



Team Spotlight

Making an impact that matters

제 33 호 | 2018.8.31

꼼짝 마! 디지털 설록 홈즈가 여기 있다

딜로이트 안진 재무자문본부 eCrime Solutions 팀

4 차 산업혁명 시대에는 인공지능(AI), 자율주행차, 기업 내 시스템 등에서 데이터 문제가 생기면 철저히 분석해야하는 상황이 증가한다. 즉, 여러 사건 사고의 디지털 증거물을 수집, 분석해 법률적인 대응이 필요한 시대가 온 것. 세계 최고 수준의 포렌식 기술과 데이터 분석 능력으로 최상의 서비스를 제공하는 딜로이트 안진 재무자문본부 Finance crisis 그룹 eCrime Solutions 팀이 바로 그 첨병이다.

국내 최대 규모 포렌식랩 전문가 포진...경쟁 컨설팅·회계법인과 비교 불허

재무자문본부 Finance Crisis 그룹(그룹장 백철호 전무)에 소속된 eCrime Solutions 팀은 PC, 애플리케이션, 서버, 네트워크 등에서 기업의 부정적인 사건 및 사고에 대한 조사를 수행하고, 그 흔적이 되는 데이터가 법적인 증거로 효력이 있도록 추출, 확보하는 서비스를 진행하는 전문가 그룹이다.

이창성 부장이 리더를 맡고 있는 eCrime Solutions 팀에는 최기훈 차장, 성승창 차장, 김미정 과장, 유경민 과장, 최현규 과장 등 Financial Crisis 그룹이 운영하고 있는 포렌식랩(Forensic Lab.)의 전문가들이 포진해 있다. 또한 변호사, 회계사, 통계학 전문가, 빅데이터 전문가, 정보보호 심사원 등 종합 서비스를 제공하기 위한 최적의 인력 구성을 자랑하는데, 딜로이트 안진은 One-stop 서비스가 가능한 유일한 컨설팅 기업으로 정평이 나있다. 특히 포렌식랩은 국내 최대 규모로, 16 명의 전문인력을 확보하고 있다.

이러한 '외인구단'급 전문팀은 현재 포렌식 관련 서비스 수행 횟수, 실적 면에서 다른 컨설팅 기업이나 회계법인과는 비교를 불허하는 성과를 내고 있으며, 매년 가파른 성장을 기록하고 있다.

eCrime Solutions 팀은 정보통신기술 기반 사고에 대한 조사 및 대응을 위한 종합적인 서비스를 제공한다. eCrime Solutions 서비스는 기업에서 발생한 부정적인 사건 및 사고(횡령, 배임, 비리, 도난, 유출, 시스템 오류 등)의 원인을 조사하고, 포렌식 기술을 활용해 전자적인 증거를 확보하는 서비스를 말하는 것으로 법적 리스크, 내부통제, 시스템 아키텍처, 빅데이터 분석, 정보보안 등 다양한 분야의 전문성이 종합적으로 필요하다. 예를 들어, 기밀정보의 유출에 대한 증거를 PC 및 서버에서 확보하거나, 배임 및 횡령에 대한 증거자료를 ERP(전자적자원관리) 시스템 및 기타 업무시스템에서 찾아내 소송이나 내부 징계에 활용할 수 있도록 준비하는 역할을 수행한다.



Forensic 분석

(부정, 정보유출 등에 대한 Forensic 조사)

PC, 이메일, 서버 등에 대한 데이터 수집 및 복구하여 사건/사고에 대한 원인을 확인하고 증거를 확보하는 서비스

대용량 데이터 분석 및 검증

(매출/비용/실적 정산 과정 등의 부정 및 오류 조사)

사고 발생 여부, 이상 징후 등을 확인하기 위하여 독립적으로 데이터를 확보하고 분석하여 전수 검증

시스템 이상 진단

(프로그램 조작, 설정 변경 등으로 인한 이상내역 확인)

복잡성이 높고, 검증이 어려운 시스템에 대하여 독립적으로 로직을 설계하고 산출되는 수치에 대한 정확성을 검증하여 사고 발생 여부를 확인하는 서비스

Advanced Analytics

(사건/사고 발생 여부에 대한 모니터링 방안 수립)

통계적 기법과 AI등을 활용한 데이터 분석 기법으로 사건/사고 발생 여부에 대한 추가 검증을 수행하고 조기 발견 및 사전 대응을 위한 모니터링 방안을 수립

전자적 증거 확보 및 지원

(조사결과를 소송/분쟁에 활용할 수 있도록 증적화)

형사/행정/민사 등 다양한 소송에서 필요한 전자적인 증거를 법적 효력이 있도록 확보하고 지원하는 서비스



<세계 최고 수준의 포렌식 기술과 분석능력을 가진 전문가들이 한자리에 모여 사진 촬영을 하고 있다.>

사이버 사건사고, 국내외 규제 강화...국내 기업들도 발 빠른 대응

최근 IT 전문 정보조사 기관인 가트너가 정보시스템의 취약점 또는 오류로 인해 발생하는 피해액은 연 1,140 억 달러 규모이나, 그 중 84%는 적절한 책임 규명 및 보상이 이루어지지 않고 있다고 밝혔다. 또 다른 조사결과에 따르면, 국내에서 발생하는 영업비밀 및 기밀정보와 관한 분쟁 중, 78%가 증거, 입증 부족으로 무혐의 처리되고 있으며 유출 건당 피해액은 평균 16 억 원에 달한다는 조사 결과가 있다.

최근에는 기업 시스템에 대한 복잡성, 데이터의 규모 및 중요도가 증가하면서 IT 기반의 사고 발생 시 기업 이미지에 큰 부정적인 영향을 미칠 뿐만 아니라, 과징금, 소송 등으로 인한 재무적인 영향도 커지고 있어 시스템 사고에 대한 국·내외 감독기관 규제가 더욱 강화되고 있는 상황이다.

실제로 최근 국내의 한 기업이 개인 정보 유출로 45 억 원의 과징금이 부과된 사례가 있었는데, 해외에서는 유럽 GDPR(General Data Protection Regulation, 개인정보보호규정)이 발효되면서 위반 시 매출액의 4% 또는 2,000 만 유로의 과징금이 부과될 수 있는 등 전 세계적으로 사고 발생 시 책임 유·무에 대한 분쟁 및 소송이 증가할 것으로 예상하고 있다.

이런 상황에서 eCrime solutions 팀에서 진행한 실제 사례를 보면, 임직원의 배임과 협력사의 정보유출에 대한 국내 A 공공기관 조사요청에 따라, 포렌식 기법으로 삭제된 PC의 데이터를 복구하고 USB 보안, 내·외부망 연계 솔루션, 이메일, 네트워크 로그 등을 분석해 기술도면의 유출여부를 확인했으며, ERP 시스템, 출입시스템, 인사시스템, 그룹웨어 로그 등의 연계 분석을 통해 업무 배임여부에 대한 조사를 수행한 바 있다. 또한 기업에서 활용하는 다양한 유형의 정보기술 관련 데이터에 대해 종합적인 데이터 확보 및 분석을 수행, 정확한 사고의 규모를 파악함으로써 증거자료를 확보하는 등 재발방지 방안까지 수립한 의미 있는 프로젝트를 수행하기도 했다.

또한, 국내 B 기업을 대상으로 시스템 오류 및 이상 내역(임의적인 조작, 변경)에 대한 조사를 수행한 바 있다. 이 기업은 비즈니스 특성상 대용량 데이터에 복잡한 정산과정을 수행해 매출과 비용을 확정하고 있어 산출되는 금액의 검증이 어려운 상황이었었는데, eCrime Solutions 팀에서는 독립적으로 400 억 건의 데이터를 확보하고 자체 시스템 로직(logics)을 개발 구현해 시스템 오류에 대한 검증과 더불어 원인과 책임 여부를 규명했다. 고객으로부터 유의미한 성과로 인정받아 매년 정기적으로 해당 업무를 수행하게 되는 실적을 세우기도 했다.

기업 내 영업기밀이나 산업기술 유출의 경우 그 피해액이 연간 50 조 원에 달한다는 연구결과도 있으나 이에 대한 소송과 피해 보상은 미비한 것이 현실이다. 사이버보험 가입이 의무화되면서 보험상품의 설계 및 평가, 납입금 및 보상금의 규모, 책임 여부의 증명 등에서 많은 이슈가 발생하고 있어, 여러 사건사고에 대한 독립적인 조사와 정확한 증거자료를 확보하기 위한 기업의 요구사항이 더욱 커질 것으로 예상하고 있다.

'국내 No.1 eCrime 해결사'로 성장의 목표



<eCrime solutions 팀에서 끼와 열정이 넘치는 멤버들이 인터뷰를 위해 한자리에 모였다.

사진 왼쪽부터 최기훈 차장, 김미정 과장, 이창성 부장, 성승창 차장, 유경민 과장>

앞서 언급한 바와 같이 eCrime Solutions 팀은 국내 최대 규모의 포렌식랩을 보유하고 있다. 물리적, 논리적으로 철저하게 분리된 연구실에서는 독립된 분석 인프라를 운영하고 있으며, 20 여 대의 서버와 국내외 포렌식 전문 솔루션(FTK, EnCase, MD-Nex 등) 15 종 이상을 적극 활용하고 있다. 게다가, 정형 및 비정형 등 모든 데이터의 유형의 수집과 400 억 건이 넘는 데이터 분석 및 처리가 가능한 국내 몇 안 되는 Top 레벨 수준의 포렌식랩까지 운영하고 있다

기업의 사건 사고에 관한 조사는 그 부정적 이미지로 인해 외부에 공개되거나 제 3 자에게 업무를 위탁하기가 어려운 것이 현실이다.

하지만 eCrime Solutions 팀은 고객의 비밀을 유지하면서, 객관적인 위치해서 조사를 수행하기에 필요한 모든 것을 갖추고 있다고 해도 과언이 아니다. 이렇게 완벽한 인프라와 전문가를 활용하여 고객이 원하는 수준의 신속하고 효율적인 분석, 고객의 신뢰까지 얻어 eCrime solution 팀은 국내 최고 수준으로 성장할 것을 목표로 하고 있다.

글·사진 Brand & Communications 팀



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 264,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2018. For information, contact Deloitte Anjin LLC & Deloitte Consulting LLC