Anomali Enterprise

실시간 포렌식

매일 새로운 위협이 발견되며 수백만의 기존 침해지표(IOC, Indicators of Compromise) 목록에 추가되고 있다. 이와 관련하여 두가지 새로운 어려움을 겪게 된다.

- 이미 진행 중인 공격을 찾기 위해 새로 식별된 위협 정보를 지속적으로 추가 적용
- 새로운 공격의 식별을 위해 수백만의 IOC 항시 확인 및 대입 적용

첫 번째 어려움은 특별히 더 치명적이다. 새로운 위협이 알려질수록 보안팀은 특정 공격자가 이미 우리 회사의 네트워크를 공격 대상으로 설정했는지 아니면 이미 침입하여 진행 중인지 알아야 할 필요가 있다. 즉, 잠재적 침해가 있는지 파악하기 위해 과거 이력 데이터를 6개월 이전 혹은 그 보다 더 이전부터 훑어봐야 한다는 것을 의미한다. 두번째 어려움은, 수백만 이상의 침해지표에 대해 매일같이 매칭 작업을 수행하는 것으로 그 조직은 확산 중인 위협에 대해 네트워크의 가시성을 유지할 필요성이 있음을 의미한다.

32% 의 조직만이 **이전 3개월치 데이터**를 보관하고 있으며,

4% 의 조직만이 **이전 1년치 데이터**를 보관하고 있다.

2017 Ponemon Survey

새로운 위협의 탐지

어떤 조직에 침해가 발생했는지 판단하려면 보안팀은 반드시 새로운 위협 인텔리전스를 가져와 수개월에서 일년 전까지의 네트워크 활동 기록과 비교해봐야 한다. Anomali는 실시간 포렌식(RTF) 기술을 개발하여 과거의 방대한 이력정보를 대상으로 수시간/수일에 걸쳐 수행해야 하는 비교 작업을 수초 내로 끝낼 수 있다. RTF는 Anomali Enterprise의 핵심이며, 보안팀에게 모든 이력 데이터에 대한 신속한 가시성을 제공해준다.

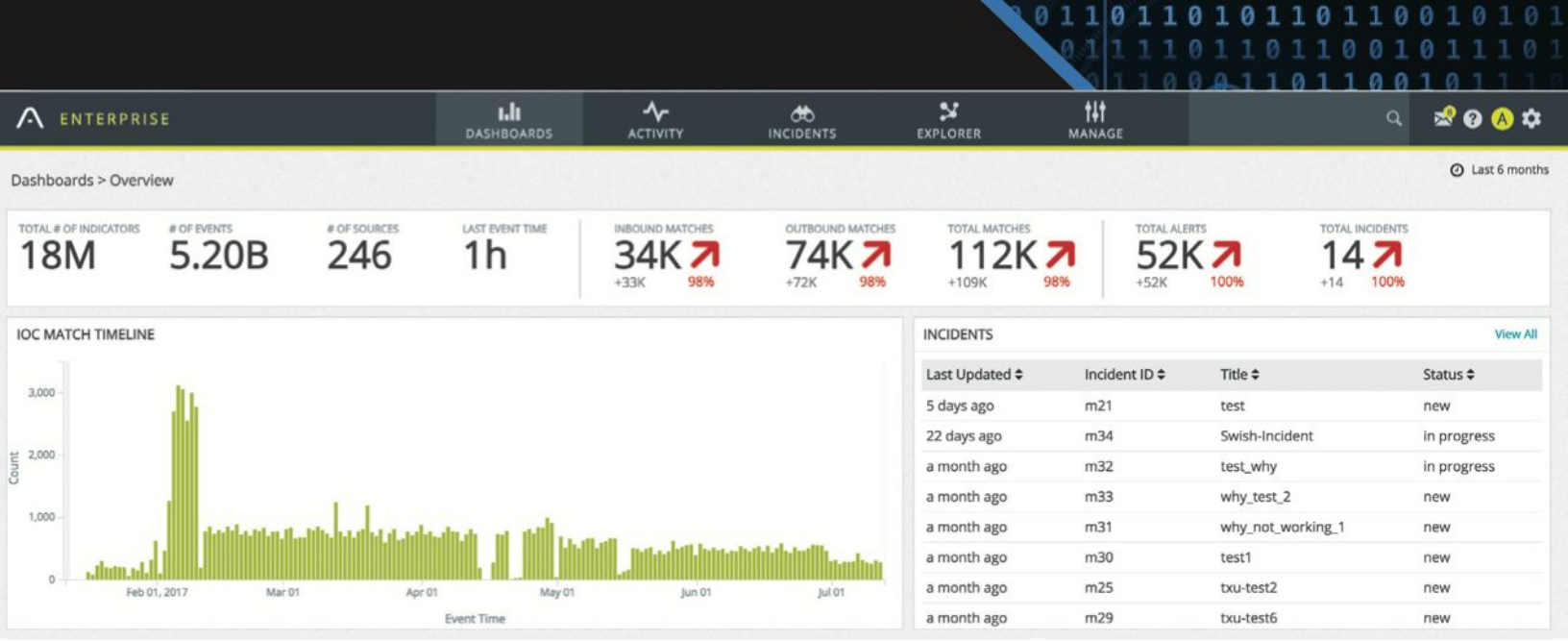
진행 중인 위협의 탐지

보안팀은 기업의 트래픽과 알려진 위협을 상호 대조하여 조직의 보안 상태가 건강한지 모니터링하는 작업을 끊임없이 수행한다. 위협 인텔리전스 지표는 순식간에 수백만 단위로 증가하며 그 각각은 내부 로그와 이벤트 데이터에 적용되어야 한다. Anomali Enterprise는 이러한 방대한 인텔리전스 매칭 작업을 수행하기 위해 만들어졌으며, 수백만 단위의 IOC를 수십억 단위의 내부 로그 및 이벤트 데이터와 비교하는데 특화되어 있다. 특별히 식별된 "관심 지표(Indicators of Interest)"는 자동으로 SIEM에 전달되어 지속적인 모니터링과 차단에 활용된다.

지표들은 관련 정보로 더 강화되거나 Anomali의 위협 인텔리전스 플랫폼인 ThreatStream을 통해 추가 조사할 수 있다. 보안팀은 Anomali Enterprise의 강력한 검색 기능을 ThreatStream의 통합, 공유, 데이터 강화 기능과 쉽게 연동할 수 있다.

실시간 포렌식(RTF)을 통한 즉각적인 위협 식별

ANOMALI®
808 Winslow Street, Redwood City, CA 94063 USA
1-844-4-THREATS | info@anomali.com | www.anomali.com



직관적인 인터페이스와 대시보드로 위협 매칭의 체계적 알림 및 분석 과정 간소화

핵심 기능

Anomali Enterprise는 조직에 이미 구축된 SIEM 및 로그 시스템과 통합되어 일 년 이상의 이력 데이터를 별도의 데이터 복제 없이 시각화할 수 있다. 이 이력 데이터들은 기존 위협 인텔리전스 정보를 포함한 새로운 위협 정보와 지속적으로 상관시키면서 침해의 증거들을 찾아낸다. 실시간 포렌식(Real-Time Forensics)은 이들 데이터에서 일치하는 요소들을 즉시 찾아내어 탐지 시간을 수초 단위로 감소시켜 준다. 또한, Anomali Enterprise는 분석가에게 위협의 분류와 대응을 위한 지표의 분류 및 등급 조정에 사용할 수 있는 각종 도구들도 제공한다.

- 365일 이상의 이력 데이터로부터 새로운 위협을 식별
- 매일 생성되는 수십억 건의 이벤트와 침해지표를 수 초 내로 매칭
- DGA 알고리즘에 의한 의심스러운 활동 탐지
- 상급 침해지표를 선정하여 SIEM으로 전달, 지속적인 모니터링에 활용

DGA

도메인 생성 알고리즘(DGA)은 통제/제어(C&C)를 위한 도메인 설치를 위해 멀웨어에서 널리 사용되는 기술이다. 특정 멀웨어는 DGA에서 생성한 도메인과 통신하도록 만들어져 있다. 이런 도메인은 알아보기 어려운 이름을 사용하는 경향이 있으며 하루 이틀 정도 활동한다. 예, jcxeionotdssqkdun.pw. 짧은 활동 기간 특성으로 인해 DGA 도메인은 통상 위협 인텔리전스 목록에 포함되지 않는 경우가 많다. 그럼에도 불구하고 Anomali Enterprise는 DGA 도메인과 통신을 시도하는 트래픽을 탐지하여 경고를 생성할 수 있다. DGA 활동을 탐지하기 위해 세련되고 정교한 알고리즘을 적용했으며 문서화된 위협 지표에만 의존하지 않는다.

포네몬(Ponemon) 연구 자료:
State of Threat Intelligence:
anomali.com/ponemon

Event Time	Event Source	Destination	URL	DGA Probability	Malware Family	Count
Aug 30th 2017, 19:50:00 -05:00	172.18.15.16	wgtbnpt64a74r7wdnyoygsqpz8s.com	-	0.96	Gameover_DGA, MadMax	11
Aug 30th 2017, 19:50:00 -05:00	172.18.19.14	tjotvtrdd1jdb9hd6xb4o85icf.com	-	1	Gameover_DGA, MadMax	16
Aug 30th 2017, 19:50:00 -05:00	172.18.13.15	1pdhc2u20gf32oqunv8uqpzbgc6.com	-	0.99	Gameover_DGA, MadMax	6
Aug 30th 2017, 19:50:00 -05:00	172.18.20.13	gh8eoyfrvr0ayxxt.com	-	0.903	Bedep, Chinad, Corebot, MadMax	8

Anomali Enterprise는 강력한 DGA 탐지 능력 보유

ANOMALI®
808 Winslow Street, Redwood City, CA 94063 USA
1-844-4-THREATS | info@anomali.com | www.anomali.com