Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.4, Aug. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.4.793

위협 헌팅 개념 정립 및 방어기법 비교분석에 관한 연구

류 호 찬,[1†] 정 익 래[2‡]
[1,2]고려대학교 (대학원생, 교수)

A Study on the Establishment of Threat Hunting Concept and Comparative Analysis of Defense Techniques

Ho Chan Ryu,[1†] Ik Rae Jeong[2‡]
[1,2]Korea University (Graduate student, Professor)

요 약

위협 헌팅은 기존 보안 솔루션의 한계를 극복하기 위한 방어 기법이며, 최근 위협 헌팅에 대한 관심이 높아지고 있다. 위협 헌팅은 시스템 내부에 존재하는 위협을 식별 및 제거하는 기법으로 인식되고 있지만 그 정의가 명확하지 않기 때문에 모의 해킹, 침입 탐지, 침해사고 분석 등 다른 용어들과 혼용이 많이 발생하고 있다. 따라서 본 논문에서는 보고서 및 논문에서 발췌한 위협 헌팅의 정의를 비교 분석하여 그 의미를 명확히 하고 방어기법을 비교분석한다.

ABSTRACT

Recently, there has been a growing interest in threat hunting presented to overcome the limitations of existing security solutions. Threat hunting is generally recognized as a technique for identifying and eliminating threats that exit inside the system. But, the definition is not clear, so there is confusion in terms with penetration testing, intrusion detection, and incident analysis. Therefore, in this paper, compare and analyze the definitions of threat hunting extracted from reports and papers to clarify their implications and compare with defense techniques.

Keywords: Threat hunting, Security solution, Penetrations testing, Intrusion detection, Incident analysis

I. 서 론

사이버 공간에서 공격 방법은 고도화 되고 있으며, 공격자는 목표 달성을 위해 가능한 모든 방법을 사용한다. 이에 반해 방어자는 모든 외부와의 접점을 보호해야하며, 알려진 취약점 및 공격 방법에 대해서만 방어가 가능하다. 이러한 이유로 사이버 수단은 공격자에게 유리한 비대칭 전력으로 명시된다[1].

따라서 방어자는 취약점 패치, IP기반 접근통제, 악성코드 탐지 등 내부 자산 보호에 필요한 일련의 활동을 수행하는 한편, 시스템 내에 미처 탐지하지 못한 위협이 존재할 가능성을 고려해야 한다. FireEye에서 발간한 보고서에서는 보안 평가팀이 12개월에 걸쳐 모의 테스트한 결과 53%의 공격이 탐지되지 않고 시스템 내부로 성공적으로 침투했으며, 보안 솔루션에 의해 완전히 차단된 공격은 33%에 불과했다고 밝혔다.[2]. 하지만 외부와 내부 네트워크 경계에서 모든 위협을 차단하지 못하더라도 시스템 내부의 위협을 조기 식별하여 제거한다면 피해를 최소화할 수 있다.

아래 Fig.1.은 MITRE에서 제안한 Cyber Kill-Chain이다. 4단계 '악용(exploitation)' 부터의 과정은 피해 시스템 내부에서 일어나며, 방어자는 마지막 단계인 '목표 달성(actions on objectives)'까지 도달하지 못하도록 시스템 내부에 존재하는 위협을 식별하고 제거해야 한다.

Received(04. 21. 2021), Modified(1st: 05. 12. 2021, 2nd: 06. 09. 2021), Accepted(06. 09. 2021)
† 주저자, ryuhochan@korea.ac.kr
‡ 교신저자, irjeong@korea.ac.kr(Corresponding author)

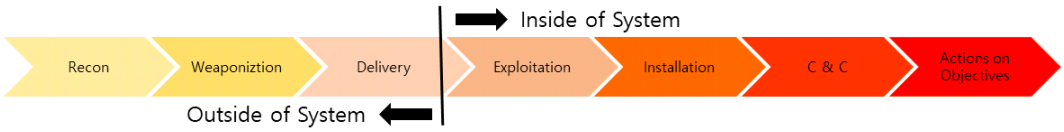

Fig. 1. Cyber Kill-Chain 7 Steps

실제 침해사고가 발생한 사례를 살펴보면 내부 시스템에 존재하는 위협 제거의 필요성을 알 수 있다. FireEye에서 발간한 'M-Trend 2020' 보고서에 따르면 공격자가 탐지되기 전 까지 피해 시스템에 존재하는 일수의 중앙값은 56일 이다[3]. 일반적으로 공격자는 56일동안 시스템 내부에서 활동한다는 의미이고 그 활동의 흔적, 즉 침해지표가 남게 된다. 이렇게 공격자가 시스템 내부에 남긴 침해지표를 찾아서 공격자의 전략, 기술, 절차(TTPs)를 밝혀내는 방어기법이 바로 위협 헌팅이다.

최근 기존 보안 시스템의 한계를 극복하기 위해 많은 조직에서 위협 헌팅의 도입을 추진하고 있다. SANS의 '2020 Threat Hunting survey'에 따르면 현재 글로벌 조직의 65%에서 이미 위협 헌팅을 도입하였으며, 29%는 1년 내로 도입을 계획 하고 있다[4]. 이처럼 보안 실무에서는 위협 헌팅의 중요성을 인식하고 적용하고 있지만 여전히 위협 헌팅의 정의가 명확히 정립되지 않아 모의해킹, 침입 탐지, 침해사고 분석 등 다른 용어와 혼용이 발생한다. 이러한 필요성에 따라 본 논문은 2장에서는 위협 헌팅 개념을 포함한 보고서 및 논문의 주요 내용 및 한계점을 제시한다. 그리고 3장에서는 각 자료에서 발췌한 위협 헌팅의 정의를 비교분석하여 그 의미를 명확히 한다.

II. 관련 연구

위협 헌팅은 기존 보안 시스템의 한계를 보완하기 위해 만들어진 개념으로 학술논문보다는 보안 전문기업의 보고서가 먼저 발간되기 시작했고, 최근에는 다양한 IT기술과 위협 헌팅을 접목시킨 연구 논문이 발간되고 있다. 본 단락에서는 위협 헌팅의 개념을 포함한 보고서 및 논문의 주요 내용을 소개하고 한계점을 제시한다.

미국의 사이버보안 기업 SANS에서는 2016년부터 2021년 현재까지 매년 위협 헌팅을 도입한 조직의 위협 헌팅 수행 수준, 수행 주기, 인력 운영, 한계점 등에 대한 보고서를 발간하고 있다[5 ~ 9]. 특히 2016년 보고서 'Threat Hunting : Open Season on the Adversary' 에서는 위협 헌팅을 '내부 네트워크에서 사이버 공격자를 능동적으로 추적하여 가능한 빠르게 제거하는 행위'로 정의하고 있다. 하지만 위협 헌팅을 직접 수행하는 담당자에게 트렌드 정보를 제공하기 위한 목적으로 작성된 보고서이므로 위협 헌팅의 개념에 대한 세부적인 설명이 미흡하다.

또 다른 미국의 사이버 보안 기업 Sqrrl에서도 2017년부터 위협 헌팅 가이드 보고서를 발간하고 있다[10 ~ 12]. 2018년에 발간된 Sqrrl의 보고서 'A Framework for Cyber Threat Hunting'는 위협 헌팅의 개념 설명 및 성숙도 모델 제시, 프로세스에 대한 전반적인 내용을 포함한다. 그리고 위협 헌팅을 '기존 보안 솔루션을 우회하는 고도화된 위협을 탐지 및 제거하기 위하여 능동적이고 반복적으로 네트워크를 탐색하는 프로세스'로 정의하고 있다.

SANS Institute와 Sqrrl의 보고서에서 제시된 위협 헌팅 정의는 서로 비교분석하여 그 의미를 명확히 할 수 있을 것이다. 그 외에 위협 헌팅을 IT기술과 접목시킨 연구 논문이 있다. Hamed Haddad Pajouh외 4인은 '18년 'A Deep Neural Network Based Approach for Internet of Things Malware Threat Hunting' 논문에서 DRNN 딥러닝 기술을 활용하여 악성코드를 탐지하는 방법을 제안하였다[13]. 논문 제목에는 위협 헌팅이라는 단어를 사용하였지만 논문의 내용은 악성코드 탐지에 관한 것이다. 시스템 내부에 존재하는 악성코드를 탐지하여 위협을 제거하는 관점에서 좁은 의미의 위협 헌팅으로 생각할 수 있지만, 위협 헌팅에 대한 개념이 정립되어 있지 않은 상태에서 잘못 사용된 예시라고 볼 수 있다.

III. 위협 헌팅 정의 비교 분석

3.1 위협 헌팅 정의

현재까지 각종 보고서 및 논문에서 제시한 위협 헌팅의 정의를 정리하고 공통점과 차이점을 분석하면 그 의미를 명확히 할 수 있을 것이다.

현재까지 보고서 및 논문에 제시된 위협 헌팅의 정의는 아래 Table 1.과 같다. 위협 헌팅 정의에서 공통적으로 나타나는 표현은 네트워크(또는 기타 시스템)를 탐색하여 위협(또는 공격자)을 탐지한다는 표현이다. 기타 내용은 자료의 표현 정도에 따라 차이가 있다. 결국 위협 헌팅의 두 가지 요소, 즉 위협 헌팅 대상과 목표는 모든 자료에서 일치함을 알 수 있다.

좁은 의미에서 위협 헌팅은 '내부 시스템을 대상으로 사이버 위협을 찾고 제거하는 활동' 으로 정의내릴 수 있을 것이다. 그 외에 위협 헌팅을 정의하는 표현들에는 '기존의 보안 솔루션을 우회하는 위협(threats that evade existing security solutions)', '능동적이고 반복적인 프로세스(proactive and iterative process)', '자동화(automation)' 및 '분석가'(human analysis)' 등이 있다. 이 표현들은 위협 헌팅을 수행하는 조직의 상황에 맞게 적용될 수 있다.

Table 1. Definition of Threat Hunting

Reference	Definition
SANS Institue, 'Threat Hunting:Open Season on the Adversary' (2016)	Act of aggressively tracking and eliminating cyber adversaries from your network as early as possible.
Md Nazmus Sakib Miazi, 'The Design of Cyber Threat Hunting Games : A Case Study' (2017)[14]	Finding threats and anomalies within the organization's networks and systems with monitoring and analyzing logs promptly both by automation and human analysis
SANS Institute, 'Threata Hunting Survey Result' (2018)	A focused and iterative approach to searching out, identifying and understanding adversaries who have entered the defender's networks
Sqrrl, 'A Framework for Cyber Threat Hunting' (2018)	Process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions
Sqrrl, 'Hunt Evil : Your Practical Guide to Threat Hunting' (2020)	Human-driven, proactive and iterative search through networks, endpoints, or datasets in order to detect malicious, suspicious, or risky activities that have evaded detection by existing automated tools
Danish Javeed, 'An Efficient Approach of Threat Hunting Using Memory Forensics' (2020)[15]	Practice of proactively searching around the networks or datasets for the detection and responding to progressive cyber threats that escape outdated rule or signature-based security panels

Table 2. Object and Purpose of Threat Hunting

Object	Purpose
Organization's System	Finding and eliminating of cyber threats

3.1.1 기존의 보안 솔루션을 우회하는 위협

위협 헌팅은 이미 내부 시스템에 존재하는 위협을 찾는 방어기법이므로 해당 위협은 기존에 운영되는 보안 솔루션을 우회하였다고 볼 수 있다. MITRE ATT&CK에서 제시하는 Techniques는 총 343개이며, 여기서 중복을 제거한 266개 중 단독으로 수행되었을 때 악성행위로 식별할 수 없는 Techniques가 220개로 전체의 83%이며, 명시적인 악성행위로 식별되어 CAPEC(Common Attack Pattern Enumeeration and Classification) ID가 부여된 것은 43개로 전체의 16%에 불과하다[16]. 물론 조직의 규모와 보안 시스템의 수준에 따라 그 정도의 차이는 존재하지만 외

부와 내부 시스템의 경계에서 모든 위협을 탐지하고 차단하는 것은 불가능하다. 경계에서 차단되지 않고 내부 시스템에 존재하는 위협을 찾아서 제거하는 방어 기법이 위협 헌팅이며, 반드시 필요한 과정이다.

3.1.2 능동적이고 반복적인 프로세스

기존의 방어기법은 알려진 공격 패턴의 탐지 규칙을 적용시키는 형태이다. 따라서 수동적 형태를 띠고 있으며 사후 대처의 성격이 강하다고 볼 수 있다. 이에 비해 위협 헌팅은 시스템 내부에 존재하는 위협을 제거함으로써 피해 발생을 최소화 시킬 수 있다는 측면에서 능동적인 성격을 띠고 있다. 또한 내부 시스템에 대하여 반복적으로 위협 헌팅을 수행함으로써 내부 위협을 탐지하고 제거할 확률이 올라간다. 위협 헌팅 수행 주기를 정하여 반복 수행할 수 있는데, 수행 주기를 정하는 방법은 크게 3가지로 나뉜다.

첫째는 자동화하여 지속적으로 수행하는 것, 둘째는 1주에 한 번 등 일정 주기를 정해서 수행하는 것, 마지막으로 공격 상황이 식별될 때 수행하는 것이다. 따라서 자산의 중요도 및 위협 헌팅 수행 인력 현황에 맞게 주기를 정하여 합리적으로 위협 헌팅을 수행할 수 있다.

3.1.3 자동화 및 분석가

위협 헌팅은 수행자(헌터)의 역량에 의존적인 성격이 있다. 내부 시스템의 특성과 외부 위협 정보를 바탕으로 위협 헌팅의 방향성을 설정해야하기 때문이다. 하지만 위협 헌팅의 성숙도 단계가 올라갈수록 위협 헌팅 프로세스의 자동화가 구현될 수 있다. 아래 Fig.2.는 2018년 Sqrrl보고서 'Framework for Cyber Threat Hunting'에서 제시된 위협 헌팅 성숙도 모델이다. 초기 단계부터 리딩 단계까지 위협 헌팅의 성숙도 모델을 제시한다. 초기 단계(LEVEL 1)에서는 보안 솔루션의 경고 기능 등 기초적인 수준만 자동화 되어 운영되지만, 성숙도 단계가 올라갈수록 고수준의 데이터 수집 및 분석이 자동으로 이루어진다(LEVEL 4). 위협 헌팅의 성숙도 단계는 조직의 상황과 필요에 맞게 발전시켜 나가야 한다. 보호해야 할 내부 자산이 많은 데이터센터와같은 조직의 경우 일정 수준 이상의 정보 수집 및 분석 자동화 시스템이 구축되지 않으면 위협 헌팅을 수행하기가 어려울 수 있다. 하지만 내부 자산의 수가 적다면 위협 헌팅 담당자가 직접 데이터를 수집 및 분석 가능하므로 자동화에 큰 노력을 투자할 필요가 없다. 이처럼 조직의 자산 규모에 맞게 수행 방법을 조정하여 합리적으로 위협 헌팅을 수행할 수 있다.

3.2 방어기법 비교

위협 헌팅의 개념을 명확히 하기 위해 다른 방어기법과 비교하였다. 비교 대상은 [14] 등에서 지속적으로 언급 되고 있는 3가지 방어기법인 모의 해킹(penetration testing), 침입 탐지(Intrusion

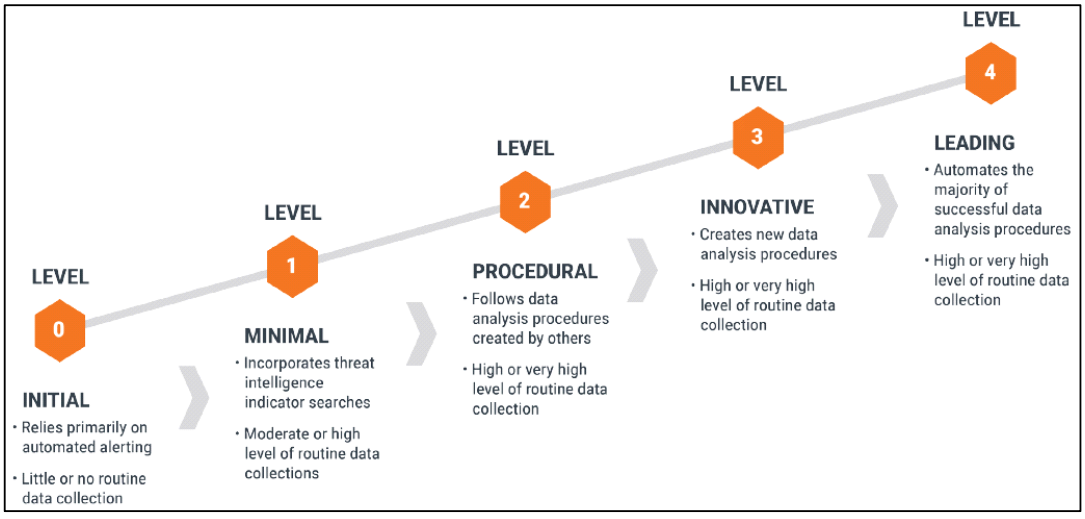

Fig. 2. Threat Hunting Maturity Model

Table 3. Threat hunting vs Other terms

	Threat hunting	Penetration testing	Intrusion detection	Incident analysis
Objective	Organization's system	Organization's system	Boundary between inside and outside of system	Organization's system
Purpose	Elimination of internal threats	Evaluation of security	Intrusion detection	Evidence gathering and analysis
Timing	During attacks	Before attacks	During attacks	After attacks
Tools	Data collection / analysis tools	Hacking tools	Intrusion detection solutions	Data collection / analysis tools

detection), 침해사고 분석(incidentanalysis)이다. [14]에서는 해당 방어기법의 기술적 차이를 위주로 비교하였지만 본 논문에서는 Table 3.과 같이 대상(obejctive), 목적(purpose), 수행 시기(timing) 및 사용 도구(tools)를 비교하여 각각의 의미를 명확히 하고 위협 헌팅과의 관계를 파악한다.

3.2.1 위협 헌팅 vs 모의 해킹

모의 해킹은 위협 헌팅과 가장 많이 비교되는 방어기법이다. 두 기법 모두 내부 시스템을 대상으로 수행된다는 공통점이 있지만 그 목적과 수행 시기 및 사용 도구에 차이가 있다. 모의 해킹은 시스템에 대한 공격이 발생하기 전에 수행하며, 공격 도구를 사용한 승인된 공격을 통해 보안성을 평가하여 실제 공격을 예방하고 위험수준을 낮추는 것이 그 목적이다. 하지만 위협 헌팅은 데이터 수집, 분석 도구를 사용하며 시스템에 대한 공격의 진행을 가정한 상태에서 수행된다. 그리고 내부에 존재하는 위협을 제거하여 피해를 최소화 시키는 것이 그 목적이다. 위협 헌팅을 통해 내부에 존재하는 위협을 식별했다면 이후 모의해킹을 통해 가능한 내부 침투 경로를 확인해야 한다.

3.2.2 위협 헌팅 vs 침입 탐지

침입 탐지는 위협 헌팅과 동일하게 공격 진행 중에 수행되는 방어기법이지만 그 대상과 목적 및 사용 도구에 차이가 있다. 침입 탐지는 보안 솔루션에 의존하며 시스템의 외부 내부 네트워크 경계를 대상으로 악성 트래픽을 차단하는데 그 목적이 있다. 하지만 위협 헌팅은 데이터 수집, 분석 도구를 사용하여 시스템 내부에 존재하는 침해지표를 찾고 위협을 제거하는 것이 그 목적이다. 자동화된 침입 탐지 도구를 사용하여 일반적인 위협을 차단하고 이를 우회하는 고도화된 위협에 대하여 위협 헌팅을 수행하는 것이 효과적이다.

3.2.3 위협 헌팅 vs 침해사고 분석

사고 분석은 내부 시스템 데이터를 수집하고 분석한다는 측면에서 위협 헌팅과 유사한 성격이 있다. 하지만 수행 시기와 목적에는 분명한 차이가 있다. 사고 분석은 공격이 발생하여 피해사실을 인지한 후 수행되며 공격의 증거 확보 및 원인 분석에 그 목적이 있다. 하지만 위협 헌팅은 공격 진행을 가정한 상태에서 수행되며 내부에 존재하는 위협 제거를 통해 피해를 최소화하는 것이 목적이다. 침해사고 분석 시 확인한 침해지표 및 취약점을 이후 위협 헌팅 진행 시 참고한다면 효과적인 위협 헌팅 프로세스를 개발할 수 있다.

위협 헌팅, 모의 해킹, 침입 탐지, 사고 분석은 서로 상호보완적인 관계이므로 조직의 보안 시스템을 운영하면서 적절하게 수행되어야 한다. 시스템 초기 단계에 모의 해킹을 통해 침투 가능한 경로를 미리 파악하여 시스템 보안 수준을 향상시킬 수 있고 침입 탐지 솔루션을 구축하여 대다수 패턴화된 공격을 자동 차단할 수 있다. 하지만 기존의 보안 시스템을 우회하여 시스템 내부에 존재하는 위협을 탐지하고 제거하기 위해서는 주기적인 위협 헌팅이 반드시 필요

하다.

IV. 결 론

본 논문에서는 기존 보고서 및 논문에서 사용된 위협 헌팅의 정의를 정리하고 다른 방어기법과 비교분석하여 그 의미를 명확히 하였다.

모든 자료에서 공통적으로 나타나는 위협 헌팅의 정의는 '내부 시스템을 대상으로 위협을 찾고 제거하는 활동' 이다. 또한 조직의 규모 및 인력 상황에 따라 일정 주기를 가지고 반복하여 위협 헌팅 효과를 증대시키거나 데이터 수집 및 분석을 자동화시킴으로써 위협 헌팅 수행 범위를 확장시킬 수 있다.

그리고 위협 헌팅과 혼용되어 혼란을 초래하는 대표적인 방어기법들에 대하여 대상, 목적, 수행 시기 및 사용 도구를 기준으로 비교분석하고 상호보완적으로 적용할 수 있는 방법을 제시하였다.

References

[1] Dae-Sung Lee, "Analysis and prospect of North Korea's Cyber threat," *Convergence Security Journal*, 16(5), pp. 11-16, Sep. 2016

[2] FireEye, Inc., "SECURITY EFFECT--IVENESS REPORT 2020," FIREEYE MANDIANT, 2020

[3] FireEye, Inc., "M-Trend 2020," *FIREEYE MANDIANT SERVICES / SPECIAL REPORT,* 2020

[4] Mathias Fuchs, "Is Your Threat Hunting Working? A New SANS Survey for 2020," *SANS Institute Information Reading Room*, 2020

[5] Eric Cole, "Threat Hunting: Open Season on the Adversary," *SANS Institute Information Reading Room,* 2016.

[6] Rob Lee, "The Hunter Strikes Back: The SANS 2017 Threat Hunting SSurvey," *SANS Institute Information Reading Room,* 2017.

[7] Robert M. Lee, "SANS 2018 Threat Hunting Survey Result," *SANS Institute Information Reading Room,* 2018.

[8] Mathias Fuchs, "SANS 2019 Threat Hunting Survey: The Differing Needs of New and Experienced Hunters," *SANS Institute Information Reading Room,* 2019.

[9] Dan Gunter, "A Practical Model for Conducting Cyber Threat Hunting," *SANS Institute Information Reading Room,* 2021.

[10] Dannly Akacki, "HUNTPEDIA : Your Threat Hunting Knowledge Compendium," Sqrrl, 2017.

[11] Sqrrl, Inc, "A Framework for Cyber Threat Hunting," Sqrrl, 2018.

[12] Sqrrl, Inc, "Hunt Evil : Your Practical Guide to Threat Hutning," Sqrrl, 2019.

[13] HaddadPajouh, H., "A Deep Recurrent Neural Network Based Approach for Internet of Things Malware Threat Hunting," *Future Generation Computer System*, Vol. 85, pp. 88-96, Aug, 2018.

[14] Nazmus Sakib Miazi, "The Design of Cyber Threat Hunting Games: A Case Study," *International Conference on Computer Communication and Networks*, Vol. 26, pp. 1-6, July, 2017.

[15] Danish Javeed, "An Efficient Approach of Threat Hunting Using Memory Forensics," *International Journal of Computer Networks and Communication Security*, Vol. 8, no.5, pp. 37-45, May, 2020.

[16] Hyukjun Kim, "TTP response based ATT&CK Netowrk," KISA Cyber Threat Report, 4th, 2020.

〈저자소개〉

류 호 찬 (Ho Chan Ryu) 정회원
2016년 2월: 고려대학교 사이버국방학과 졸업
2017년 9월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 IDC보안, 위협 헌팅, 인공지능, 개인정보보안

정 익 래 (Ik Rae Jeong) 종신회원
1998년 2월: 고려대학교 전산학과 졸업
2000년 2월: 고려대학교 전산학과 석사
2004년 8월: 고려대학교 정보보호학과 박사
2006년 3월~2008년 2월: 한국전자통신연구원 암호기술연구팀 선임연구원
2008년 3월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 암호 이론, 프라이버시 향상 기술 (PET), 생체인증, 블록체인보안