코드나 위험 웹페이지의 정보를 확인합니다. 달력 모양을 눌러 날짜를 지정할 수 있으며, **최근 한주**나 **최근 한달**을 누르면 해당 기간의 정보를 볼 수 있습니다.
  - 정렬 기준: 목록을 정렬하는 기준을 정합니다. 발견된 악성코드의 수를 기준으로 정렬하려면 **악성코드 순위**를 선택하고, 위험 웹페이지의 접속 시도 횟수를 기준으로 정렬하려면 **웹페이지 접속 순위**를 선택합니다. 기본 값은 **악성코드 순위**로 설정되어 있습니다.
  - 검색 내용: **악성코드 이름**이나 위험 **웹페이지 주소** 중에서 선택하여 검색어를 입력합니다.
  - 엑셀로 저장: 악성코드 및 위험 웹페이지에 대한 검색 결과를 엑셀 파일로 저장합니다. **엑셀로 저장**을 누르면 <파일 다운로드> 창이 나타납니다. **저장**을 선택하면 <다른 이름으로 저장>이 나타납니다. 이 파일을 저장할 위치를 지정한 후 **저장**을 누릅니다.

참고

기본 설정은 내부 PC의 전체 정보를 보는 것입니다. 화면 왼쪽의 **그룹 선택**에서 특정 그룹을 선택하면, 오른쪽 화면이 해당 그룹의 정보로 변경됩니다.

로그 정보

2

SiteGuard Security Center의 관리자가 실행한 작업 기록을 실시간으로 확인할 수 있습니다. 로그 정보는 시간 순서대로 정렬되어 나타납니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center에 접속하면 **모니터링** 화면의 왼쪽에서 을 눌러 **로그 정보**를 선택합니다.

3 검색 기간을 설정하거나 정렬 기준을 선택하여 **검색**을 누릅니다.

- 검색 기간: 달력 모양을 눌러 날짜를 지정할 수 있으며, **최근 한주**나 **최근 한달**을 누르면 해당 기간의 정보를 볼 수 있습니다.
- 정렬 기준: 등록된 아이디를 기준으로 목록을 정렬합니다.

4 최신 로그부터 정렬된 작업 내용을 확인합니다. 로그 정보가 남는 작업은 다음과 같습니다.

- 적용 시간: 해당 업무가 적용된 시간을 보여줍니다.
- 수준: 로그인과 같은 일반적인 작업과 정책 변경과 같은 주의할 작업을 구분하여 보여줍니다.
- 종류: 다음과 같이 수행한 업무별로 구분하여 보여줍니다..
  - 로그인: SiteGuard Security Center에 로그인한 특정 아이디와 IP 주소를 확인할 수 있습니다.
  - 비밀번호 변경: 비밀번호를 변경한 아이디와 적용 시간을 확인할 수 있습니다.
  - 관리자 설정 변경: 설정을 변경한 아이디의 로그 정보를 확인할 수 있습니다.
  - 정책 변경: 차단 정책의 추가, 삭제 및 정책 예외의 추가, 삭제 내용을 확인할 수 있습니다.
  - 그룹 설정 변경: 그룹 설정을 변경한 아이디와 시간을 확인할 수 있습니다.
  - 설치 파일 변경: 설치 파일을 변경한 아이디와 시간을 확인할 수 있습니다.
  - 보고서 출력: 보고서를 출력한 아이디와 시간을 확인할 수 있으며, 출력한 보고서의 제목을 볼 수 있습니다.

    - 보고서 내보내기: 보고서를 내보내기한 아이디와 시간을 확인할 수 있으며, 보고서의 제목을 볼 수 있습니다.
- 아이디: 해당 업무를 수행한 아이디입니다.
- 상세 내용: 작업 종류별로 상세 내용을 보여줍니다.

3장
정책 관리

웹페이지 차단 관리

보안 정책이나 내부 정책에 따라 내부 네트워크 사용자가 특정한 웹사이트나 웹페이지를 방문하지 못하도록 설정합니다. 차단할 웹페이지의 목록은 해당 웹페이지 주소를 직접 입력하거나 CVS 형식으로 불러올 수 있습니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center의 **정책 관리 -> 웹페이지 차단 관리**를 누릅니다.

3 내부 네트워크에서 접속할 수 없도록 차단할 웹페이지를 등록합니다. **웹페이지 차단 관리**에서는 현재 차단하고 있는 웹페이지의 개수를 확인할 수 있습니다.

- 차단한 웹페이지 목록: 보안 정책이나 내부 정책에 따라 차단한 웹페이지의 목록입니다. 웹페이지 주소와 차단을 적용한 시간이 나타납니다. 특정 웹페이지 주소를 선택한 후 **삭제**를 누르면 해당 웹페이지는 차단 목록에서 삭제됩니다.

⚠ 주의

차단한 웹페이지가 300개를 넘으면 PC의 웹브라우징 속도가 느려질 수 있습니다.

- 차단 목록 추가: 차단할 웹페이지 주소를 직접 입력하여 추가합니다. 웹페이지 주소는 http://나 https://를 포함하여 정확하게 입력하십시오.
  - 특정 웹페이지 차단: 웹페이지 단위로 차단하려면 웹페이지 단위의 주소를 입력합니다. (예: http://www.test.com/test/test.htm)
  - 웹사이트의 전체 host 차단: 특정 웹사이트의 전체 host를 차단하려면 http://*.test.com과 같은 형태로 입력합니다.
  - 해당 웹사이트 전체 차단: 특정 웹사이트의 전체 웹페이지를 차단하려면 http://www.test.com/*과 같은 형태로 입력합니다.
- 차단 목록 가져오기: CVS 형식으로 구성된 서식 파일에 웹페이지를 작성하여 일괄 적용합니다. 차단 정책을 적용할 웹페이지가 많거나 기존의 차단 목록을 등록할 때 편리하게 이용할 수 있습니다.

4 **적용**을 누릅니다.

정책 예외 관리

웹페이지 차단 정책을 사용하고 있는 경우에 해당 정책의 적용을 받지 않고, 모든 웹페이지에 연결이 허용된 PC를 등록합니다. 정책 예외로 등록된 PC에서는 웹페이지 차단 정책의 적용을 받지 않습니다.

정책 예외 PC 추가하기

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center의 **정책 관리 -> 정책 예외 관리**를 누릅니다.

3 <정책 예외 PC 목록>이 나타납니다.

- 설정 시간: 정책 예외를 적용한 시간입니다.
- 그룹: 해당 PC가 속해있는 그룹 정보입니다.
- 컴퓨터 이름: 사용자 PC에 부여된 이름입니다.
- MAC 주소: 해당 PC의 MAC 주소입니다.

참고

MAC 주소는 Media Access Control Address의 약어로 네트워크 카드의 물리적인 주소를 말합니다. MAC 주소의 크기는 48비트이며, 제조 회사에서는 모든 네트워크 카드에 각기 고유한 주소를 부여합니다.

- IP 주소: 해당 PC의 IP 주소를 보여줍니다.

참고

IP 주소는 인터넷에 연결된 통신망을 이용할 때 모든 컴퓨터에 부여되는 고유의 식별 번호입니다.

4 **정책 예외 PC 추가**를 누릅니다. <정책 예외 PC 추가> 화면에서 추가할 PC를 선택합니다.

- 그룹 내 전체 PC: 해당 그룹에 속하는 모든 PC는 웹페이지 차단 정책의 적용을 받지 않습니다. 왼쪽 화면에서 그룹을 선택합니다.
- 특정 PC: 정책 예외를 적용할 PC를 지정합니다. 컴퓨터 이름, MAC 주소, IP 주소 중에서 정책 예외를 적용할 PC를 검색할 수 있습니다. 검색한 PC가 아래 목록에 나타나면 선택합니다.

- 컴퓨터 이름: PC에 부여되어 있는 고유한 이름을 입력합니다.
- MAC 주소: 네트워크 카드의 물리적인 주소를 입력합니다.
- IP 주소: 해당 PC의 IP 주소를 입력합니다.

5 **추가**를 누르면 <정책 예외 PC 목록>에 등록됩니다.

⚠ 주의

추가를 누르지 않은 상태에서 **정책 예외 PC 목록**을 누르면 저장하지 않고 바로 <정책 예외 PC 목록>으로 이동하므로 주의하시기 바랍니다.

정책 예외 PC 삭제하기

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center의 **정책 관리 -> 정책 예외 관리**를 누릅니다.

3 <정책 예외 PC 목록>이 나타납니다. 목록에서 삭제할 PC를 선택한 후, **삭제**를 누릅니다.

4장
환경 설정

그룹 설정

그룹 설정을 하면 조직도와 같은 특정 기준에 따라 그룹을 지정하여 그룹별로 보안 위험 현황을 파악하고 관리할 수 있습니다. SiteGuard 설치 파일을 배포하기 전에 그룹을 지정해 놓으면, 사용자 PC에서 SiteGuard를 설치함과 동시에 자동으로 그룹이 적용되어 편리합니다. 그룹은 CVS 형식의 서식 파일을 등록하거나 자동 그룹핑을 이용해 설정할 수 있습니다.

⚠ 주의

관리자가 그룹 설정을 하기 전에 사용자 PC에서 SiteGuard를 설치하면 해당 PC는 그룹 미등록 PC로 자동 등록됩니다. **그룹 미등록 PC**화면에서는 삭제만 되고, 그룹 이동이나 그룹 지정을 지원하지 않습니다. 따라서 그룹은 설치 파일 주소를 배포하기 전에 미리 설정해 두는 것이 편리합니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center의 **환경 설정->그룹 설정**을 누릅니다.

3 그룹을 등록할 방법을 선택합니다.

- 그룹 목록 가져오기: CVS 형식으로 구성된 서식 파일에 맞춰 그룹 목록 파일을 등록하면 관리자가 설정한 상태로 그룹을 관리할 수 있습니다.
  - PC 정보 설정: 사용자 PC의 정보를 보여줄 때 기준이 되는 대표 정보를 설정합니다. PC 정보는 모니터링이나 보고서의 표시 기준이 되며 IP 주소, 컴퓨터 이름, MAC 주소 중에서 선택할 수 있습니다.
- 자동 그룹 만들기: IP 주소의 클래스나 네트워크 도메인/워크 그룹 등으로 자동 그룹을 설정합니다.
  - 자동 그룹화 방법: 개별 PC가 서버에 등록될 때의 방법에 따라 자동으로 그룹화합니다.
    - C 클래스 IP 주소: IP 주소의 C 클래스에서 배분한 그룹을 자동으로 등록합니다. 그룹 이름은 3개 단위의 IP 주소와 마지막 번호인 0으로 구성합니다(예: 123.45.678.0). 이 그룹에는 해당 IP의 0에서 254까지 포함한 C 클래스 주소의 모든 PC가 포함됩니다.

- B 클래스 IP 주소: IP 주소의 B 클래스에서 배분한 그룹을 자동으로 등록합니다. 그룹 이름은 2개 단위의 IP 주소와 마지막 번호인 0으로 구성합니다(예: 123.45.0.0). 이 그룹에는 해당 IP의 0에서 254까지 포함한 B 클래스 주소의 모든 PC를 포함합니다.
- NT 도메인/워크 그룹: NT 도메인이나 시스템 등록 정보의 워크 그룹을 자동으로 등록합니다.

▪ 내부 IP 주소 범위: 내부에서 사용하는 IP 주소의 범위를 구분하여 그룹을 설정합니다. 최대 5개의 그룹 범위를 지정할 수 있습니다.

⚠ 주의

내부 IP 주소를 이용해 그룹을 등록할 경우, 해당 IP 주소 외의 모든 PC는 그룹 미등록 PC로 설정됩니다.

4 **저장**을 누릅니다.

그룹 미등록 PC

특정 그룹에 속하지 않은 PC 정보를 보여줍니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center의 **환경 설정->그룹 미등록 PC**를 누릅니다.

3 특정 그룹에 속하지 않은 PC의 목록이 나타납니다.

- 설치 시간: 해당 PC에서 설치 파일의 다운로드 주소로 접속하여 SiteGuard를 설치한 시간입니다.
- 컴퓨터 이름: 사용자 PC에 부여된 이름입니다.
- MAC 주소: 해당 PC의 MAC 주소입니다.

참고

MAC 주소는 Media Access Control Address의 약어로 네트워크 카드의 물리적인 주소를 말합니다. MAC 주소의 크기는 48비트이며, 제조 회사에서는 모든 네트워크 카드에 각기 고유한 주소를 부여합니다.

- 내부 IP 주소: 인터넷에 연결된 내부 통신망을 이용하는 컴퓨터에 부여된 고유의 식별 번호입니다.
- 외부 IP 주소: 인터넷에 연결된 외부 통신망을 이용하는 컴퓨터에 부여된 고유의 식별 번호입니다.
- 사용 차단: 해당 PC의 사용 여부를 나타냅니다.

4 목록에서 PC를 선택한 후, **사용 차단**을 누르면 해당 PC의 보안 현황을 수집하지 않으며 설치 목록에서도 제외됩니다.

긴급 경보 알림

SiteGuard가 설치된 사용자 PC를 실시간으로 모니터링하여 인터넷 변조 등의 보안 위험 현상을 발견하면 관리자에게 문자메시지나 이메일로 긴급 경보를 알려줍니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center의 **환경 설정->긴급 경보 알림**을 누릅니다.

3 긴급 경보 알림 메시지를 전달 받을 방법을 선택합니다. 문자메시지 전송과 이메일 발송을 모두 선택할 수 있습니다.

- 문자메시지로 알리기: 긴급한 보안 위협이 발생하면 저장된 휴대전화로 문자메시지를 전송합니다.
  - 휴대전화: 문자메시지를 전송할 휴대전화 번호를 입력합니다. 공백없이 10~11자리의 숫자를 입력하고, 필요한 경우 '-'도 사용할 수 있습니다. 최대 3개의 번호를 저장할 수 있습니다.
  - 알림 주기: 문자메시지 전송 주기를 선택할 수 있습니다. 시간 간격은 5분, 15분, 30분으로 구분되어 있으며 1~3회의 전송 횟수를 선택할 수 있습니다.
- 이메일로 알리기: 긴급한 보안 위협이 발생하면 저장된 메일 주소로 이메일을 발송합니다.
  - 이메일: 긴급 경보를 받을 사람의 이메일 주소를 입력합니다. admin@example.com과 같은 형태로 입력하십시오. 이메일은 최대 3개까지 저장할 수 있습니다.

4 **저장**을 누릅니다.

설치 파일 설정

설치 파일 설정에서는 가장 최근에 만들어진 설치 파일의 다운로드 주소를 보여줍니다. 설치 파일은 다운로드 주소를 이메일로 전송하거나 공지하여 배포할 수 있습니다. 설치 파일의 다운로드 주소는 필요에 따라 다시 만들 수 있습니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center의 **환경 설정->설치 파일 설정**을 누릅니다.

설치 파일 다시 만들기

새로운 설치 파일을 다시 만드는 과정입니다. <초기 설정 마법사>에서 진행한 과정과 동일합니다.

1 <설치 파일 설정> 화면 하단의 **다시 만들기**를 누릅니다.

2 <설치 파일 생성>이 나타나면 설치 파일을 만드는 과정을 선택합니다.

- 설치 과정 모두 보이기(권장): 설치 파일을 실행했을 때 설치에 필요한 모든 단계가 화면에 나타납니다.
- 설치 과정 모두 숨기기: 설치 파일을 실행했을 때 사용자 컴퓨터의 화면에 표시되는 내용없이 설치를 마칩니다.

3 **다시 만들기**를 누릅니다. 설치 파일을 만드는 작업은 최대 몇 분이 소요될 수 있습니다.

4 새로 만들어진 설치 파일 다운로드 주소가 나타납니다.

참고

설치 파일은 다운로드 주소를 이메일로 전송하거나 공지하는 방법으로 배포할 수 있습니다.

주의

설치 파일을 새로 만들면 이전에 사용하던 설치 파일 다운로드 주소는 더이상 사용할 수 없습니다.

계정 관리

SiteGuard Security Center에 로그인할 수 있는 관리자의 계정을 추가, 삭제할 수 있습니다. 관리자 계정은 모든 영역을 관리할 수 있는 계정과 모니터링 업무만 수행할 수 있는 계정으로 구분되어 있습니다. 관리자 계정의 추가나 수정은 모든 권한을 갖는 아이디만 할 수 있습니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center의 **환경 설정->계정 관리**를 누릅니다.

계정 추가하기

새로운 관리자 계정을 만듭니다. 관리자는 모든 권한을 갖는 관리자와 모니터링만 할 수 있는 관리자로 구분합니다. 관리자는 초기 설정 관리자를 포함하여 최대 10개까지 만들 수 있습니다.

1 계정 관리 화면의 오른쪽 아래에 있는 **계정 만들기**를 누릅니다.

2 <관리자 계정 추가>가 나타납니다. 추가할 아이디와 관리권한, 비밀번호를 입력하고 로그인 환경을 설정합니다.

- 아이디: 각 관리자 계정의 고유한 아이디를 입력합니다. 중복된 아이디는 사용할 수 없으며, 등록 후에는 수정할 수 없습니다. 아이디는 초기 설정 관리자 아이디에서 파생된 아이디만을 만들 수 있습니다. 예를 들어, 초기 설정 아이디가 'admin'이라면 이후 관리자 아이디는 'admin.1', 'admin.2'와 같은 형태가 됩니다.
- 관리 권한: 해당 아이디의 관리 권한을 선택합니다. **모든 영역**의 권한을 갖는 관리자는 정책을 적용하거나 그룹을 등록하는 등의 모든 관리를 총괄할 수 있는 권한이 주어집니다. **모니터링** 권한을 갖는 관리자는 모니터링에만 접근할 수 있으며, 모니터링 외에 정책 관리, 환경 설정, 보고서의 내용에는 접근할 수 없습니다.
- 비밀번호: 8자리 이상의 비밀번호를 입력합니다. 비밀번호는 영문자나 숫자만 이용할 수 있습니다.
- 비밀번호 확인: 입력한 비밀번호를 다시 입력하십시오.

- 로그인 환경 설정: SiteGuard Security Center에 로그인할 수 있는 사용자의 IP 주소 범위를 설정합니다. 관리자가 IP 주소 범위를 설정하면 해당 IP 주소 범위 안에 있는 컴퓨터에서만 SiteGuard Security Center에 로그인할 수 있습니다. 기본 설정은 모든 IP 주소에서 로그인할 수 있도록 부여되어 있습니다.

3 **확인**을 누르면 새 계정이 추가된 목록이 나타납니다. **취소**를 누르면 <관리자 계정 목록>으로 이동합니다.

계정 삭제하기

관리자 계정을 삭제합니다. 모든 영역에 관리 권한이 있는 관리자만 계정을 삭제할 수 있습니다. 단, 초기 설정 관리자는 삭제할 수 없습니다.

1 <관리자 계정 목록>에서 삭제할 계정을 선택합니다.

2 **삭제**를 누릅니다.

3 해당 계정이 삭제된 목록이 나타납니다.

5장
보고서

요약 정보

SiteGuard Security Center 데이터베이스에 등록되어 있는 각종 기록 정보를 이용해 현황별로 보고서를 작성합니다. 요약 정보에서는 제품의 설치 현황, 인터넷 변조 현황, 위험 웹페이지 접속 현황, 정책 적용 현황 등의 정보를 간략하게 보여줍니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center의 **보고서**를 누르면 **요약정보**가 나타납니다.

3 요약 보고서를 작성할 그룹, 기간, 항목을 선택합니다.

- 그룹 선택: 그룹 관계도에서 보고서를 작성할 그룹을 선택합니다. **그룹 미등록 PC 포함**을 누르면 그룹을 지정하지 않은 PC 정보도 보고서에 포함됩니다.
- 기간 선택: 보고서를 작성할 기간을 선택합니다. 일간, 주간, 월간, 사용자 기간 중에서 설정할 수 있습니다.
- 항목 선택: 제품 설치 현황, 인터넷 변조 현황, 위험 웹페이지 현황, 악성코드 현황, 정책 위반 PC 현황 중에서 보고서를 작성할 항목을 선택합니다.

4 작성된 보고서를 확인할 방법을 선택합니다.

- 엑셀로 보기: 보고서를 엑셀 파일로 열거나 저장합니다.
- 인쇄: 만들어진 보고서를 인쇄합니다.
- 보고서 보기: 선택한 그룹, 기간, 항목에 따라 작성된 보고서를 보여줍니다. **보고서 보기**를 누르면 화면 하단에 선택한 항목에 따라 요약 정보가 나타납니다.
  - 보고서 제목: 기본으로 설정된 보고서의 제목이 나타납니다. **제목 수정**을 누르면 보고서의 제목을 새로 입력할 수 있습니다.
  - 그룹: 보고서를 작성할 그룹의 이름입니다.
  - 기간: **기간 선택**에서 설정한 보고서 작성 기간입니다.
  - 제품 설치 현황: SiteGuard가 설치된 현황이 나타납니다. 보유한 제품 수량 중에서 개별 PC에 설치된 개수를 보여주며, 보고서 기간을 선택한 경우 해당 기간 내 설치된 개수도 함께 보여줍니다.

- 인터넷 변조 현황: 해당 기간 동안 인터넷 변조가 발생한 PC 정보와 변조 종류, 발생 비율을 보여줍니다. 또한 인터넷 변조가 가장 많이 발생한 1~5위까지의 PC 정보를 보여줍니다.
- 위험 웹페이지 접속 현황: 해당 기간 동안 위험 웹페이지에 접속한 PC의 수와 접속 비율이 나타납니다. 또한 위험 웹페이지에 가장 많이 접속한 1~5위까지의 PC 정보를 보여줍니다.
- 악성코드 현황: **악성코드 순위**에서는 해당 기간 동안 가장 많이 발견된 악성코드와 웹페이지 주소, 감염 수에 대한 정보를 1~5위까지 보여줍니다. **위험 웹페이지 순위**에서는 가장 많이 접속한 1~5위까지의 위험 웹페이지 주소와 종류, 개수를 보여줍니다.
- 정책 위반 PC 현황: 해당 기간 동안 정책 위반을 시도한 PC 정보를 보여줍니다. **정책 위반 순위**에서는 가장 많이 위반을 시도한 PC 정보가 1~5위까지 나타납니다.

제품 설치 현황

SiteGuard가 설치된 현황에 대한 보고서를 작성합니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center의 **보고서->제품 설치 현황**을 누릅니다.

3 보고서를 작성할 그룹, 기간, 항목을 선택합니다.

- 그룹 선택: 그룹 관계도에서 보고서를 작성할 그룹을 선택합니다. **그룹 미등록 PC 포함**을 누르면 그룹을 지정하지 않은 PC 정보도 보고서에 포함됩니다.
- 기간 선택: 보고서를 작성할 기간을 선택합니다. 일간, 주간, 월간, 사용자 기간 중에서 설정할 수 있습니다.
- 항목 선택: 제품 설치 현황, 설치 PC 목록, 삭제 PC 목록, 미사용 PC 목록 중에서 보고서를 작성할 항목을 선택합니다. 미사용 PC 목록은 SiteGuard 설치 후 일정 기간 사용하지 않은 PC 정보를 보여줍니다. 미사용 기준일의 기본값은 30일입니다.

4 작성된 보고서를 확인할 방법을 선택합니다.

- 엑셀로 보기: 보고서를 엑셀 파일로 열거나 저장합니다.
- 인쇄: 만들어진 보고서를 인쇄합니다.
- 보고서 보기: 선택한 그룹, 기간, 항목에 따라 작성된 보고서를 보여줍니다. **보고서 보기**를 누르면 화면 하단에 선택한 항목에 따라 요약 정보가 나타납니다.
  - 보고서 제목: 기본으로 설정된 보고서의 제목이 나타납니다. **제목 수정**을 누르면 보고서의 제목을 새로 입력할 수 있습니다.
  - 그룹: 보고서를 작성할 그룹의 이름입니다. 전체를 선택한 경우에는 그룹 미등록 PC의 정보도 포함됩니다.
  - 기간: **기간 선택**에서 설정한 보고서 작성 기간입니다.
  - 제품 설치 현황: SiteGuard가 설치된 현황이 나타납니다. 보유한 제품 수량 중에서 개별 PC에 설치된 개수를 보여주며, 보고서 기간을 선택한 경우 해당 기간 내 설치된 개수도 함께 보여줍니다.

- 설치 PC 목록: 최근에 SiteGuard가 설치된 PC 목록입니다. SiteGuard를 설치한 시간, IP 주소, MAC 주소, 컴퓨터 이름, 그룹 이름이 나타납니다.
- 삭제 PC 목록: 최근에 SiteGuard를 삭제한 PC 목록입니다. SiteGuard를 삭제한 시간, IP 주소, MAC 주소, 컴퓨터 이름, 그룹 이름이 나타납니다.
- 미사용 PC 목록: 기준일 이상 SiteGuard를 사용하지 않은 PC 정보입니다. SiteGuard를 마지막으로 사용한 시간과 설치 시간, IP 주소, MAC 주소, 컴퓨터 이름, 그룹 이름이 나타납니다.

인터넷 변조 현황

인터넷 변조의 발생 현황을 보고서로 작성합니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center의 **보고서->인터넷 변조 현황**을 누릅니다.

3 보고서를 작성할 그룹, 기간, 항목을 선택합니다.

- 그룹 선택: 그룹 관계도에서 보고서를 작성할 그룹을 선택합니다. **그룹 미등록 PC 포함**을 누르면 그룹을 지정하지 않은 PC 정보도 보고서에 포함됩니다.
- 기간 선택: 보고서를 작성할 기간을 선택합니다. 일간, 주간, 월간, 사용자 기간 중에서 설정할 수 있습니다.
- 항목 선택: IP 주소, MAC 주소, 컴퓨터 이름을 선택하고 중복 행을 삭제할 것인지 정합니다.

4 작성된 보고서를 확인할 방법을 선택합니다.

- 엑셀로 보기: 보고서를 엑셀 파일로 열거나 저장합니다.
- 인쇄: 만들어진 보고서를 인쇄합니다.
- 보고서 보기: 선택한 그룹, 기간, 항목에 따라 작성된 보고서를 보여줍니다. **보고서 보기**를 누르면 화면 하단에 선택한 항목에 따라 요약 정보가 나타납니다.
  - 보고서 제목: 기본으로 설정된 보고서의 제목이 나타납니다. **제목 수정**을 누르면 보고서의 제목을 새로 입력할 수 있습니다.
  - 그룹: 보고서를 작성할 그룹의 이름입니다. 전체를 선택한 경우에는 그룹 미등록 PC의 정보도 포함됩니다.
  - 기간: **기간 선택**에서 설정한 보고서 작성 기간입니다.

위험 웹페이지 접속 현황

위험 웹페이지에 접속한 현황을 보고서로 작성합니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center의 **보고서->위험 웹페이지 접속 현황**을 누릅니다.

3 보고서를 작성할 그룹, 기간, 항목을 선택합니다.

- 그룹 선택: 그룹 관계도에서 보고서를 작성할 그룹을 선택합니다. **그룹 미등록 PC 포함**을 누르면 그룹을 지정하지 않은 PC 정보도 보고서에 포함됩니다.
- 기간 선택: 보고서를 작성할 기간을 선택합니다. 일간, 주간, 월간, 사용자 기간 중에서 설정할 수 있습니다.
- 항목 선택: 악성파일 다운로드, 악성 ActiveX, 악성 스크립트, 웹기반 비정상 프로세스, 사기 사이트, 피싱 사이트 중에서 보고서를 작성할 항목을 선택합니다. 선택한 항목은 최신 순이나 누적 순으로 정렬할 수 있습니다. 보고서에 표시할 PC 정보를 선택합니다. IP 주소, MAC 주소, 컴퓨터 이름 중에서 해당 PC를 대표하는 정보를 선택합니다.
  - 악성 파일 다운로드: 악성코드를 포함한 웹페이지에 접속하여 악성 파일이 다운로드 되는 것을 진단하여 차단합니다.
  - 악성 ActiveX: 악의적인 목적으로 작성된 ActiveX를 진단하여 차단합니다.
  - 악성 스크립트: SiteGuard의 자체 휴리스틱 진단 기법으로 해킹에 사용하는 주된 기법과 행위를 감지하여 차단합니다. 백신 프로그램에는 반영되지 않은 새로운 악성코드나 변종 악성코드까지 차단할 수 있습니다.
  - 웹기반 비정상 프로세스: 웹브라우저의 취약점을 이용하여 비정상 프로세스가 일어나는 경우를 감시합니다. 백신 프로그램에는 반영되지 않은 새로운 악성코드나 변종 악성코드까지 차단할 수 있습니다.
  - 사기 사이트: 서울특별시전자상거래센터에 사기 사이트로 등록된 웹사이트입니다.
  - 피싱 사이트: 국제 안티피싱 단체인 Anti-Phishing Working Group에서 제공하는 정보를 기반으로 피싱 사이트라고 알려진 웹사이트입니다.

4 작성된 보고서를 확인할 방법을 선택합니다.

- 엑셀로 보기: 보고서를 엑셀 파일로 열거나 저장합니다.
- 인쇄: 만들어진 보고서를 인쇄합니다.
- 보고서 보기: 선택한 그룹, 기간, 항목에 따라 작성된 보고서를 보여줍니다. **보고서 보기**를 누르면 화면 하단에 선택한 항목에 따라 요약 정보가 나타납니다.
  - 보고서 제목: 기본으로 설정된 보고서의 제목이 나타납니다. **제목 수정**을 누르면 보고서의 제목을 새로 입력할 수 있습니다.
  - 그룹: 보고서를 작성할 그룹의 이름입니다. 전체를 선택한 경우에는 그룹 미등록 PC의 정보도 포함됩니다.
  - 기간: **기간 선택**에서 설정한 보고서 작성 기간입니다.

정책 적용 현황

정책 위반을 시도한 현황에 대한 분석 보고서를 작성합니다.

1 http://sc.siteguard.co.kr에 접속하여 로그인합니다.

2 SiteGuard Security Center의 **보고서->정책 적용 현황**을 누릅니다.

3 보고서를 작성할 그룹, 기간, 항목을 선택합니다.

- 그룹 선택: 그룹 관계도에서 보고서를 작성할 그룹을 선택합니다. **그룹 미등록 PC 포함**을 누르면 그룹을 지정하지 않은 PC 정보도 보고서에 포함됩니다.
- 기간 선택: 보고서를 작성할 기간을 선택합니다. 일간, 주간, 월간, 사용자 기간 중에서 설정할 수 있습니다.
- 항목 선택: 정책 위반 종류, 정책 위반 PC 중에서 보고서 정렬 기준을 선택합니다. 보고서에 표시할 PC 정보를 선택합니다. IP 주소, MAC 주소, 컴퓨터 이름 중에서 해당 PC를 대표하는 정보를 선택합니다.

4 작성된 보고서를 확인할 방법을 선택합니다.

- 엑셀로 보기: 보고서를 엑셀 파일로 열거나 저장합니다.
- 인쇄: 만들어진 보고서를 인쇄합니다.
- 보고서 보기: 선택한 그룹, 기간, 항목에 따라 작성된 보고서를 보여줍니다. **보고서 보기**를 누르면 화면 하단에 선택한 항목에 따라 요약 정보가 나타납니다.
  - 보고서 제목: 기본으로 설정된 보고서의 제목이 나타납니다. **제목 수정**을 누르면 보고서의 제목을 새로 입력할 수 있습니다.
  - 그룹: 보고서를 작성할 그룹의 이름입니다. 전체를 선택한 경우에는 그룹 미등록 PC의 정보도 포함됩니다.
  - 기간: **기간 선택**에서 설정한 보고서 작성 기간입니다.

색인

ㅈ

ㅊ

ㅋ

ㅍ

ㅎ

B

C

H

M

N

P