splunk> turn data into doing

Boss of the SOC 대회에 대한 자주 묻는 질문 **(FAQ)**

updated: 2022.11.01

Q: BOTS (Boss of the SOC) 대회는 어떤 행사입니까?
A: BOTS 대회는 블루 팀 (blue-team: 방어팀)의 문제풀이(jeopardy-style) 형태로 진행되며 CTF(해킹방어대회)와 유사한 형식으로 진행됩니다. 대회 참가자들은 스플렁크의 Security Suite와 기타 리소스를 활용하여 보안 애널리스트들이 일상적으로 마주하는 실제 보안 사고와 관련된 다양한 문제를 풀게 됩니다. 본 대회가 진행되는 동안 모든 참가자들은 최대 4인으로 구성된 팀을 결성해 현실적인 보안 문제를 풀게 됩니다. 참가자들은 Splunk Search, Enterprise Security, ESCU, UBA 및 Phantom을 사용해 가능한 빠르고 정확하게 문제를 해결해야 합니다. 이를 통해 고객들은 흥미진진한 경쟁 환경에서 여러 데이터 소스, 프리미엄 제품 그리고 스플렁크 전문가들을 접할 수 있게 됩니다.

Q: 무엇을 기대할 수 있습니까?
A: BOTS 대회 참가자들은 스플렁크 데이터에서 실제와 같은 APT 해커를 조사할 수 있습니다. 고객들은 Windows Endpoints, AWS 보안로그, Microsoft Cloud Logs (Azure Authentication 및 Office365), Google Cloud Logs, Linux, Cisco NVM 그리고 Stream wire data 등에서 데이터를 탐색할 수 있습니다. 이 과정에서 고객들은 단순히 Splunk Search를 활용하는 것뿐만 아니라, UBA, ES, ESCU, 및 Phantom과 같은 자사 프리미엄 제품을 활용해야 합니다.

Q: 대회 진행은 어떻게 하나요?
A: 게임에 참가하는 모든 분들께 스플렁크 검색 서버와 문제 서버에 접속할 수 있는 계정, 암호가 게임 시작 전 메일을 통해 전달 됩니다. 우선 문제 서버에서 문제를 확인하시고, 이를 검색 서버를 통해 원하는 답을 찾아서 입력하시면 됩니다.

Q: 저희 회사에서는 참가전에 방화벽 허용을 해야해서 접속이 필요한 url 정보를 알아야 합니다.
A: 서버는 미리 할당해 놓은 상태로 대회 전날 오픈될 예정이며 방화벽 신청은 미리 해두시는 것이 좋을 것 같습니다. 참고로, 스코어링서버와 서치해드서버는 모바일로 접속해서 진행하기 힘듭니다.

1) 스플렁크 서치헤드 : AWS 에 스플렁크 클라우드 인스턴스가 제공됩니다. AWS에 접근이 가능하시면, 문제가 없습니다.
2) BOTN 스코어링 서버 URL: bots.splunk.com

Q: 어떤 제품들을 알고 다뤄야 하나요?
A: 가장 기본적으로는 **Splunk Enterprise**를 다루는 것을 기본으로 하고 있습니다. 그리고 **SPL**을 이용해서 검색해서 원하는 정보를 찾을 수 있어야 합니다. 그리고 추가적으로 ITSI 관련해서도 문제가 있지만, 이는 ITSI 화면에서 원하는 정보를 찾는 수준이기 때문에 문제를 푸는데 크게 지장은 없습니다.

Q: 문제의 난이도가 어떻게 되나요?
A: 문제의 난이도는 다양합니다. 대시보드 화면에서 단순하게 정보를 찾아서 입력하는 것에서 실제로 SPL 문을 만들어서 원하는 정보를 추출해야 풀 수 있는 문제도 있습니다. 그리고 문제의 난이도에 따라서 점수도 다르게 적용됩니다. 적절하게 힌트를 사용하세요.

Q: index나 sourcetype 등이 사전에 제공이 되는지 아니면 다 스스로 찾아서 해야 하는지요?
A: index나 sourcetype 을 문제에서 지정해 주지 않습니다. 그러나 많은 문제들이 문제를 해결하는 과정에서 index나 sourcetype을 찾을 수 있습니다. 그리고 힌트에 숨어있는 경우도 있습니다.

Q: 이번 대회에서 Enterprise Security (혹은 SOAR)가 활용됩니까?
A: 네, 당연히 활용됩니다! ES 와 SOAR 뿐만 아니라 ESCU와 UBA도 사용됩니다.

Q: MLTK도 사용됩니까?
A: 아니요.

Q: 고객이 위협사냥(Threat Hunting) 혹은 침해사고 대응에 관심이 있는 경우 도움이 될 수 있을까요?
A: BOTS대회는 고객의 스킬 연습을 위한 것으로 교육에 치중된 워크숍들의 캡스톤 프로젝트로서 기획되었습니다. 일부 고객은 직접 해보고 바로 실행에 옮기는 것을 통해 많이 배울 수 있습니다. 교육에 좀 더 관심이 있으시다면, 11월 24일 버츄얼로 진행되는 Advanced APT hunting workshop 워크샵에 오시면, Threat Hunting에 대해 더 자세히 배우실 수 있는 기회가 될 것입니다.

Q: 참 좋은 것 같습니다. 어떻게 진행되는지요?
A: BOTS 대회의 문제 난이도는 쉬운 문제에서 어려운 문제까지 다양합니다. 문제 별 올바른 방향으로 안내하는 힌트가 있으며, 힌트가 더 필요한 경우를 대비해 현장과 온라인상에 코치들이 배치되어 지원해드립니다. 또한 유념할 것은 BOTS대회는 팀 경기이기 때문에 팀원을 직접 모시고 오시면 함께 참여할 수 있습니다.

Q: 총 소요시간은 얼마나 되나요?
A: 약 5~6시간 소요될 예정입니다. (셋업 및 종료에는 1.5시간소요, 경기진행은 4.5시간 소요)

Q: 사전 준비는 어떻게 하나요?
A: BOTS 대회 준비를 위한 몇 가지 매우 유용한 방법은 다음과 같습니다.

- ☐ “Hunting With Splunk” 블로그 시리즈 확인해 보세요. 무엇보다 이 시리즈에서 다루는 주제들을 정복하면 더 많은 문제를 더 빨리 풀 수 있는데 도움이 됩니다.
- ☐ 무료 Free Splunk Fundamentals 1 Training 활용해 보세요. (https://www.splunk.com/en_us/training/free-courses/splunk-fundamentals-1.html)
- ☐ 스스로 BOTS 대회 환경을 구축하여 연습해 보세요. (https://www.splunk.com/blog/2018/05/10/boss-of-the-soc-scoring-server-questions-and-answers-and-dataset-open-sourced-and-ready-for-download.html)

Q: 팀 구성에 어려움이 있습니다. 2명 팀도 지원이나 혼자서도 지원을 할 수 있을까요? 추가 멤버 등록을 하고 싶으면 어떻게 하나요?
A: 2명 또는 혼자서도 게임에 참여를 하실 수는 있지만, 점수 획득에 3명 또는 4명팀과 차이가 나게 됩니다. 추가 멤버 등록은 등록 기간 12월 7일 내에 가능합니다.

Q: 대회 준비에 도움을 받고 싶습니다. 어디에 문의 할 수 있을까요?

사전 문의 사항 및 필요한 기술 팁을 Splunk Korea 2022 Boss of the SOC 슬랙 채널을 통해 문의할 수 있습니다. 스플렁크 유저 그룹 가입 신청서를 제출하신 후, Korea BOTS 슬랙채널에 입장해주세요. 가입에 어려움이 있으시면 여기(splunk@purplepig.co.kr)로 문의 해주세요.