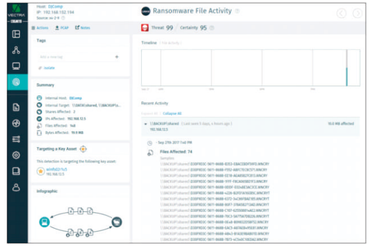
관리자의 관리 행위 감시!

공격자는 침입 초기에 사용자 PC를 감염 시킬 수 있지만, 실제의 목적은 관리자 PC 또는 주요 시스템의 접근 권한을 얻기 위해 노력할 것입니다. Cognito는 간단한 사용자의 이상 행위를 감시를 넘어 의심스런 관리 행동의 징후를 감지합니다.

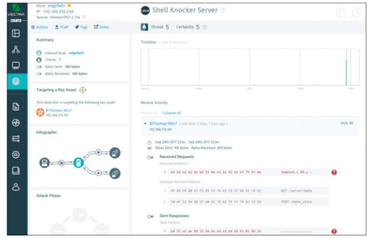
Cognito는 관리자들이 사용하는 관리 프로토콜을 추적하고, 특정 호스트, 서버 및 업무 등을 관리하기 위해 사용되는 특정 시스템이나 중간에 거치는 점프 시스템간의 관리 행위를 학습합니다. 이러한 학습 결과를 기반으로 공격자가 관리자로 위장하여 공격을 시도할 때 신속하게 감지 할 수 있습니다.

가상화 환경 보안

Private-Cloud 데이터 센터는 많은 조직에서 중요한 데이터 활용 공간으로 사용되고 있지만 보안 관리 측면에서는 관리의 어려움이 존재합니다. Cognito는 매우 세밀하고 정교한 공격까지 탐지할 수 있는 엔진을 통해 서비스 어플리케이션, 데이터 및 인프라를 지속적으로 모니터링 합니다.



Cognito의 Ransomware 공격 행위 탐지



Cognito의 Shell-Knocker 행위 탐지

데이터 센터 트래픽의 약 80 %는 데이터 센터를 벗어나지 않으며 전형적인 경계선 기반 보안 솔루션들로는 모니터링 되지 않습니다. Cognito 가상화 센서(vSensors)는 모든 VMware vSwitch에 연결하여 가상 환경에서 발생되는 모든 트래픽을 확인하고 위협을 탐지합니다.

또한 Cognito는 VMware vCenter와 연동되어 가상화 환경에 대한 운영 정보를 실시간으로 확인 할 수 있습니다. 실제로 Cognito는 필요한 가시성, 행위 학습 및 분석결과 그리고 인텔리전스를 결합하여 데이터 센터 내부의 고급 공격을 찾아낼 수 있습니다.

하드웨어부터 업무 프로세스까지!

데이터 센터 보안은 가상화 환경이 적용된 물리적 서버의 하드웨어 및 데이터 센터를 관리하는데 사용되는 Low-Level의 도구를 포함합니다. Cognito는 응용 프로그램 계층에서 하드웨어까지 전례없는 위협 탐지 기능을 제공합니다.

예를 들어, Cognito의 Port Knocking 탐지 기능은 실제 운영체제 자체에 상주 할 수 있는 루트킷에 의해 손상된 서버를 나타냅니다. 또한 Cognito는 IPMI 및 iDRAC와 같은 Low-Level 관리 프로토콜의 부적절한 사용을 모니터링하고 탐지합니다.

서버 하드웨어의 ILO(Infrastructure-Light-Out) 관리를 위해 관리자가 일반적으로 사용하는 이러한 프로토콜은 공격자가 지속적으로 목표로 삼고 있지만, 자체적으로 로깅 및 모니터링이 거의 되지 않기 때문에 공격자의 백도어로 사용될 수 있습니다.

가상화 환경 통합

최근 데이터 센터는 네트워킹, 응용 프로그램 개발, 가상화 관리 및 보안 등의 조직들 간의 지속적인 조정 및 협업이 필요합니다. Cognito를 사용하면 모든 조직이 가상 환경에 대한 완벽한 가시성을 유지할 수 있습니다.

Cognito는 가상화 환경의 모든 업무와 그 사이에 흐르는 트래픽 종류 별로 연결 상태를 시각적으로 표시합니다. VMware vCenter 연동을 통해 위협 모니터링이 되지 않는 자산에 대한 환경정보 및 시스템 자체의 Alerts을 확인 할 수 있습니다.

Data sheet

X-Series Appliances
S-Series Sensors

Cognito platform specification

SOFTWARE/NETWORKING 특징

FIPS 140-2 인증

FIPS-승인 알고리즘:
- **AES (Cert. #2273)**
- **HMAC (Cert. #1391)**
- **DSA (Cert. #709); ECDSA (Cert. #368)**
- **RSA (Cert. #1166)**
- **SHS (Cert. #1954)**
- **Triple-DES (Cert. #1420)**
- **DRBG (Cert. #281)**
- **CVL (Cert. #44)**
- **RNG (Cert. #1132)**

기타 알고리즘:
- **RSA**
  - key wrapping - RSA(키래핑)
  - Key establishment methodology provides between 112 and 256 bits of encryption strength - 112 ~ 256비트 암호화 제공
  - Non-compliant less than 112 bits of encryption strength. – 암호화 미 준수
- **EC Diffie-Hellman**
  - key agreement – 키교환
  - Key establishment methodology provides between 112 and 256 bits of encryption strength
  - Non-compliant less than 112 bits of encryption strength

미연방 정보 처리 표준 인증

하드웨어 사양

	S2 Sensor	X29 Appliance	X80 Appliance
Capture 포트	• 4EA * 10/100/1000 BASE-T • 2개의 인라인 구성 가능	• 2EA * 10/100/1000 BASE-T • 2EA * 10G SFP+	• 4EA * 10G SFP+
관리 포트	• 2EA * 10/100/1000 BASE-T 1개는 지원 포트 • One RJ-45 serial 콘솔 포트	• 2EA * 10/100/1000 BASE-T • 1EA * VGA video port • 2EA * USB 3.0 ports • 1EA DB-9 serial port	• 1EA * 10/100/1000 BASE-T • 1EA * 10G SFP+ • 1EA * VGA video port • 2EA * USB 2.0 ports • 1EA DB-9 serial port
저장 용량	• 1TB HDD	• 1.2TB HDD * 4EA(Data) • 480G SSD * 2EA(Data) • 240G SSD (system) 총 6TB	• 1.2TB HDD * 8EA(Data) • 1TB SSD * 2EA (system) 총 12TB
입력 전압	•100-240 VAC, 50-60 HZ	•Dual modular power supplies : auto-sensing 100-240 VAC, 50-60 Hz	•Dual modular power supplies : auto-sensing 100-240 VAC, 50-60 Hz
Power	•60 watts	•550 watts	•1800watts
전류	•5A	•7.4 A at 120 VAC, 3.7 A at 240VAC	•7.5A – 18A
크기	•1.74 in. (44.19 mm) H x 9.09 in. (230.88 mm) W x 7.74 in. (196.59 mm) D	•1.75 in. (45 mm) H x 17 in. (432 mm) W x 26 in. (660 mm) D	•1.7 in. (43 mm) H x 17.2 in. (437 mm) W x 27.82 in. (707 mm) D
무게	•5.18 lbs (2.3 kg)	•27 lbs (12 kg)	•26 lbs (11.8 kg)
환경	Operating Temperature: • 32° to 104° F (0° to 40° C) Non-Operating Temperature: • -4° to 158° F (-20° to 70° C)	Operating temperature: •32° to 95°F(0°to35°C) Non-operating temperature: • 32° to 122° F (0° to 50° C)	Operating Temperature: •50° to 95°F(10°to35°C) Non-Operating Temperature: •-40° to 158°F(-40°to70°C)

VIRTUAL SENSORS

Throughtput	• 400 Mbps • 1 Gbps • 2 Gbps • 5 Gbps	• 2 virtual CPU cores • 4 virtual CPU cores • 8 virtual CPU cores • 16 virtual CPU cores	• 8GB RAM • 8GB RAM • 16GB RAM • 64GB RAM	• 100 GB disk space • 150 GB disk space • 150 GB disk space • 600 GB disk space
필요 사양	• VMware ESXi 5.0 or later • Intel or AMD CPUs supporting SSE3 and SSE4 • 2EA network interfaces			

VECTRA Security that thinks® Goodus Breathing Life into Technology

관련 문의 : 한국 총판 굿어스㈜ Security.biz@goodus.com / 070-7017-4100

Overview

VECTRA®

The **Cognito** Automated Threat Detection and Response Platform

Highlights

- 네트워크 내에서 활동중인 공격자를 찾습니다.
- 결정적인 응답으로 보안 조사를 자동화합니다.
- 모든 공격 단계에서 위협을 지속적으로 추적합니다.
- 내부 및 인터넷의 모든 트래픽을 모니터링 합니다.
- 보안 시스템, 인증 시스템 및 SaaS 애플리케이션의 로그를 분석합니다.
- 모든 장치 (운영 체제, BYOD 및 IoT)를 포함합니다.
- 모든 인프라(물리적 및 가상환경)를 보호합니다.
- SIEM, 방화벽, NAC 및 EndPoint 솔루션과 통합 연계하여 상관 분석을 지원합니다.

Vectra의 Cognito™는 네트워크에서 공격자를 발견하고 막을 수 있는 가장 빠르고 효율적인 솔루션입니다. 인공 지능을 사용하여 실시간 공격 가시성을 제공하고 탐지된 공격 세부 내용을 기반으로 즉각적인 조치를 취할 수 있도록 지원합니다.

Cognito는 고급 머신러닝 기술(지도학습, 비지도학습, Deep Learning 및 Neural 네트워크 기술을 포함)을 사용하여 숨겨진 공격자와 알려지지 않은 공격자가 피해를 주기 전에 신속하고 효율적으로 탐지합니다.

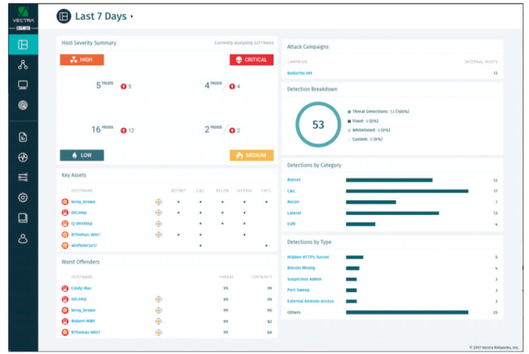
또한 Cognito는 보안 시스템, 인증 시스템 및 SaaS 어플리케이션등의 모든 네트워크 트래픽 및 로그를 분석하여 사각 지대를 제거합니다. 이는 데이터 센터, Cloud 환경, 사용자 PC 및 IoT 장치에 이르기까지 네트워크 전체의 가시성을 제공하므로 공격자가 아무것도 숨길 수 없습니다.

Security Analyst in Software

Cognito는 사이버 공격자의 Hunting을 자동화하고 그들이 숨어있는 곳을 보여주고 그들이 하는일을 알려줍니다. 가장 위험도가 높은 위협은 즉시 검토되고 호스트와 상관 분석되며 우선 순위가 지정되므로 보안 팀은 진행중인 공격을 중지하고 데이터 손실을 방지하기 위해 보다 빠르게 대응할 수 있습니다.

Cognito는 수작업으로 시간이 많이 걸리는 보안 이벤트 분석을 자동화함으로써 몇 주에서 몇 달 동안의 작업을 수분 내로 단축하고 위협 조사의 보안 분석 작업 부하를 29배 줄입니다.

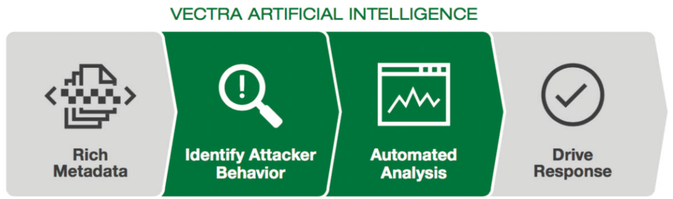
이러한 자동화를 통하여 보안 운영팀이 사이버 공격자가 시도하는 숨겨진 위협을 보다 빠르게 대응할 수 있습니다.



Cognito는 사이버 공격의 우선 순위를 결정하고 주요 자산과 상호 연관시켜 공격자의 위치와 진행중인 공격 행위를 보여줍니다.

AUTOMATE SECURITY OPERATIONS USING AI

How Cognito works



- Network traffic
- System, Auth logs
- IoCs (STIX

- Machine learning
- Data Science
- 행위 분석
- 자동 상관 분석

- 내부에 침투한 공격자를 탐지!
- 위협에 따른 조치 우선순위 제공
- 공격 및 감염호스트들의 연관성 제공 (Attack Campaigns)

- 위협에 대한 직관적인 UI 제공
- 자동 대응 방안 제공
- 통합 연동을 통한 조치 (F/W, Endpoint, SIEM, etc...)

다양한 분석 데이터 - Metadata

Cognito는 정밀한 패킷 검사를 수행하는 대신 패킷에서 Metadata를 추출하여 네트워크 트래픽을 실시간으로 파악할 수 있게 하여 정보를 누출하지 않고 보호 할 수 있습니다.

Metadata 분석은 모든 내부(East-West) 트래픽, 인터넷(North-South)트래픽, 가상 인프라 및 클라우드 컴퓨팅 환경에 적용됩니다. Cognito는 네트워크 내의 모든 IP 지원 장치를 식별하고 추적하며 위협점수를 산정합니다.

이러한 가시성은 랩탑, 서버, 프린터, BYOD 및 IoT 장치뿐만 아니라 데이터 센터 및 클라우드의 가상 환경의 트래픽, SaaS 애플리케이션까지 포함하여 모든 운영 체제 및 어플리케이션까지 확장됩니다.

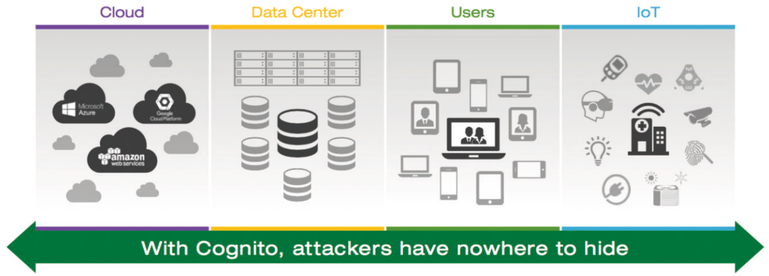
시스템, 인증 및 SaaS 로그는 시스템 및 사용자의 정확한 식별을 위해 네트워크 Metadata 분석결과를 강화시키는 효과를 제공합니다.

Cognito는 STIX 위협 인텔리전스 사용하여 알려진 위협 지표를 기반으로 위협을 탐지할 수 있습니다. 이는 호스트의 위험도와 정확도 점수의 확실성을 보장합니다.

공격자의 행위 분석!

수집된 Metadata는 숨겨진 공격자와 알려지지 않은 공격자를 찾아내는 행위 탐지 알고리즘으로 분석됩니다.

이것은 원격 액세스 도구, 숨겨진 터널, 백도어, 자격 증명 남용, 내부 정찰 및 확장, 데이터 유출과 같은 기본적인 공격자 동작을 나타냅니다.



Cognito는 기업 전체의 가시성을 제공합니다.

Cognito는 지속적으로 로컬 환경을 학습하고 모든 물리적 호스트 및 가상 호스트를 추적하여 감염된 장치 및 내부자 위협의 징후를 찾아냅니다. 다음과 같은 다양한 종류의 사이버 위협이 공격의 모든 단계(킬체인)에서 자동으로 탐지됩니다.

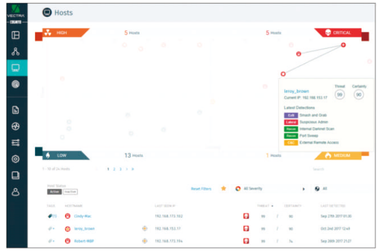
- C&C 및 기타 숨겨진 통신
- 내부 정찰(Internal Reconnaissance)
- 측면 확장(Lateral Movement)
- 계정 자격 정보 남용
- 데이터 유출
- Ransomware 활동의 초기 증상
- 봇넷 활동
- 내부의 위협 호스트 및 외부의 C&C로 의심되는 서버와의 연관성(Attack Campaigns)

또한 Cognito는 권한이 부여된 직원이 중요한 자산에 의심스러운 형태로 접근하는 행위뿐만 아니라, 클라우드 또는 USB 저장장치로의 데이터 저장 행위 및 네트워크에서 데이터를 이동하는 방법 및 툴 등과 관련된 정책 위반 행위를 모니터링하고 탐지합니다.

자동화된 분석!

Cognito는 Metadata를 분석하여 내부적으로 수천 개의 이벤트와 장기간에 걸쳐 학습된 상황을 자동으로 통합 상관분석하여 공격자가 공격을 성공시키기 위해 할 수밖에 없는 행위라고 판단될 경우 위협도와 정확도 점수를 산정하여 운영자에게 보여줍니다.

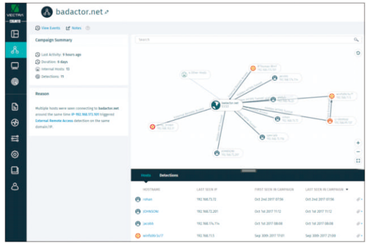
Cognito에 의해 탐지된 결과는 SIEM, Firewall, IPS, 포렌직, Endpoint 등의 보안 솔루션들과의 연계를 통하여 조치 할 수 있습니다.



Cognito는 위협이 탐지된 호스트들을 우선순위를 정하여 보여줍니다.

"Attack Campaigns" 기능은 C&C 서버로 판단되는 외부 호스트와 내부의 위험호스트들 간에 통신 상황을 자동 분석하여 연관도를 제공합니다.

탐지된 이벤트를 하나하나 분석하여 연관성을 찾을 필요 없이 자동으로 분석하여 연관성을 제공하므로 운영자는 공격의 진행 상황을 빠르고 편하게 인지할 수 있습니다. (분석 시간 및 비용 절감 효과)



Cognito는 내/외부 위협 호스트들간의 연관성을 자동분석하여 제공합니다.

대응 및 조치!

Cognito의 탐지 결과를 활용하여 위협에 신속하게 대응 할 수 있습니다. 다른 보안 분석 제품과 달리 Cognito는 공격의 대상인 손상된 호스트 및 주요 자산과 위협을 자동으로 상관 분석하여 조치 우선 순위를 제공함으로써 기존의 수 많은 이벤트들을 분석하고 결과를 산출하는 작업을 제거시켜 줍니다.

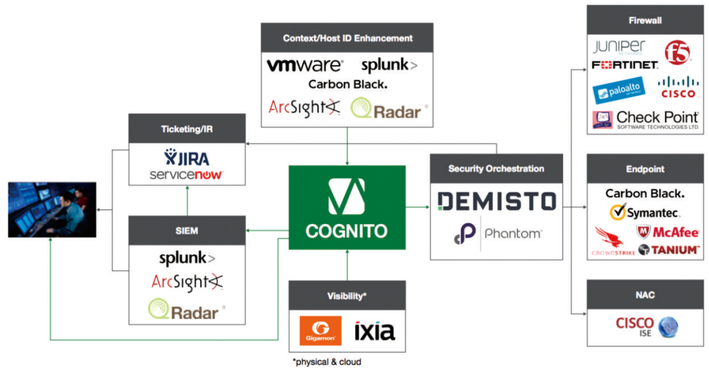
Cognito는 위협 탐지 세부 정보(위협에 대한 상세정보, 패킷, 위협도 및 확실성 점수 포함)를 즉각적으로 제공합니다.

또한 Cognito는 차세대 방화벽, Endpoint 보안, NAC 및 기타 솔루션들과 협력하여 알려지지 않은 맞춤형 사이버 공격을 자동으로 방어 및 차단할 수 있습니다.

Cognito는 기업에서 발생되고 있는 위협 조사에 대한 명확한 시작 포인트를 제공하여 SIEM 및 포렌직 등 분석 솔루션들의 활용도 및 효율성을 높여줍니다.

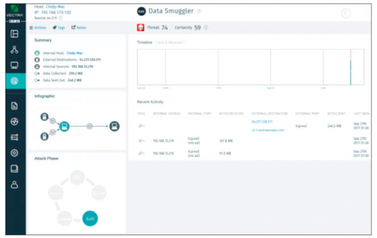
Cognito는 자동화된 위협 탐지 및 대응방안을 제공합니다.

Cognito's Integration!



Cognito는 다양한 보안 솔루션 및 분석 솔루션과 연동되어 있습니다.

Security that thinks®



데이터를 유출하는 행위를 실시간으로 탐지

보안 운영 비용 및 시간 절감효과!

Cognito는 신속하고 정확하게 위협 탐지 및 조치를 해야하는 보안 운영 팀의 부담을 덜어주고 팀원들의 업무 효율성을 향상 시켜줍니다. 이는 시간이 많이 걸리는 보안 이벤트 분석을 자동화하고 숨겨진 위협을 끊임없이 찾아야 할 필요성을 없애주기 때문입니다.

각 탐지는 다양한 근거 데이터와 함께 자세히 설명됩니다. 운영자는 탐지되는 즉시 호스트의 위협 상황 및 위협 공격을 시도한 방법을 확인할 수 있습니다.

또한 Cognito는 포렌직 분석을 위해 탐지된 위협 행위의 패킷을 제공합니다. 이를 통해 보안팀은 신속하고 정확하게 조치에 대한 의사 결정을 할 수 있습니다.

기존 보안 인프라의 활용도 상승효과!

Cognito는 방화벽, Endpoint 보안, NAC 및 기타 솔루션들을 통해 새로운 위협 요소 차단을 위한 인텔리전스를 제공하거나, SIEM 및 포렌직 도구를 이용하여 추가 상세분석을 할 수 있도록 명확한 분석의 시작점을 제공함으로써 기존 보안 인프라의 활용도를 더욱 높여줍니다.

Cognito는 주요 Endpoint 보안 솔루션들과 연동하여 위협 호스트에 대한 대응 및 조치를 자동으로 진행 할 수 있습니다.

또한 RestAPI를 제공하여 사실상 모든 통합분석솔루션들이 Cognito가 탐지한 위협 정보를 활용할 수 있고, 이 위협 정보를 syslog 및 CEF 로그로 전송할 수도 있습니다.

Ransomware 공격의 전체 과정을 탐지!

Cognito는 기업 및 기타 조직에 대한 Ransomware 공격의 전체 과정을 탐지합니다.

내부 네트워크의 전체 트래픽을 모니터링 함으로써 Ransomware를 직접 탐지할 뿐만 아니라 Ransomware 공격을 성공시키기 위해 사전에 실행하는 모든 단계의 위협 행위를 탐지합니다.