SANGFOR | SANGFOR SECURITY

SANGFOR
Cyber Command

지능형 위협 탐지 & 대응 플랫폼

www.sangfor.com

NDR(네트워크 탐지 및 대응)은 새로운 사이버 위협에 맞서 싸우는 데 필수적인 도구입니다

끊임없이 진화하는 사이버 보안 위협 환경은 특히 고도로 정교하고 AI를 지원하는 악성 코드와 사이버 공격이 지속적으로 증가하고 있기 때문에 전 세계 조직의 우려를 불러일으키고 있습니다. 이러한 지능형 위협은 감지되지 않은 채 기존 방어 수단을 우회하고, 민감한 데이터를 훔치고, 중요한 인프라에 심각한 피해를 입히도록 설계되었습니다. 결과적으로, 조직은 이러한 진화하는 위협에 맞서기 위해 기계 학습 및 인공 지능과 같은 고급 기술을 통합하는 새롭고 더욱 강력한 보안 솔루션을 채택하는 것이 필수적입니다.

그러한 보안 기술 중 하나가 네트워크 탐지 및 대응(NDR)입니다. 이는 위협이 네트워크를 막으려는 대신 이미 네트워크에 침입했다고 가정하여 위협 탐지 및 위협 사냥에 대한 사전 예방적 접근 방식을 취합니다. NDR 솔루션은 고급 AI 알고리즘과 기계 학습을 사용하여 네트워크 전반의 트래픽을 실시간으로 모니터링 및 분석하고 네트워크 활동의 이상 현상을 식별하고 보안 팀에 알립니다. 이러한 이상 현상은 지능형 악성 코드나 정교한 공격 기술에 의해 조작되거나 위장된 무해한 네트워크 트래픽으로 나타날 수 있습니다. NDR은 네트워크 트래픽에 대한 향상된 가시성을 제공함으로써 오늘날의 AI 기반 고급 맬웨어 및 사이버 공격을 방어하기 위한 조직의 보안 무기고에 필수적인 도구입니다.

보안팀이 어려움을 겪는 이유
• 빠르게 진화하는 위협 환경을 따라잡기가 어렵습니다
• 지능형 위협을 탐지하고 예방할 리소스 부족
• 전반적인 보안 상태와 사이버 공격 라이프사이클에 대한 가시성 부족
• 통합되지 않은 여러 보안 도구의 복잡한 관리
• 수많은 경고 및 오탐으로 인한 경고 피로 및 비효율성
• 불충분한 포렌식 조사, IOC 및 BIOC 부족

Sangfor Cyber Command로 정교한 위협에 앞서 나가세요

AI 기반 지능형 위협 탐지 및 대응 플랫폼

Sangfor Cyber Command는 숨겨진 위협, 진행 중인 공격, 섀도우 IT를 포함한 자산, 취약점 및 위험을 포함하여 조직에 네트워크 환경에 대한 전례 없는 가시성을 제공하는 동급 최고의 네트워크 탐지 및 대응(NDR) 솔루션입니다.

인공 지능과 기계 학습 기술의 힘을 활용하는 Cyber Command는 고급 보안 분석 및 실시간 위협 인텔리전스를 갖춘 정교한 보안 사고를 탐지하고 대응하기 위한 포괄적인 솔루션을 제공합니다. 이를 통해 기업은 잠재적인 공격이 비용이 많이 드는 침해로 확대되기 전에 이에 대해 단호한 조치를 취할 수 있습니다.

실시간 모니터링, 분석 및 경고 기능을 통해 Cyber Command는 네트워크 트래픽의 이상 현상이 발생하는 즉시 이를 감지하여 조직이 사후 조치에 의존하는 대신 사이버 보안에 대해 사전 대응할 수 있도록 지원합니다.

Sangfor Cyber Command를 통해 조직은 수동적인 방관자에서 사이버 위협에 맞서 싸우는 적극적인 참여자로 변모할 수 있습니다. 이 고급 보안 솔루션을 갖추고 있으면 현재는 물론 미래에도 점점 더 정교해지는 사이버 위협에 효과적으로 대비할 수 있습니다.

비교할 수 없는 위협 탐지

Cyber Command는 AI 및 ML 기반 UEBA(사용자 및 개체 행동 분석)와 규칙 기반 분석을 포함한 다양한 위협 탐지 기술을 활용하여 랜섬웨어, APT, 제로 데이 공격, 파일리스 공격과 같은 지능형 위협에 대한 탁월한 탐지 기능을 제공합니다. 또한 Cyber Command는 최신 위협과 새로운 위협을 탐지할 수 있도록 Sangfor Neural-X의 실시간 위협 인텔리전스 피드를 지속적으로 강화하고 있습니다.

전례 없는 네트워크 가시성

Cyber Command는 네트워크 전체의 트래픽을 지속적으로 모니터링하고 고급 기술을 사용하여 보안 팀에 네트워크 환경에 대한 탁월한 가시성을 제공합니다. 이는 숨겨진 위협을 찾아낼 뿐만 아니라 네트워크 자산에 대한 실시간 통찰력을 제공하여 위험한 섀도우 IT와 패치되지 않은 소프트웨어, 취약한 비밀번호, 암호화 누락과 같은 취약점을 노출시켜 즉각적인 치료를 가능하게 합니다. 또한 Sophos, Symantec, PaloAlto, Kaspersky 등과 같은 유명 공급업체의 다양한 방화벽 및 엔드포인트에서 데이터를 쉽게 수집할 수 있도록 타사 도구와의 통합 기능을 확장했습니다. 이렇게 확장된 용량은 운영 가시성을 향상시켜 네트워크 내의 잠재적인 위협에 대한 보다 전체적인 이해를 제공하고 이를 효과적으로 탐지하고 대응할 수 있는 도구를 제공합니다.

심층적인 위협 탐지 및 조사

Cyber Command는 공격 체인 시각화, MITRE ATT&CK 매핑 프레임워크, 고유한 Golden Eye 기능과 같은 고급 기술을 활용하여 보안 사고에 대한 자세한 통찰력을 제공합니다. 보안팀은 공격의 진입점, 공격 경로, 영향 범위를 직관적으로 발견하여 환경에서 위협을 완전히 근절하고 공격자가 악용하는 취약점과 약점을 교정할 수 있습니다.

자동화되고 통합된 사고 대응

Cyber Command에는 식별된 보안 위협에 자동으로 대응할 수 있는 SOAR(보안 오케스트레이션, 자동화 및 대응) 모듈이 내장되어 있습니다. 보안 팀은 사전 정의된 플레이북이나 맞춤형 플레이북을 사용하여 일반적인 위협 시나리오 또는 조직별 시나리오를 해결할 수 있습니다. Cyber Command는 또한 Sangfor 및 타사 보안 도구와 원활하게 통합되어 조정된 대응 조치를 시작합니다.

> **Cyber Command는 포괄적인 위협 탐지 및 자동화된 대응 기능을 제공하면서도 관리 및 운영이 간단하고 직관적입니다.**

» Cyber Command을 보안 생태계에 원활하게 통합하세요

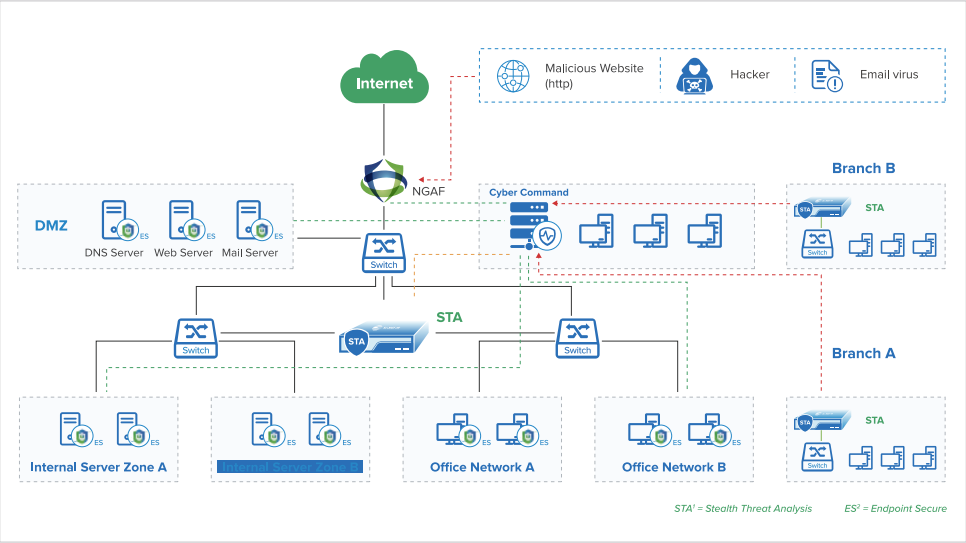
오랫동안 조직에서는 여러 보안 도구가 서로 겹쳐져 있는 복잡한 보안 스택을 구축해 왔습니다. 이러한 접근 방식으로 인해 보안 허점으로 이어지는 통합 불량, 기능 중복, 복잡한 관리 등 다양한 문제가 발생했습니다.

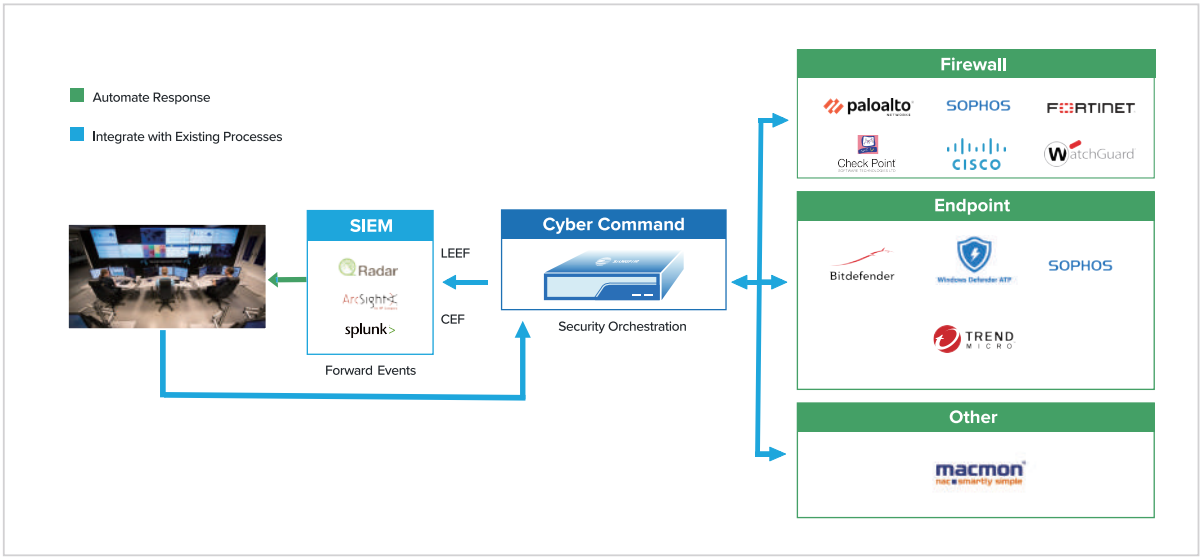
따라서 조직은 사이버 위협에 대한 통합 방어를 제공하기 위해 여러 보안 기술, 도구 및 서비스가 통합된 포괄적인 네트워크 보안 아키텍처인 보안 생태계를 채택하여 접근 방식을 재고하기 시작했습니다. 통합 보안 에코시스템은 보안 스택에 비해 많은 이점을 제공합니다. 특히 보안 도구를 동기화하여 작동하고 통합 관리 플랫폼을 통해 운영 및 유지 관리를 단순화함으로써 위협 탐지 및 대응이 향상되었습니다.

Cyber Command는 Sangfor의 확장된 탐지, 방어 및 대응(XDDR) 프레임워크의 일부로 NGAF, Endpoint Secure 및 Neural-X를 포함한 다른 Sangfor 제품 및 서비스와 원활하게 통합되도록 설계되었습니다. 내장된 SOAR 모듈을 사용하는 Cyber Command는 이 통합 시스템의 핵심이며 다른 구성 요소에 효과적인 대응 조치를 취합니다. 예를 들어, NGAF에 특정 IP 주소나 포트와의 통신을 차단하도록 지시할 수 있습니다. Endpoint Secure는 손상된 호스트의 데이터를 Cyber Command에 제공하여 IOC를 추출할 뿐만 아니라 NDR 플랫폼의 지침을 실행하여 손상된 호스트를 격리하고 모든 엔드포인트에서 동일한 악성 코드를 검색할 수 있습니다.

또한 Cyber Command는 Palo Alto, Fortinet, Sophos, Cisco, Bitdefender, Trend Micro, WatchGuard 등과 같은 업계를 선도하는 다양한 공급업체의 타사 방화벽과 엔드포인트 보호 시스템을 통합하여 기능을 확장합니다. 이러한 협력적 접근 방식은 사고 대응 역량을 제공하는 역량을 강화합니다.

또한 이제 보다 심오한 분석 및 탐지 프로세스를 위해 타사 장치에서 데이터를 수집하기 위한 향상된 지원을 제공합니다. 우리는 Sophos, Symantec, PaloAlto, Microsoft, Kaspersky, McAfee, Cisco, Fortinet 등과 같이 높이 평가되는 공급업체의 다양한 방화벽 및 엔드포인트에서 데이터를 수집하는 기능을 통해 통합 기능을 확장했습니다. 이 기능은 네트워크 내의 잠재적인 엔드포인트 위협에 대한 보다 포괄적인 이해를 제공하여 운영 가시성을 강화하고 이를 효과적으로 탐지하고 대응할 수 있는 역량을 제공합니다.





» 구성요소

Cyber Command

Cyber Command는 Sangfor 통합 보안 생태계의 핵심 구성 요소로, 알고리즘과 기계 학습을 적용하여 데이터의 상관 관계를 분석하고 네트워크 이상 현상의 형태로 숨겨진 위협을 사전에 찾아냅니다. 또한 사고 대응 중에 지휘관의 역할을 맡아 감지된 위협을 억제하고 해결하기 위한 대응 조치를 실행하도록 다른 보안 구성 요소에 지시를 내립니다.

Stealth Threat Analysis (STA)

Sangfor STA는 Cyber Command 솔루션에 사용되는 센서입니다. 스위치에서 미러링된 원시 네트워크 트래픽을 수집하고 소스 및 대상 IP 주소, 프로토콜, 포트, 패킷 크기, 타임스탬프 및 기타 네트워크 수준 데이터와 같은 트래픽 메타데이터를 추출하는 장치입니다. 데이터를 상황별 이벤트 로그와 연관시킨 다음 보다 심층적인 분석을 위해 Cyber Command에 전달합니다.

Neural-X Threat Intelligence

Sangfor Neural-X는 AI로 구동되는 고급 클라우드 기반 위협 인텔리전스 및 분석 플랫폼입니다. VirusTotal, IBM X-Force, AlienVault OTX, EmergingThreats.net, Abuse.ch 등을 포함하여 널리 확립된 소스의 악성 패턴 및 동작에 대한 실시간 위협 인텔리전스를 지속적으로 강화합니다. 딥 러닝, 봇넷 탐지, 샌드박싱, 파일 평판과 같은 추가 구성 요소는 모든 Sangfor 보안 제품이 진화된 위협과 새로운 위협에 대해 효과적인 상태를 유지하도록 보장합니다.

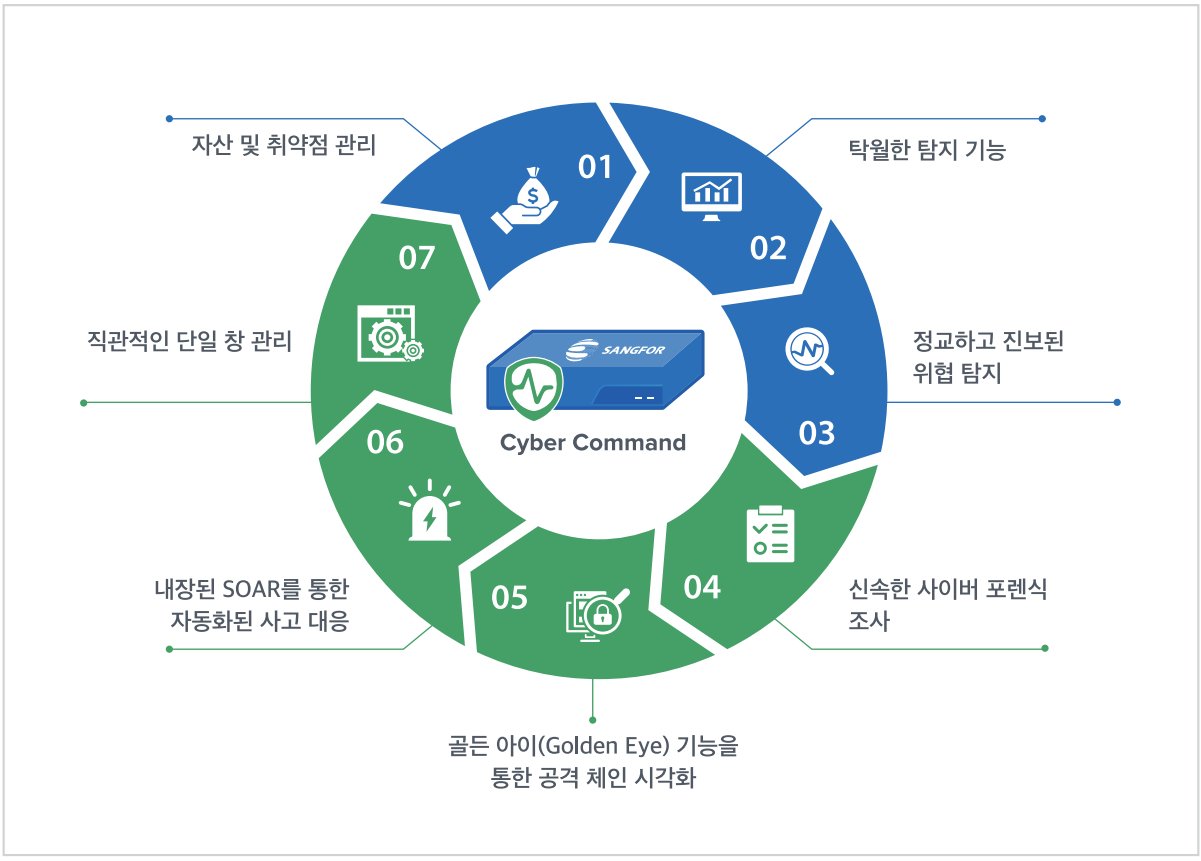
Network Secure Firewall

Sangfor Network Secure는 네트워크 경계, 데이터 센터 및 웹 애플리케이션에 포괄적인 L2-L7 보안 보호를 제공하는 차세대 방화벽입니다. Cyber Command와 통합되면 NGAF는 분석을 위한 중요한 네트워크 보안 이벤트 정보를 제공하고 Cyber Command의 지시를 받아 IOC(침해 지표)를 차단하고 감염된 네트워크 세그먼트를 격리합니다.

Endpoint Secure (EDR)

Sangfor Endpoint Secure는 Sangfor AI 악성코드 탐지 엔진인 Engine Zero를 기반으로 PC와 서버에서 악성코드를 식별하고 대응하는 고급 엔드포인트 보안 솔루션입니다. Endpoint Secure는 Cyber Command가 풍부한 디지털 증거를 수집하여 법의학 조사를 지원하는 동시에 Cyber Command가 Endpoint Secure와 협력하여 엔드포인트 위협을 해결하도록 돕습니다.

» 주요 특징들



1. 자산 및 취약점 관리

Cyber Command는 네트워크 환경에 위험을 초래하는 이전에 알려지지 않은 섀도우 IT 자산을 포함하여 환경의 모든 자산을 자동으로 검색하고 목록을 작성합니다. 또한 Cyber Command는 제거된 시스템 패치, 취약한 비밀번호, 잘못된 구성, 암호화되지 않은 트래픽과 같은 다양한 취약성을 탐지하여 보안 팀이 위협 행위자가 악용하기 전에 즉각적인 해결 조치를 취할 수 있도록 지원합니다.

2. 뛰어난 탐지 능력

Cyber Command는 AI 및 ML 알고리즘은 물론, 적이 사용하는 전술, 기술 및 절차를 자세히 설명하는 광범위한 MITRE ATT&CK 매핑 프레임워크를 활용하여 비교할 수 없는 실시간 탐지 기능을 제공합니다. 이 프레임워크를 사용하면 위협 패턴과 공격 벡터를 세부적으로 이해할 수 있습니다. UEBA 기술과 함께 Cyber Command는 사용자 및 개체 동작을 모니터링하여 기준을 설정하고 실시간 이상 탐지를 위한 기계 학습을 사용합니다.

3. 정교하고 진보된 위협 탐지

Cyber Command는 최첨단 AI 및 기계 학습 방법론을 활용하여 랜섬웨어 및 암호화폐 채굴을 포함한 지능적이고 정교한 위협을 탐지하는 데 탁월합니다. 이러한 고급 알고리즘은 네트워크 트래픽, 시스템 동작 및 사용자 상호 작용을 지속적으로 면밀히 조사하여 잠재적인 위협을 실시간으로 정확하게 인식합니다. 위협을 효과적으로 식별하고 완화하기 위해 Cyber Command는 행동 분석, 서명 기반 탐지, 동적 샌드박스 분석을 포함하는 다각적인 접근 방식을 사용합니다.

4. 신속한 사이버 포렌식 조사

유사한 보안 로그를 통합 이벤트로 병합하고, 영향을 받은 자산을 강조 표시하고, 포괄적인 포렌식 분석을 수행하여 보안 자동화를 통해 대응 효율성을 높입니다. 이 방법론에는 IOC(침해 지표) 및 BIOC(행동 손상 지표) 수집과 사고 후 평가 보장이 포함됩니다. 혁신적인 Cyber Command 플랫폼에서 필요에 따라 원활하게 다운로드하고 내보낼 수 있는 광범위한 IOC 및 BIOC를 효율적으로 조사하고 인증합니다.

5. 골든 아이(Golden Eye) 기능을 통한 공격 체인 시각화

Sangfor Cyber Command의 고유한 Golden Eye 기능은 보안 팀에게 IP 주소, 도메인, 포트 또는 URL을 입력하기만 하면 사이버 공격의 모든 단계를 표시하는 공격 체인에 대한 매우 직관적인 그래픽 표현을 제공합니다. 이는 진입점, 공격 소스 등을 추적하고 공격의 영향과 심각도를 이해하는 등 심층적인 근본 원인 분석을 통해 보안 팀이 가장 적절하고 효과적인 조치를 취할 수 있도록 지원합니다. 사용자는 각 단계를 자세히 분석하여 해결을 위한 자세한 통찰력과 해결 제안을 얻을 수 있습니다.

6. 내장된 SOAR를 통한 자동화된 사고 대응

Cyber Command는 고유한 내장 SOAR 모듈을 통해 자동화된 대응을 제공합니다. 사전 정의된 플레이북 템플릿을 통해 보안 팀은 몇 가지 일반적인 위협 시나리오에 대한 사고 대응 조치를 쉽게 조정할 수 있습니다. 또한 특정 요구 사항에 맞게 응답을 맞춤화할 수도 있습니다. Cyber Command SOAR을 통해 조직은 보안 사고로 인한 영향을 크게 최소화하고 보안 팀을 기본적이고 반복적인 작업에서 해방시킵니다.

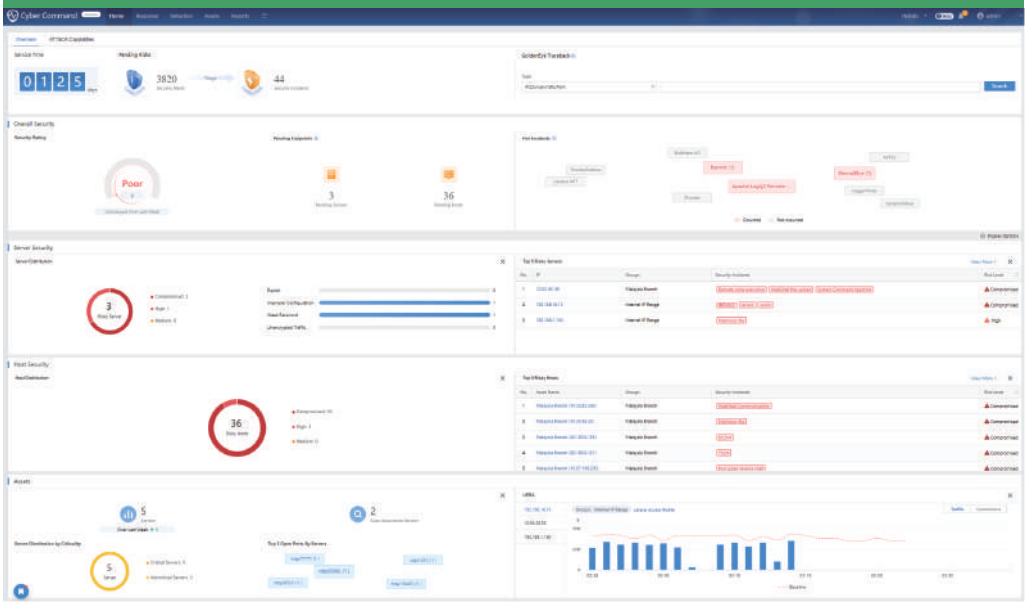
7. 직관적인 단일 창 관리

Cyber Command 플랫폼은 매우 직관적이고 사용자 친화적인 관리 콘솔을 제공합니다. 단 몇 번의 클릭만으로 보안 상태, 사이버 공격 상태, 자산 상태 및 취약성 상태에 대한 포괄적인 개요를 제공하는 단일 창 대시보드에서 보안 운영을 관리할 수 있습니다. 이 중앙 집중식 보기를 통해 시스템 성능을 쉽게 모니터링 및 분석하고, 잠재적인 위협을 식별하고, 위험을 완화하기 위한 사전 조치를 취할 수 있습니다.

» 최상의 가시성과 고급 탐지 및 대응으로 위협을 차단하세요

Cyber Command는 전반적인 보안 상태의 그래픽 표시, 보안 사고 모니터링, 아웃바운드 위협 모니터링 및 글로벌 공격 모니터링을 포함하여 전체 네트워크 환경에 대한 전례 없는 실시간 가시성을 제공합니다.

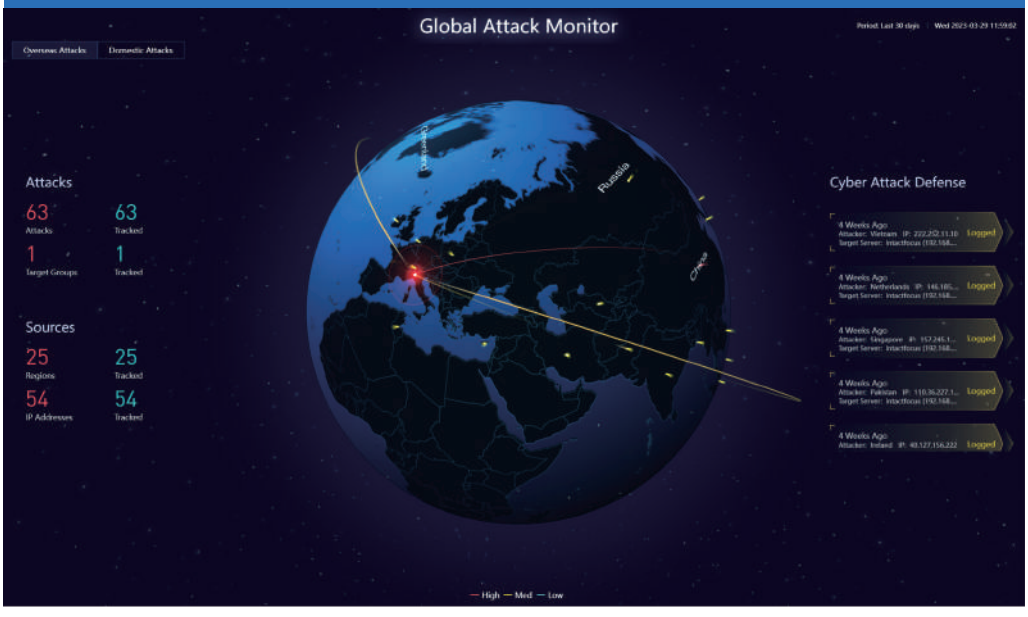
사이버 공격 자세



보안 사고 모니터링

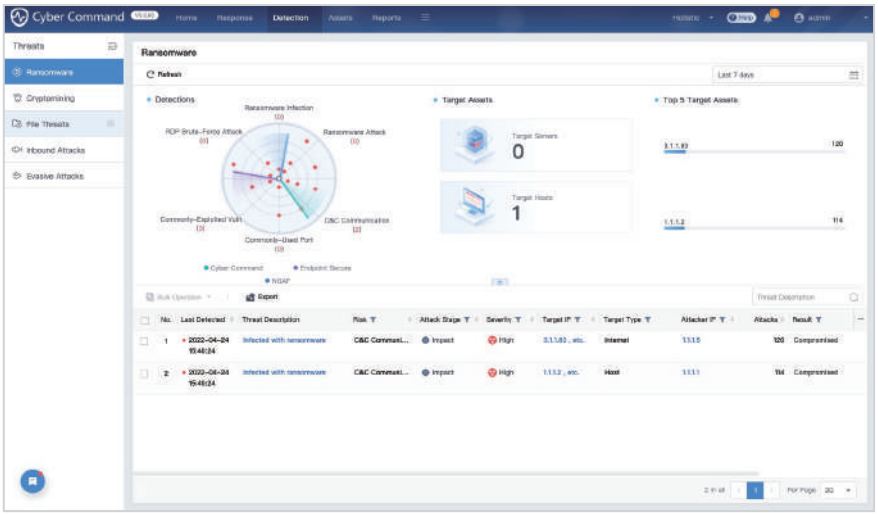
아웃바운드 위협 모니터링

글로벌 공격 모니터링

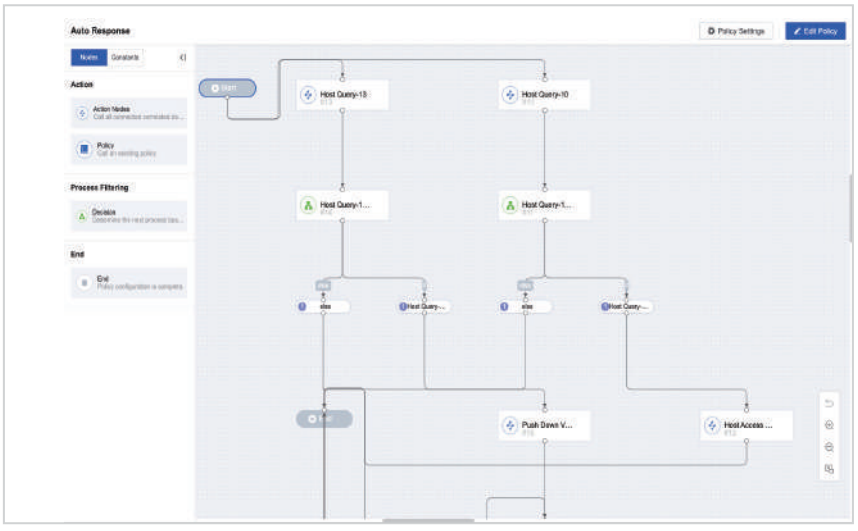


Cyber Command는 다중 탐지 엔진과 고급 위협 탐지 기술을 통해 정교한 사이버 위협으로부터 조직을 보호하고, 내장된 SOAR은 탐지된 위협에 대한 즉각적인 사고 대응을 보장합니다. 전체 MITRE ATT&CK 매핑은 정보에 입각한 의사 결정을 위한 자세한 통찰력을 추가로 제공합니다.

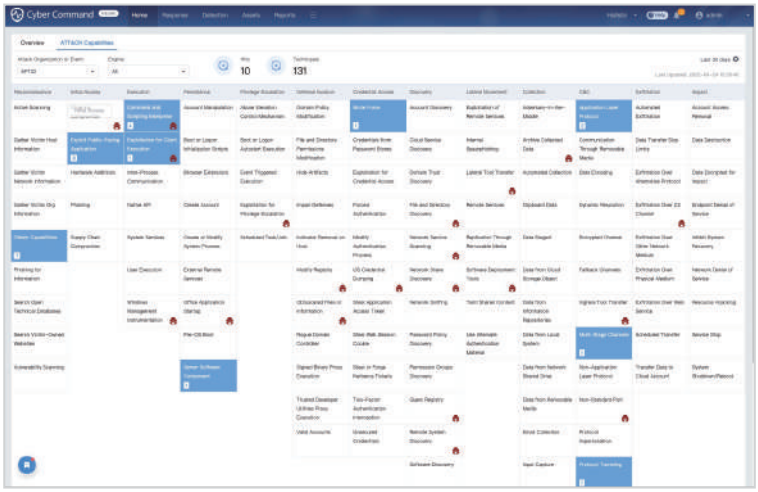
고급 위협 감지

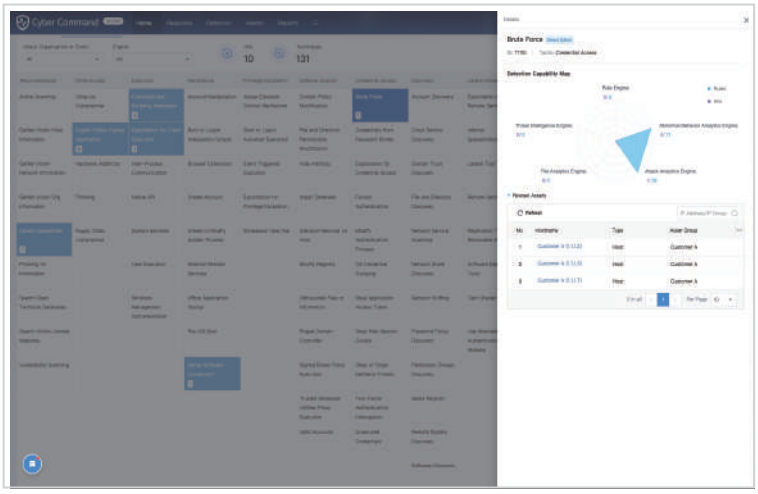


SOAR를 통한 자동 응답



MITRE ATT&CK 매핑





» Cyber Command는 어떻게 다른가요?

탁월한 위협 탐지 및 분석	
AI 기반 위협 탐지 및 분석	Cyber Command는 고급 AI 알고리즘과 기계 학습 기술을 활용하여 위협 환경을 지속적으로 학습하고 이에 적응함으로써 랜섬웨어, 제로데이 공격, APT, 사이버 마이닝과 같은 광범위한 위협을 정확하게 식별하고 분석할 수 있습니다. Cyber Command에는 Sangfor의 Neural-X 위협 인텔리전스 및 분석 플랫폼이 탑재되어 있어 광범위한 소스의 실시간 위협 인텔리전스, 패턴 및 행동을 지속적으로 강화하여 지능형 위협과 새로운 위협에 효과적으로 대응할 수 있습니다.
사용자 및 개체 행동 분석(UEBA)	Cyber Command는 UEBA 기술을 통합하여 불규칙성이나 네트워크 이상 현상을 신속하게 식별하고 추가 비용 없이 사용자와 장치, 애플리케이션, 서비스 등 네트워크 개체 모두에서 비정상적인 행동 패턴을 탐지합니다. 이를 통해 플랫폼은 정상적인 행동의 동적 기준을 설정하고 잠재적인 위협을 나타낼 수 있는 이상 현상을 정확하게 식별할 수 있습니다.
전체 MITRE ATT&CK 범위	Cyber Command는 MITRE ATT&CK 프레임워크에 대한 탐지 및 대응 기능의 포괄적인 매핑을 제공하여 조직에 초기 정찰부터 데이터 유출까지 공격 라이프사이클의 모든 단계에 걸쳐 공격 기술에 대한 광범위한 적용 범위를 제공하고 보안 팀에 우선순위를 정할 수 있는 가시성과 통찰력을 제공합니다. 대응 조치를 취하고 자원을 보다 효과적으로 할당합니다.

보다 심층적인 위협 탐지 및 법의학 조사	
비즈니스 영향 분석	Cyber Command는 다른 NDR 솔루션보다 뛰어난 BIA(비즈니스 영향 분석)가 포함된 내장형 위협 사냥 모델을 제공합니다. BIA는 자산 우선순위와 자산 손상 시 비즈니스에 미치는 영향을 이해하는 데 도움이 됩니다. 이를 통해 조직의 네트워크 및 자산에 대한 잠재적 영향을 명확하게 파악하여 복구 전략을 미리 준비할 수 있습니다.
혁신적인 골든 아이 기능	Cyber Command는 보안 팀이 전체 공격 라이프사이클을 쉽게 조사할 수 있는 능력을 부여하도록 설계된 Sangfor의 고유한 "골든 아이(Golden Eye)" 기능을 활용합니다. IP, 도메인, URL 또는 포트를 입력하기만 하면 공격자의 진입점과 공격 경로를 보여주는 포괄적인 실시간 타임라인 보기에 액세스할 수 있습니다. 이는 일반적으로 다른 공급업체에서 제공하는 기본 보안 사고 보고를 넘어서는 심층적인 근본 원인 분석을 제공합니다.
사이버 포렌식 조사	단 몇 번의 클릭만으로 탐지부터 컨텍스트 및 증거 통찰력까지 얻을 수 있는 간소화된 워크플로를 통해 조사 프로세스를 향상하세요. 혁신적인 Cyber Command 플랫폼을 통해 필요할 때 언제 어디서나 쉽게 다운로드하고 내보낼 수 있는 다양한 IOC(침해 지표) 및 BIOC(침해 행위 지표)를 신속하게 연구하고 검증합니다.

진정한 자동화 및 통합 사고 대응	
내장형 SOAR 모듈	Cyber Command는 추가 비용 없이 내장된 SOAR 모듈을 통해 NDR 솔루션을 혁신하고, 자동 사고 대응을 제공하여 조직이 감지된 위협의 잠재적 영향을 최소화하고 표적 대응 조치를 자동으로 생성 및 실행함으로써 보안 팀의 작업 부하를 크게 줄일 수 있도록 지원합니다. Cyber Command의 SOAR 모듈은 몇 가지 일반적인 위협 시나리오에 맞춰진 사고 대응 플레이북과 함께 제공됩니다. 사고 대응 전략에 대한 더 큰 유연성과 통제력을 제공하기 위해 보안 팀은 조직의 고유한 요구 사항 및 정책에 맞게 플레이북을 쉽게 사용자 정의할 수 있으며, 내장된 템플릿을 복제하거나 복사하여 기존 보안 도구에서 실행할 수 있습니다.
완전히 통합된 보안 플랫폼	Sangfor는 보안 제품을 전체적인 보안 플랫폼에 통합하는 몇 안 되는 보안 공급업체 중 하나입니다. Sangfor XDDR(Extended Detection, Defense, and Response)은 Cyber Command, NGAF, IAG 및 Endpoint Secure를 원활하게 통합하여 보안 사일로를 무너뜨리고 전체 네트워크 인프라에 엔드투엔드 보호를 제공합니다. Cyber Command는 Cisco, Trend Micro, Sophos, Bitdefender, Microsoft, Fortinet, Palo Alto 등과 같은 업계 거대 기업의 유명 타사 보안 솔루션과 통합되어 기존 보안 프레임워크를 방해하고 구성을 복잡하게 하지 않으면서 신속하고 자동화된 사고 대응을 제공할 수도 있습니다. .

» Cyber Command의 비즈니스 가치

1 피해 영향 방지

사이버 공격의 파괴적인 영향은 데이터 손실, 금전적 손실, 평판 손상부터 규정 준수 위반에 이르기까지 기업에 심각한 영향을 미칠 수 있습니다. 이러한 위험을 완화하기 위해 Cyber Command는 사이버 위협이 피해를 입히기 전에 사전에 탐지하고 예방하는 고급 방어 시스템을 제공합니다.

2 보안 운영 간소화

Cyber Command는 네트워크 전체의 데이터를 상호 연결하여 충실도가 높은 경고를 생성하여 경고 피로와 비효율성을 초래하는 오탐의 수를 크게 줄입니다. 보안 팀은 일상적인 작업을 더욱 자동화하여 운영 및 유지 관리 워크로드를 줄여 가치를 창출하는 중요한 작업에 집중할 수 있습니다.

3 보안 지출 최적화

Cyber Command는 UEBA(사용자 및 개체 행동 분석), 위협 인텔리전스, SOAR 등 다른 공급업체에서 일반적으로 추가 구독이 필요한 많은 기능을 포함하는 비용 효율적인 NDR 솔루션입니다. 큰 비용을 들이지 않고도 사이버 보안 태세를 강화하는 포괄적인 솔루션입니다.

4 디지털 혁신 수용

보안 문제는 조직이 신기술을 채택하고 새로운 디지털 비즈니스를 전개할 때 가장 큰 장애물 중 하나입니다. Cyber Command의 지원을 받아 조직은 모든 보안 위협을 즉시 감지하고 처리할 수 있으므로 안심하고 디지털 혁신을 크게 추진할 수 있습니다.

» 사이버 보안의 골드 스탠다드를 경험해 보세요

Top 3 APAC Security Vendor
by revenue based on 2021 Gartner Market Share: Security Software

Visionary Vendor
in 2022 Gartner Magic Quadrant for Network Firewalls for Sangfor NGAF

World's 4th Largest NDR Vendor
by revenue based on 2021 Gartner Market Share: Enterprise Network Equipment

Representative Vendor for NDR
in 2022 Gartner Market Guide for Network Detection and Response

ICSA Labs Firewall Certification
Sangfor NGAF meets all of ICSA Labs' corporate and baseline firewall requirements

AV-Test Certification
Sangfor Endpoint Secure receives Top Award for Windows antivirus software for business users

AAA Rating from CyberRatings
Sangfor NGAF achieves the highest security effectiveness at 99.7%

Recognized by VirusTotal
Sangfor Engine Zero AI Malware Detection Engine included in list of VirusTotal vendors

Cybersecurity Excellence Awards
Gold Winner for the Most Innovative Cybersecurity Company & Best Cybersecurity Company 2022

InfoSec Awards
Winner of Hot Company Security Company of the Year 2022

Call Us

당사의 포괄적인 제품군을 통해 귀하의 조직을 한 단계 더 발전시킬 수 있는 완벽한 제품을 찾으실 수 있습니다.

글로벌 핫라인: +60 12 711 7511 (또는 +60 12 711 7129) **Email:** Marketing@sangfor.com

더 많은 정보를 얻으려면 오늘 저희 웹사이트를 통해 저희에게 연락하십시오!

Free POC

무료 Cyber Command POC를 통해 조직의 탄력성을 보장하세요.

이번 기회에 보안 태세를 평가하고 개선해 보세요!

SANGFOR CYBER COMMAND

INTERNATIONAL OFFICES

SANGFOR SINGAPORE
10 Ubi Crescent, #04-26 Ubi
Techpark (Lobby B), Singapore 408564
Tel: (+65) 6276-9133

SANGFOR HONG KONG (CHINA)
Unit 1612-16, 16/F, The Metropolis Tower,
10 Metropolis Drive, Hung Hom, Kowloon, Hong Kong
Tel: (+852) 3845-5410

SANGFOR INDONESIA
Atrium Mulia 3rd Floor, Jl. H.R. Rasuna Said Kav.
B 10-11 Kuningan, Setia Budi, Kecamatan Setiabudi, Kota Jakarta
Selatan, Daerah Khusus Ibukota Jakarta 12910, Indonesia
Tel: (+62) 21-2168-4132

SANGFOR MALAYSIA
No. 45-10 The Boulevard Offices, Mid Valley City,
Lingkaran Syed Putra, 59200 Kuala Lumpur, Malaysia
Tel: (+60) 3-2702-3645

SANGFOR THAILAND
141 Major Tower Thonglor (Thonglor10) Floor 11 Sukhumvit Road,
Kholngtan Nuea Wattana BKK, Thailand 10110
Tel: (+66) 02-002-0118

SANGFOR PHILIPPINES
Unit 14B 14th Floor, Rufino Pacific Tower, 6784 Ayala Avenue,
Makati City, Metro Manila, Philippines
Tel: (+63) 916-267-7322

SANGFOR VIETNAM
210 Bùi Văn Ba, Tân Thuận Đông, Quận 7,
Thành phố Hồ Chí Minh 700000, Vietnam
Tel: (+84) 903-631-488

SANGFOR SOUTH KOREA
Floor 15, Room 1503, Yuwon bldg. 116, Seosomunro,
Jung-gu, Seoul, Republic of Korea
Tel: (+82) 2-6261-0999

SANGFOR UAE
D-81 (D-Wing), Dubai Silicon Oasis HQ Building,
Dubai, UAE
Tel: (+971) 52855-2520

SANGFOR PAKISTAN
Office No.210, 2nd Floor, "The Forum",
Plot No. G-20, Block 9, Khayaban-e-Jami, Clifton, Karachi, Pakistan
South Region: +92 321 2373991
North Region: +92 345 2869434
Central Region: +92 321 4654743

SANGFOR ITALY
Floor 8, Via Marsala, 36B, 21013 Gallarate VA, Italia
Tel: (+39) 0331-6487-73

SANGFOR TÜRKIYE
A Blok. Kat 51. D 643, Atatürk Mh, Ertuğrul Gazi Sk,
Metropol İstanbul Sitesi. 34758 Ataşehir/İstanbul
Tel: (+90) 216-5156969

AVAILABLE SOLUTIONS

IAG - Internet Access Gateway
Secure User Internet Access Behaviour

Network Secure - Next Generation Firewall
Smarter AI-Powered Perimeter Defence

Endpoint Secure - Endpoint Security
The Future of Endpoint Security

Cyber Command - Network Detection and Response
Smart Efficient Detection and Response

Omni-Command - Extended Detection and Response
Revolutionize Your Cyber Defense with Intelligent XDR

TIARA - Threat Identification, Analysis and Risk Assessment
Smart Threat Analysis and Assessment

IR - Incident Response
Sangfor Incident Response – One Call Away

Cyber Guardian - Managed Threat Detection & Response Service
Faster Response Through Human/AI Collaboration

HCI - Hyper-Converged Infrastructure
Fully Converge Your Data Center

MCS - Managed Cloud Services
Your Exclusive Digital Infrastructure

VDI - aDesk Virtual Desktop Infrastructure
Seamless Experience, Secure and Efficient

Access Secure - Secure Access Service Edge
Simple Security for Branches & Remote Users

EDS - Enterprise Distributed Storage
The Only Secured Data Storage You Need

SD-WAN
Boost Your Branch with Sangfor

SANGFOR

Sales: sales@sangfor.com

Marketing: marketing@sangfor.com

Global Service Center: +60 12711 7129 (or 7511)

www.sangfor.com

CC_BR_P_Cyber Command-Brochure_20240515