안녕하세요.
파이어몬 "Cloud Security Operation - SecOps 와 DevOps 의 줄다리기"을 주제로 한 WEBINAR 에 참석해 주셔서 감사드립니다.
WEBINAR 진행중에 문의 주셨던 내용들에 대한 답변을 간략하게 작성하였습니다.
추가 궁금한 점이 있으시거나 더 자세한 답변을 원하시는 경우 알려주시면 상세하게 답변 드리겠습니다. 다시 한번 감사드립니다.

<Q&A 리스트>

1. 일반적인 클라우드 보안

[질문] 요즘 화두가 devops 다음의 aiops 그리고 secops 같습니다. secop 는 앱가상화레벨에서 고민이 되어야 할까요/ 아니면 이것도 운영체제 아랫단에서부터 고민되어야 할까요?

[답변] 클라우드 보안의 Shared Responsibility Model 에서 어떤 단계의 클라우드 서비스를 사용하시는 지에 따라서 사용자가 책임져야 할 보안의 범위가 결정됩니다. PaaS/SaaS 를 사용하고 계시다면 운영체제와 아랫단의 보안/운영은 CSP(Cloud Service Provider)가 책임지게 됩니다.

[질문] 클라우드 보안에도 제로데이 취약성 같은 성질의 보안 우려 영역이 있을까요?

[답변] 제로데이 취약성은 벤더와 개발자가 알지 못하는 소프트웨어의 취약점을 공격자가 이용하는 것으로 클라우드에도 위협은 여전히 존재합니다. 다만 서비스 모델에 따라 CSP 가 책임지는 보안의 영역이 있기 때문에 사용자는 사용자 책임 영역에만 집중을 하면 되는 장점이 있습니다. 이런 위협에 대응하기 위해서 위협이 퍼져 나가지 못하게 하는 Zero Trust 의 개념이 중요하며 VPC/VNET 의 보안 컨트롤에 대한 설정과 관리가 더욱 중요합니다.

[질문] 온프레미스 환경과 클라우드 환경의 보안의 큰 차이점이 무엇인가요? 백업, 보안솔루션등으로 불가한 건지, 취약점이 많다면 그에 가장 큰 대책은 무엇인가요?

[질문] 일부 회사에서는 Schedule 백업을 지원하여 보안사고가 발생했을 경우 보안사고 이전의 Snapshot 을 이용하여 몇 초 내로 복구될 수 있도록 지원합니다. FireMon 에서는 클라우드 백업 시 어떤 방식을 주로 추천하나요?

[답변] 많은 차이점이 있지만 다른 운영 환경, 스킬셋의 부족, 빠른 변화 등이 가장 큰 이유가 아닐까 생각됩니다. 실제로 전문가들은 misconfiguration 을 클라우드 환경의 가장 큰 위

협이라고 얘기하고 있습니다. 예로, 백업은 이메일 보안등과 같은 데이터를 백업하는데 클라우드는 많은 장점을 제공합니다. 하지만 계속해서 변하는 (CI/CD pipeline) 어플리케이션을 백업을 사용하여 보호하기는 힘듭니다. 결국 클라우드의 이런 차이점과 우선순위를 이해하고 그에 맞는 보안 대책을 세우는 것이 필요할 것 같습니다. 웨비나 발표에서 소개 드린 클라우드 보안의 우선순위를 참고하시면 도움이 될 것 같습니다.

[질문] CI/CD 의 속도 관점에서 보면 보안의 적용을 strict --> loose 틱하게 가는게 좋을지 문의 드립니다.

[질문] 데브옵스의 발생 동기는 빠른 릴리즈를 근본 목표로 하고 있습니다. 이를 위해서는 빠른 개발 릴리즈 프로세스를 만드는 것도 중요하지만, 테스트 절차를 효율화 하는 것이 무엇보다도 중요합니다. 하지만 기존 기업들이 개발하던 방식과 레거시 코드가 테스트를 자동화를 적용하기에 쉽지 않은 구조인데요. 이를 위해서 어떻게 해야 할지요?

[답변] 아무래도 CI/CD 환경에서 정적인 보안 프로세스를 적용하는 것은 무리가 있습니다. CI 단계에서는 어플리케이션 보안으로 어플리케이션 관점의 보안 적용이 필요하며 CD 단계에서는 Deploy/Operate 단계에서의 가드레일 설정을 통한 보안 적용을 통해 misconfiguration 을 방지하는 노력이 필요할 것 같습니다.

[질문] 멀티클라우드 환경하에서 각 클라우드 간에 통합 사용자 인증과 안전한 데이터 공유 방안은?

[질문] IAM 이 중요하다고 하셨는데 멀티 클라우드를 사용중일때는 IAM 을 프라빗과 퍼블릭 별도로 가져가야 하는 것 인지 궁금하고 그럴 경우 보안 솔루션이 중복되는 것은 아닌지 궁금합니다. 또 파이어몬은 어떤지 궁금합니다.

[답변] 클라우드 환경에서 제공하는 IAM 서비스를 활용할 수 있으나 멀티 클라우드 환경에서는 전용 보안 솔루션이 필요할 것 같습니다. 최근에는 기존 on-prem IAM 서비스를 cloud 로 확장하고 있고, 또한 클라우드 기반의 IAM (IDaaS)이 on-prem 까지 확장하고 있습니다. 파이어몬은 IAM 서비스를 제공하는 업체는 아닙니다. 하지만 IAM 의 잘못된 설정을 확인하고 교정하는 프로세스를 제공하고 있습니다.

[질문] 클라우드 보안 같은 경우도 계속 IT 환경의 변화에 따라 기업이 계속 지속적으로 비용을 지불해야 하는 부분이 있는데요. 솔루션 도입 같은 부분뿐만 아니라 지속적인 업그레이드,

컨설팅, 전문 보안 인력 지원 등 토탈서비스를 구독 형 형태로 지원받을 수 있는 방법은 없을지요?

[질문] 공공기관에는 보안전문인력이 부족한데 인원늘리기가 참 어려운데 이런 상황에서 클라우드로 전환 시 걱정이 온프라미스 상보다 더 복잡하고 관리가 어려운 환경을 기존 인력으로 관리가 가능한지가 최대관심사인데 파이어몬은 이런 점에서 어떤 특징과 장점이 있는지요?

[답변] 클라우드 보안의 접근 방식은 기존의 SecOps 와는 달라야 합니다. 기존의 SecOps 를 DevOps 에 적용하는 것은 많은 제약점이 있고 효과적인 운영 방안이 아닙니다. FireMon DisruptOps 는 마치 DevOps 환경에 보안엔지니어를 가지게 되는 것과 같습니다. 결국 DevSecOps 프로세스를 확립하여 클라우드 운영의 주체인 DevOps 팀에서 보안 운영이 가능하도록 하는 것이 중요할 것 같습니다.

[질문] 클라우드 환경에서의 보안 이벤트를 감지하는 방식은 어떤 것들이 있나요?

[답변] 클라우드 환경에서의 가장 큰 위협은 misconfiguration 입니다. 설정 /IAM/interface/API/Security Group 등의 잘못된 설정입니다. 이런 잘못된 설정을 감지하고 또한 AWS Security Hub 등의 이벤트를 통합하여 관리가 필요합니다. 하지만 더 중요한 것은 이러한 이벤트를 어떻게 처리할 것인가 입니다. FireMon DisruptOps 는 클라우드의 분산된 환경에서 이벤트가 적절한 주체 (보안팀 혹은 DevOps 팀)에게 효과적으로 전달되어 손쉽게 처리할 수 있도록 도와줍니다.

[질문] 퍼블릭 클라우드(AWS)을 도입 중인데 보안을 위해서 IAM 을 구성하지 않고 퍼블릭 클라우드의 관리 콘솔 상 작업이 필요한 경우에 항상 담당자에게 직접 연락하라고 하는 회사를 본 적 있는데 관련하여 human error 가 그 회사에서 많이 발생하는 것 같았습니다. 이렇게 운영하는 회사에서도 FireMon 을 도입하여 도움을 받을 수 있는지 그리고 어떤 도움을 받을 수 있는지 궁금합니다.

[답변] 클라우드 보안에서 IAM 보안의 중요성/위험성을 경험한 회사가 아닌가 싶습니다. FireMon DisruptOps 는 IAM 설정 뿐 아니라 다양한 클라우드 네이티브 서비스에 대한 보안을 제공해 주고 있습니다. 또한 IAM 의 보안 위협을 방지해 관리 콘솔 만으로 작업하는 불편을 해소해 드릴 수 있습니다.

[질문] 클라우드 보안 솔루션 도입 시 정기적인 관리와 교체 주기는 어떻게 되나요?

[질문] 유지와 보수는 자체의 팀에서 관리하는 것이 좋은지요? 외부에 위탁하는 것이 좋은지요?

[답변] FireMon DisruptOps 는 SaaS 솔루션으로 정기적인 관리와 교체에 대한 요구가 전혀 없습니다.

[질문] 클라우드 보안 신뢰성 검증 표준이나 규격이 있는지요?

[답변] 현재는 CIS Benchmark (https://www.cisecurity.org/cis-benchmarks/)가 클라우드에 가장 널리 쓰이고 있는 것으로 알고 있습니다. FireMon DisruptOps 는 AWS 와 Azure 에 대한 CIS benchmark, 그리고 PCI-DSS 표준을 지원하고 있습니다.

[질문] 보안 문제로 사내 인트라넷 내에서만 클라우드 기능을 사용해야 하는 데, 프라이빗 방식으로 활용한 사례도 있나요?

[답변] 법적인 제한이 있는 경우가 아니면 현재 다양한 클라우드 접근방식을 통해서 보안을 제공하고 있습니다. CASB 나 SASE 기술을 고려해 보시면 좋을 것 같습니다.

2. FireMon DisruptOps 기능/유즈케이스

[질문]서버 및 네트워크등의 데이터센터 증설에 대응해 즉각적인 보안솔루션의 용량 증설이 가능한지 궁금합니다.

[답변] FireMon DisruptOps 는 SaaS 플랫폼으로 처리능력 요구에 대해서 자동으로 scaling/descaling 을 하며 이는 자동으로 이루어 집니다. 결국 솔루션의 운영/관리에 대해서 고객이 신경 쓰셔야 할 부분이 없습니다.

[질문] 작은 회사라서 DevOps 와 보안팀의 경계가 없습니다.
최소한의 자원으로 보안이벤트를 확인, 처리해야 하는데, 파이어몬의 경우 실시간으로 보안모니터링과 보안이벤트검색 과 같은 기능들이 어느 정도의 Depth 까지 지원되나요?"

[답변] 클라우드 보안에 관한 많은 솔루션이 마켓에 존재합니다. 하지만 FireMon DisruptOps 는 DevSecOps 를 실현하기 위한 솔루션으로 DevOps 에서 사용하는 ChatOps 툴 (Slack, Teams)에 연동하여 DevOps 에서 보안 운영과 교정 (remediation)이 가능하도록 하는 솔루션입니다. 클라우드 포스쳐를 관리하지만 여전히 DevOps 와의 연계를 통한 교정 프로세스를 지원하지 않는 솔루션과 그 Depth 가 많은 차이가 난다고 할 수 있습니다.

[질문]클라우드 보안의 취약점과 개발운영팀의 개발 소스 취약점에 대한 통합 가시성 확보와 보안 관리가 파이어몬으로 어느 단계까지 가능한지요?

[답변] FireMon DisruptOps 는 개발 소스 취약점에 대한 영역은 다루고 있지 않습니다. 클라우드 보안 운영, 즉 DevSecOps 를 가능하게 해주는 솔루션입니다.

[질문] 파이어몬으로 연동된 장비를 자동 대응 이후 각 인시던트 별로 보안부서 개별 담당자에게 개별 리포팅과 알람도 가능한지 궁금하며 클라우드 방화벽과 레거시 방화벽 모두 연동해서 개별 대응 프로세스를 가져갈 수 있는지 궁금합니다.

[질문] FireMon 에서는 클라우드 보안 대상 Host 에 대해 사용자가 정의해 놓은 보안 정책에 따라 수집된 데이터를 분석하여 정책에 위배되는 부분에 대해선 이벤트 알림 또는 접근제어를 수행하는 Tool 이나 솔루션을 지원하나요?

[답변] FireMon 은 기본적으로 네트워크 정책관리 솔루션으로 잘 알려져 있습니다. 특히 방화벽/ACL 정책의 가시성을 on-prem 과 cloud, 하이브리드 환경에서 통합된 가시성과 변경 자동화, 컴플라이언스 자동화를 구현해줍니다. 이번에 소개드린 FireMon DisruptOps 는 퍼플릭 클라우드 보안 운영에 관한 솔루션으로 보안부서, 개인, 팀 등에 ChatOps(Slack, Microsoft Teams)의 다양한 채널을 이용하여 리포팅과 알람이 갈 수 있도록 설정이 가능합니다. 또한 대부분의 알람은 ChatOps 상에서 직접 교정(Remediation)도 가능하게 해줍니다.

[질문] DisruptOps 적용관련 최근 이슈와 해결 사례가 궁금합니다.

[답변] FireMon DisruptOps 는 간단하게 사용이 가능합니다. 고객사의 클라우드 어카운트 정보를 SaaS 플랫폼에 입력해주면 바로 고객이 운영하는 퍼블릭 클라우드 환경의 보안 이슈를 발견해 냅니다. 대게 evaluation 을 통해 수십에서 수백여 개의 잘못된 세팅과 이슈를 바로 확인 할 수 있으며 많은 고객들이 ChatOps 와의 연동을 통해 DevOps 팀에서 이슈를 확인하고 바로 교정하는 프로세스를 가능하게 해줍니다. 보안팀과 DevOps 팀 간의 협업을 가능하게 해 줍니다.

[질문] 클라우드로 전환 시, On-Premise 에 비해 보안 운영자 분들이 서비스 구조를 이해하는데 어려움이 많습니다. 파이어몬이 이런 어려움 해결에 도움이 될 수 있는지요?

[질문] 세미나 주제가 보안팀과 DevOps 조직이 줄다리기라고 표현한 것 같은데요. 보안팀이 단순 보안 모니터링만 하는 것 만은 아니고 Devops 조직도 기본적인 보안을 고려한 개발을 하고 할

텐데요. 단순히 조직마다 우선순위가 다르기 대문에 줄다리기가 발생한다면, 두 조직간 연결시키고 모니터링하고 update 할 수 있는 공통의 솔루션을 공유하면 될 것 같은데요 파이어몬에서 제공하는 솔루션이 이런 공통으로 적용, 문제점을 해결해 주는 건지요?

[답변] 네 맞습니다. 기반 기술의 차이점으로 인해 이러한 부서간의 어려움이 커지는 것 같습니다. FireMon DisruptOps 는 보안팀과 DevOps 팀 간의 클라우드 보안 운영의 협업이 가능하게 해 줍니다. 그 핵심은 보안 프로세스를 실질적인 클라우드 운영주체인 DevOps 의 환경에 통합해주는 것입니다. 진정한 DevSecOps 프로세스를 확립하는 데 도움을 주고 있습니다.

[질문] 회사마다 보안 정책이 너무나 달라서 트리거를 회사마다 또는 부서마다 다르게 적용 하다 보면 복잡성이 계속 증가하는 문제가 있습니다. 이런 부분에 대한 보안 트리거의 Unified Security Trigger 의 운영 방법도 있을까요?

[답변] FireMon DisruptOps 에서는 보안 트리거를 플레이북 스타일로 관리가 가능합니다. 동일한 control 에 대한 플레이북을 전체 적용이 가능하며 또한 부서와 업무에 따라서 각각 다른 플레이북을 적용하는 것도 가능합니다.

[질문] Jira, Teams 를 사용중인 경우에 각각에 대한 제어로 실시간으로 보안 고지를 받을 수 있는지도 설명 부탁드립니다.

[질문] 온프레미스와 퍼블릭·프라이빗 클라우드가 혼재된 하이브리드 환경에서는 자동화가 무엇보다 중요해서 자동화를 확보할 수 있는 관리 시스템을 도입하고 검토하는데 실제 원활하게 작동하지 않고 있는게 현실입니다. 파이어몬 DisruptOps 는 완벽하게 보안 이벤트를 통합하고 연계 분석해 자동으로 관리할 수 있는지 궁금합니다.

[답변] FireMon DisruptOps 는 발견된 잘못된 설정, 리스트를 Jira, Teams, Slack 을 통해서 실시간 경고를 보내게 됩니다. 그 경고에는 문제에 대한 자세한 사항과 해결방법, 또한 'One click 해결' 등의 교정 프로세스가 포함됩니다.

[질문] 전통적인 보안관리체계는 개발과 운영 직무를 분리하도록 하는데요 클라우드 환경에서 DevOps 가 불가피한 경우 개발및운영 모두 담당하시는 분의 작업 내역을 승인 및 결재와 주기적 점검을 하도록 요구하고 있는데요 이를 시행하기 위한 승인결재 기능이 지원되는지요?

[답변] FireMon DisruptOps 는 현재 Slack, Teams, Jira 와의 연동을 통해 교정 프로세스를 지원하고 있습니다. 승인 결재를 위해서는 Jira 를 통한 연동이 필요합니다. Slack 과 Teams 는 ChatOps 툴로 승인 결재 없이 바로 DevOps 팀에서 교정 작업이 이루어 집니다. 또한 플레이

북 기능을 통해서 특정 조건의 이슈는 이메일/Jira 등을 통해 승인 결재 프로세스를 태우고 나머지 조건은 바로 ChatOps 를 통한 교정 프로세스를 진행하는 것도 가능합니다.

[질문] Playbooks 설정이 가능한 것을 보니 SOAR 같습니다. DisruptOps 가 SOAR 의 일종이라고 볼 수 있는지 또는 DisruptOps 도입 이후 SOAR 를 함께 운영할 필요가 있는지 궁금합니다.

[답변] SOAR 는 좀더 보안 incident 에 대한 운영/관리/대응/자동화에 가까울 것 같습니다. FireMon DisruptOps 는 상태/포스쳐에 대한 교정 프로세스의 자동화에 가까우며 이런 프로세스에 Playbook 을 사용합니다. 따라서 SOAR 하고는 차이가 있다고 생각됩니다.

[질문] 컴플라이언스를 체크할때 Failed, Needs Review, Passed 이렇게 3 가지만 가능한가요? 만약 필요시에 사용자가 체크 항목을 추가로 생성 하는게 지원되는가요?

[답변] Control 에 대한 상태는 Open, Failed (and still open) 그리고 resolved 로 이렇게 정의가 됩니다.

[질문] DisruptOps 를 통해 자동화할 경우 자동화가 가능한 범위(접근통제 적용/삭제, 계정 권한 관리 등)는 어디까지 인지와? 자동화 시 오류가 발생될 우려는 없는지? 궁금합니다.

[답변] FireMon DisruptOps 의 자동화된 교정의 예는 말씀하신 대로 '외부에 대한 엑세스 차단', '엑세스 컨트롤 생성', '계정 권한 삭제' 등이 있습니다. 이러한 교정은 클라우드 사업자가 제공하는 API 를 사용하여 오류발생 가능성을 최소화 합니다.

[질문] 이기종 클라우드에 대한 보안 자동화 운영시에 문제를 찾아서 응답하는 시간은 일반적으로 어느 정도 소요되는지도 문의드립니다

[답변] ChatOps 와의 연동이 이루어져 있어서 특정 이슈를 Slack 의 특정 채널에 할당을 하고 그 이슈에 대한 'one-click' 교정이 가능한 경우 수분 내에 프로세스 완료가 가능합니다. 실제 운영시에는 Playbook 에 대한 세팅 유무, ChatOps 혹은 Jira 와의 연동 유무, 그리고 교정 프로세스의 자동화 유무에 따라서 다양하게 시간이 걸릴 수 있을 것 같습니다. 하지만 일반 Security Ops 의 티케팅을 사용하는 프로세스는 클라우드 보안 운영에서 프로세스 자체에 단절이 존재합니다. 따라서 클라우드 보안 운영의 효율성 향상에 큰 도움이 될 수 있을 것이라 생각됩니다.

[질문] 비즈니스 프로세스와 기술적 프로세스가 하나로 되었다라는 것은 자동으로 이 2 개의 프로세스를 병렬구조가 아닌 단일의 싱글 프로세스로 운영이 가능하다고 이해하면 될까요?

[답변] 클라우드 운영은 대부분 DevOps 가 개발과 운영을 통합해 운영되고 있습니다. 그렇기 때문에 클라우드 운영에서 보안 프로세스를 따로 분리하는 것은 맞지도 않고 효율성도 떨어진다고 생각합니다. FireMon DisruptOps 는 클라우드 환경에서 보안이 DevOps 운영과 통합이 가능할 수 있도록 도와주는 솔루션입니다.

[질문] 기업의 보안 관리 기준 수립이나 관리 기준에 따른 이행 현황 파악 등의 지원으로 리스크 분석을 할 수 있나요?

[답변] FireMon 은 하이브리드 환경에서 기업의 보안 정책이 전체적인 보안 관리 기준(컴플라이언스)에 부합하는지를 실시간으로 파악해주며 이를 수치화하여 리스크의 현황에 대한 파악이 가능하게 해 줍니다. FireMon DisruptOps 는 퍼블릭 클라우드 상의 포스쳐/컨피그에 대한 기준을 수립하여 위반된 사항을 효과적으로 대응/교정 할 수 있도록 해주는 클라우드 보안 솔루션입니다. FireMon 은 궁극적으로 하이브리드 환경에서 Security Operation 에 대한 토털 솔루션 제공을 목표로 삼고 있습니다.