EQST insight

사이버 침해사고 사례를 통한 위험성 진단 및 개선점 도출 전략

하이테크1담당 이민주 책임

■ 개요

오늘날의 기업 조직은 산업 환경의 발전으로 인해 아날로그에서 벗어나 점점 디지털 환경으로 전환을 거듭하고 있으며, 기업의 디지털 의존도 또한 높아졌다. 이러한 환경의 변화로 인해 많은 침해사고가 발생하고 있으며, 특히 언론 보도를 통해 관련 사고에 대한 소식을 자주 접하게 됐다.

'소 잃고 외양간 고친다' 라는 속담은 사후적인 측면에서 '중요한 것을 잃은 후에 그 가치를 알게 되어 그때서야 관심을 기울이며 보완하려는 것'이라는 의미로 사용된다. 이를 정보보호 담당자 입장에서는 바라보면 몇 가지 교훈과 기대효과를 도출할 수 있다.

먼저, 보안 사고가 발생한 이후에 보안 조치를 강화하는 것이 아닌, 사전에 적절한 보안시스템과 절차를 마련해야 한다는 사전 대비와 예방이 필요하다는 것을 알 수 있다. 또한, 외양간을 고치는 것이 일회성이 아니라 정기적으로 유지보수 해야 하는 것을 인지하고 새로운 보안 위협이나 기술적 취약점이 발견되면 주기적으로 대응책을 마련해야 한다는 것이다. 마지막으로는 소를 어떻게 잃어버렸는지에 대한 원인을 파악하고 앞으로 같은 사고가 발생하지 않기 위한 대응 전략으로 보안 정책, 프로세스, 대응전략 등에 대한 종합적인 보안전략이 있어야 함을 알 수 있다.

이를 위해서는 먼저 현재의 보안 트렌드와 새로운 위협에 대한 통찰력을 가져야 한다. 이는 침해사고 소식에 대한 비판적 접근을 통해 얻을 수 있다. 이번 헤드라인에서는 비판적 접근을 위한 방법으로 사이버 침해사고 사례를 통한 조직 위험 진단 및 개선점 도출 전략을 소개하고자 한다.

■ 침해사고 사례를 통한 교훈점

침해사고 사례를 통해 학습할 수 있는 교훈점은 다음과 같다.

① 과거 침해사고 사례를 통한 최신 보안 위협에 대한 조기대처 가능

② 위험 예측

③ 향상된 대응 능력

④ 보안 업데이트

⑤ 위험 평가 및 취약점 관리

⑥ 보안산업 동향 분석

■ 정보의 피로도 관리 필요성

최근 사이버 침해사고는 끊임없이 발생하고 있으며, 정보의 양과 복잡성이 개인이나 조직에 미치는 영향력은 상당히 크다고 할 수 있다. 더욱이, 사이버 보안의 기술적인 용어나 개념들이 하루가 다르게 변화하고 발전하고 있어 정보의 피로도 또한 크다.

2023 년 주요 사이버위협 (일부)
국내 포털사이트 사칭 공격 알고 보니 북한 배후 APT
방송사 일반 기업 해킹의 배후로 지목된 Kimsuky 그룹
Clop 랜섬웨어 그룹의 Goanywhere 취약점 악용 캠페인
Mustang Panda 그룹의 유럽 기업을 대상으로 공격
중국 APT 그룹의 동아시아 데이터 손실 방지 소프트웨어를 개발하는 회사 타깃 공격
3CX 프로그램을 악용한 공급망 공격으로 대만의 PC 회사 침해사고
RedHotel 그룹의 대만 반도체 회사 공격

사이버 위협 동향을 수집하고 가공하는 업무를 하는 담당자의 입장에서는 이러한 정보의 피로도 관리 및 피로도 해소를 위한 대책이 필요하다. 또한, 업무의 효율성을 높이기 위해 정보를 효과적으로 관리하는 방안도 마련되어야 한다.

■ 정보 우선순위 설정

다양한 사고 소식 속에서 정보의 피로도를 낮출 수 있는 방법으로는 아래 표와 같이 침해사고 정보를 분류하고 정보의 우선순위를 설정해야 한다.

이러한 분류와 우선순위 설정을 통해 담당자는 중요한 정보에 집중하면서도 긴급한 상황에 신속하게 대응할 수 있어 정보의 피로도를 효과적으로 낮출 수 있다.

침해사고 정보 분류		
적합성	**시의성**	**정확성**
우리와 관련이 있는가?	즉시 대응이 필요한가?	사실여부는 파악됐는가?

① 적합성: 사고 정보가 우리 산업에 미치는 영향력을 비교해보고 우리 조직의 위협 여부 판단

② 시의성: 지금 일어나고 있는지? 빠른 대응을 통해 우리 조직을 진단할 필요성이 있는지 판단

⑤ 정확성: 수집된 정보가 정확한 정보인지?

데이터 가공 절차	
단계	**내용**
첩보	검증 및 평가가 되지 않은 자료
정보	분석 및 평가과정을 거쳐 타당성을 검증한 자료
지식화	일반적인 내용, 정보가 종합되어 활용할 수 있는 자료

① 첩보: 다양한 경로를 통해 수집한 첩보 데이터 (예:CyberTrace Threat Intelligence, OSINT)

② 정보: 첩보 보고된 데이터 및 보안 사고 뉴스, 보안 업체 등에서 발표한 가공된 자료

③ 지식화: 첩보+정보를 통해 우리 조직이 활용할 수 있는 형태의 자료 보고서

■ 타 사고 사례 활용 예시

아래의 사례 케이스는 '소 잃고 외양간 고친다' 속담을 인용한 스토리텔링 기반의 케이스다. 각 조직의 환경, 인력에 따라 침해사고를 다양한 형태로 정리할 수 있지만, 앞서 설명한 침해사고 정보 분류와 데이터 가공 기준을 기반으로 분석한다면 내부 환경의 취약성 점검의 중요성을 설명하는데 충분한 근거로 사용할 수 있다.

사례 1.
A 조직은 최첨단 시설을 활용한 외양간을 구축해서 운영하고 있는 회사이며 이웃 마을에 위치한 B 외양간과 경쟁관계에 있음. 최근 축사를 방문한 사료 업체로부터 B 외양간이 미상의 범죄자로부터 침입당한 첩보를 입수하여 확인 결과 도둑이 축사를 들어와서 키우던 소를 훔쳐간 사실 확인

침해 사고정보 분류		
적합성	시의성	정확성
우리와 관련이 있는가?	**즉시 대응이 필요한가?**	**사실여부는 파악됐는가?**
동일한 산업군에 속한 업체	A 회사도 구축 운영 중인 축사	재산 피해여부 확인

단계		스토리텔링	정보보안 관점 대응
1	첩보	축사 담벼락을 넘어왔다	백도어를 통한 침입인지?
		축사의 문으로 들어왔다	접근권한 관리가 제대로 되었는지?
		경보 시스템 무력화	탐지 정책 및 로그 관리가 제대로 되었는지?
2	정보	높이가 낮은 담벼락을 이용해 넘어와 도구들로 보안 시스템을 무력화시키고 문을 열어 나감	공격자가 손쉽게 내부 시스템으로 침입할 수 있는지 점검 공격자가 사용한 도구들을 내부에 유입할 수 있는 경로 점검 권한 없는 공격자가 보안 시스템에 접근하여 로그를 지우거나 탐지 정책을 회피할 수 있는 행위점검
3	지식화	공격자가 사용한 도구정보를 통한 공격자 특정 및 담벼락 높이, 보안 시스템에 대한 보안 정책 점검	1)침해지표를 통해 공격 그룹 프로파일링 2)침해지표에 대한 흔적 점검 3)보안장비를 활용해 해당 공격에 대한 시뮬레이션을 수행 4) 영향도 파악 4)권한 관리 및 권한 없는 사용자의 권한 외 요청, 접근에 대한 로그를 파악하여 사고 예방

■ 보안 사고 케이스 스터디 활용 방법

다양한 보안 사고 인텔리전스를 보다 효율적으로 정리할 수 있도록 여러 가지 방법론과 모델들이 개발되어 왔다. 아래에서는 시각화 하기 쉬운 방법을 실제 사례를 활용하여 소개하고자 한다.

1. 다이아몬드 모델: 사이버 공격을 분석하고 이해하는데 사용되는 개념적인 프레임워크

   A. 위협 활동 분석: 공격을 수행하는 주체인 위협 활동을 식별하며 개인, 사이버 범죄조직, 국가 기관 등 다양한 위협 활동 주체의 동기와 목표 나타냄

   B. 전술: 전술은 위협 활동 주체가 공격을 수행하는데 사용하는 방법과 기술을 설명하므로 공격자가 사용하는 공격 전술에 대한 대응을 시각화

   C. 목표: 위협 활동 주체가 수행하는 공격의 목적을 의미(정보 유출, 금전적 이득, 경쟁 업체에 대한 악의적인 행위, 정치적 영향력 확대 등)

   D. 인프라: 인프라는 위협활동 주체가 공격에 사용하는 다양한 자원과 도구를 나타냄(침해지표, 악성 소프트웨어 배포, 공급망 공격 관리시스템, 익명 프록시 서버 등)

2. 다이아몬드 모델을 통한 기대효과

   A. 위협 모니터링: 사이버 범죄조직 및 공격을 수행하는 공격 주체의 전술과 다양한 목적에 따른 공격 시도를 모니터링하며 공격 패턴과 동향을 관리할 수 있음

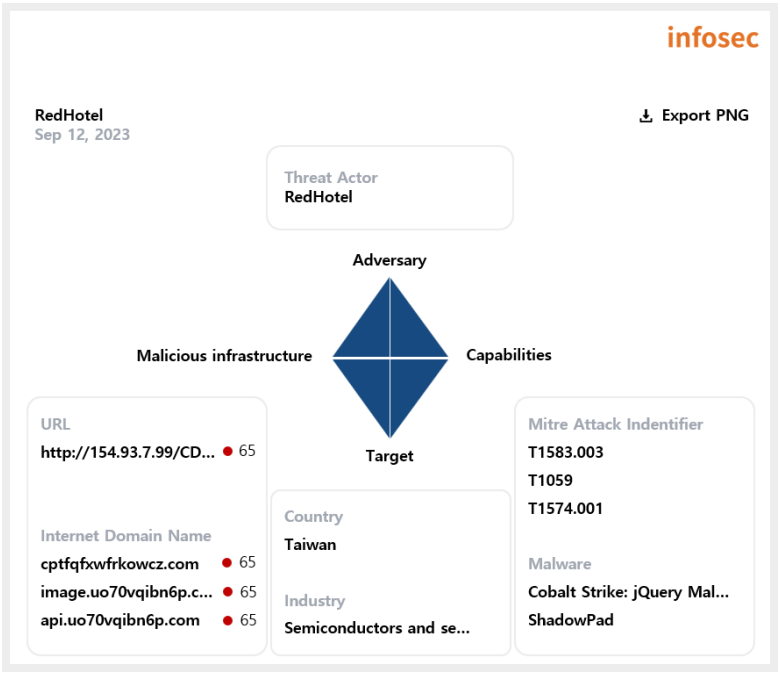
   B. 위험 평가: 사고 동향을 통해 조직의 취약성과 위협 활동 주체의 공격 가능성을 사전에 확인하여 감소시킬 수 있음

   C. 대응 전략 개발: 사이버 위협 대응 전략에 대한 통찰력을 제공하며 조직의 정보보호 및 대응 계획을 개발하고 강화할 수 있음

   D. 정보 공유: 정보공유와 협력을 장려하여 효과적인 사이버 보안 생태계를 구축할 수 있음

아래 사례는 고객사가 속한 산업군을 겨냥해서 일어난 실제 사이버 침해사고로, 이번 사고에서 발생한 위협 정보를 다이아몬드 모델에 기반하여 영향도를 점검했으며, 보안 데이터를 시각화했다.

사례 2.
China-linked cyberspies backdoor semiconductor firms with Cobalt Strike (실제기사 2023.10.05)

<table>
<tr><th colspan="4">침해 사고정보 분류</th></tr>
<tr><th colspan="2">적합성</th><th>시의성</th><th>정확성</th></tr>
<tr><td colspan="2">우리와 관련이 있는가?</td><td>즉시 대응이 필요한가?</td><td>사실여부는 파악됐는가?</td></tr>
<tr><td colspan="2">동일한 산업군에 속한 업체</td><td>고객사의 경쟁회사로 시급한 대응 필요</td><td>뉴스 보도를 통해 확인된 내용</td></tr>
<tr><th colspan="2">단계</th><th>정보 제공</th><th>다이아몬드 모델</th></tr>
<tr><td>1</td><td>첩보</td><td>뉴스 기사, CTI 업체</td><td rowspan="3"> 
</td></tr>
<tr><td>2</td><td>정보</td><td>CTI 인텔리전스 보고서</td></tr>
<tr><td>3</td><td>지식화</td><td>데이터 시각화로 대체</td></tr>
</table>

출처: 레코디드 퓨처(CTI 업체) 이미지 재가공

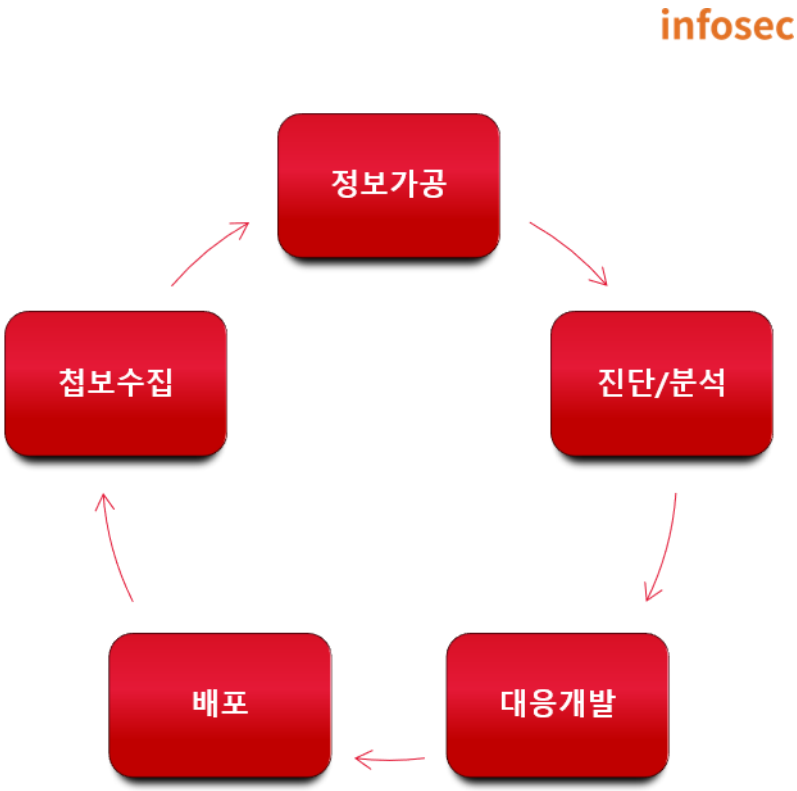
다이아몬드 모델의 각 항목을 통한 대응 방안은 다음의 항목으로 구분할 수 있다.

항목	내용	점검 필요사항
Adversary	중국 정부의 지원을 받는 것으로 추정되는 RedHotel 공격 그룹	- 공격 그룹의 최신 동향 정보 - 공격 그룹 모니터링 대상 등록
Malicious Infrastructure	공격에 악용한 침해지표	- 침해지표를 통해 내부 시스템 점검 - 침해지표에 대한 사전 차단 진행
Capabilities	마이터 어택 프레임워크를 통한 공격 전술, 전략 등을 활용해 공격 방법/경로에 대한 정보	- 공격 전술, 전략에 대한 킬체인 전략 개발 - 보안 시스템 탐지 여부 개발 - 침해 흔적 여부 조사

이러한 모델을 활용한다면 사고 동향 정보를 시각화 하여 관리할 수 있고, 공격자가 사용한 전술과 절차에 대한 이해도와 함께 연결되는 동향 정보를 연결 지을 수 있는 장점이 있다.

■ 효과적인 사고 동향 관리

많은 사고 동향을 파악하고 데이터를 생성하는 것도 중요한 일이지만, 의미 있게 사고 동향을 관리하려면 다른 조직의 사고동향을 통해 배우고 미래에 시도될 수 있는 사고에 대비하는 관리가 순환형으로 이루어져야 한다.



1. 첩보 수집: 침해 사고 정보를 다양한 정보 출처로부터 취득하여 보안 시스템 점검 방안을 수립
2. 정보 가공: 수집된 첩보 데이터를 정보화 할 수 있도록 데이터 가공
3. 진단/분석: ① 첩보+정보가공을 통해 식별된 내용에 대한 킬체인 방안 개발 및 내부 시스템 진단
   ② 전술과 기술 절차를 요약하여 진단 계획 및 탐지 계획 수립
4. 대응개발: 진단/분석을 통해 얻은 정보를 정리
5. 배포: 개선사항 및 권고사항들을 포함해 관련 부서 및 담당자 전파

■ 맺음말

다양한 사고 사례가 일어나는 환경 속에서 자신이 속한 조직을 진단하기 위해서는 외부 위협을 분석하여 개선점을 도출하고, 발전해 나가는 것이 중요하다. 이를 관리하기 위해서는 다양한 예측 방법론이 있지만, 모든 과정의 시작은 '관심'에서 출발한다. 따라서, 정보보안 담당자들은 다양한 침해사고 사례에 대해 먼저 관심을 갖고 이번 헤드라인에서 소개한 침해사고 분석 방법을 통해 조직의 위험 진단 및 개선점을 찾길 바란다.

SK 쉴더스는 축적된 노하우와 자체 기술력을 바탕으로 기업의 사이버보안 위험 진단에 필요한 전반적인 컨설팅을 종합 제공하고 있다. 업계 최대 규모의 전문인력과 인적 역량을 보유하고 있으며 보안컨설팅, 랜섬웨어 대응서비스, 해킹 사고 분석, 모의해킹, 취약점 진단 등 다양한 분야의 정보보안 컨설팅 방법론을 구축하고 실행하며 다양한 기업에게 최적화된 솔루션을 전하고 있다.

이 같은 **SK 쉴더스 컨설팅**을 통해 날로 지능화되고 있는 사이버공격에 효과적이고 체계적으로 대응하길 바란다. 보다 자세한 내용은 SK 쉴더스 공식 블로그를 통해 확인할 수 있다.