About

written by Mert SARICA | 20 November 2009

About This Blog

In 2009, I established my blog with the motto, “Knowledge is power and grows as it is shared”. Since its inception, I have featured the results of over 200 cybersecurity researches that I have conducted to date.

Until the end of 2022, I published my articles exclusively in Turkish. However, as of 2023, I have begun to publish my articles in both English and Turkish. Furthermore, I have also made available translations of both my recent articles as well as my most widely read articles in English. (If you come across any older articles in Turkish, you can utilize the translation feature at the bottom of each page.)

I hope that the research and analysis presented in these articles will prove valuable to those seeking to improve their knowledge and expertise in the field of cybersecurity.

About Me

Mert is a well-known and respected Cyber Security Researcher, Speaker and Blogger. He has been living and pursuing his career in the United States with an Alien of Extraordinary Ability visa (EB-1A), an employment-based green card, since October 2022.

As of February 2023, Mert has been working at SOCRadar® Extended Threat Intelligence as the Head of Security Research & Operations. SOCRadar is a cybersecurity company committed to democratizing threat intelligence and providing superior cybersecurity solutions to thousands of companies in hundreds of countries. SOCRadar’s mission is to provide organizations of all sizes with the tools to counter cyber threats.

In his current position, Mert has been advising the CEO on strategic decisions that align with the company’s mission, objectives, and overall goals.

He has often overseen strategic initiatives by working closely with various departments, such as product development, sales, and marketing. Also, he has been managing the day-to-day operations of the Security Analyst, Support, and

Professional Services teams to ensure efficiency, quality, service, and cost-effective management of resources.

In addition, he has been driving innovation across the product by promoting new ideas and features.

Besides that, he has been managing, mentoring, and supporting a cadre of threat researchers, threat hunters, security analysts, and technical content writers who research cyber threats, vulnerabilities, and trends.

From October 2020 to September 2022, Mert demonstrated his expertise as an Executive Vice President / CISO of IT Security & Risk Management Group which incorporates Cyber Defense Center, Cyber Security Technologies, Cyber Security Architecture, Information Security & Risk Management teams (40 HCs) at Intertech. Intertech is an Information Technology subsidiary of DenizBank, owned by Emirates NBD

From January 2018 to September 2020 as the Vice President, Mert was responsible for the management of Akbank‘s Cyber Defence Center (CDC) which incorporates Vulnerability Management, Threat Detection, Threat Response & Intel, and Security Engineering teams. (26 HCs)

From 2007 to 2017 Mert was responsible for performing and managing penetration tests, malware analysis, security incident detection, and response as a Technical Lead in the Threat & Vulnerability Management team at IBTech. (Information Technology subsidiary of QNB Finansbank)

From 2014 – 2016 Mert instructed Malware Analysis course in Cyber Security Graduate Program at Bahcesehir University.

In 2003 Mert’s career journey began by discovering a security vulnerability on the e-portal web application of the Yeditepe University where he was studying at that time. After sharing his findings with the executives of the university, he was awarded an achievement grant and recruited as an Ethical Hacker. Mert graduated from Yeditepe University, Information Systems and Technologies in 2006 and Yeditepe University, Master of Business Administration program in 2010.

From the beginning of 2011, Mert spoke at more than 30 technical cyber security conferences. In addition, he was invited as a guest speaker to more than 40 universities to share his cyber security career journey and his profession “Ethical Hacker” to the students as a role model.

For more information about his professional background, you may visit his LinkedIn profile.

Certifications
2020 – CCISO (Certified Chief Information Security Officer)
2013 – CEREA (Certified Expert Reverse Engineering Analyst)
2010 – CREA (Certified Reverse Engineering Analyst)
2009 – OPST (OSSTMM Professional Security Tester)
2009 – OSCP (Offensive Security Certified Professional)
2007 – CISSP (Certified Information Systems Security Professional)
2006 – SSCP (Systems Security Certified Practitioner)

Trainings
2021 – Cyber Threat Intelligence (SANS – FOR 578)
2020 – Certified Chief Information Security Officer (EC-Council)
2020 – Risk Management Approach & Practices (EC-Council)
2020 – Certifed Project Manager (EC-Council)
2020 – SIEM with Tactical Analytics (SANS – SEC 555)
2020 – Blue Team Fundamentals: Security Operations and Analysis (SANS – SEC 450)
2019 – Security Strategic Planning, Policy, and Leadership (SANS – MGT 514)
2018 – The Security Automation Lab (Black Hat USA 2018)
2017 – Advanced Digital Forensics, Incident Response, and Threat Hunting (SANS – FOR 508)
2016 – Hardware Hacking With Hardsploit Framework (Black Hat USA 2016)
2015 – Exploit Laboratory: Black Belt (Black Hat USA 2015)
2014 – Advanced Penetration Testing, Exploits, and Ethical Hacking (SANS – SEC 660)
2013 – Advanced Reverse Engineering Malware (InfoSec Institute)
2012 – Reverse-Engineering Malware (SANS – FOR 610)
2011 – Computer Forensic Investigations – Windows In-Depth (SANS – FOR 408)
2010 – Reverse Engineering: Malware, Binary Analysis and Software Vulnerabilities (InfoSec Institute)
2009 – OSSTMM Professional Security Tester (ISECOM – OPST)
2009 – Pentesting with BackTrack (Offensive Security – OSCP)
2008 – Oracle Anti Hacker Training (Red-Database-Security)
2007 – ISO 27001 Lead Auditor (BSI)
2006 – ISO 27001 Implementation of Information Security Management (BSI)
2005 – Certified Ethical Hacker (EC-Council)

Presentations

2023 – Why You Should Leave Your Smart Grill Unplugged ? (BSidesNoVA Conference)

2019 – Sandbox Detection (NOPcon Hacker Conference)

2019 – Backdoor Hunt (IstSec Information Security Conference)

2016 – 2017 Hunting Hackers with Custom Deception System – (Bilisim Zirvesi, Istanbul & Cyprus Cyber Security Conferences)

2016 – Malicious JavaScript Analysis – (Netsec)

2016 – Being a Penetration Tester and Career – (Cyber Security Winter Camp)

2015 – Homemade Cryptolocker Prevention Tool (CryptoKiller) – (IstSec Information Security Conference)

2015 – Cyber Attacks & Defence (International Internal Audit Conference (TIDE))

2015 – Firmware Analysis – (Hacktrick Information Security Conference)

2014 – Firmware Analysis – (IstSec Information Security Conference)

2013 – Anti Malware Analysis – (IstSec Information Security Conference)

2013 – Offensive Malware Analysis – (Euroforensics, Cyprus, IstSec Information Security Conference)

2012 – Importance Of Penetration Testing – (Netsec)

2012 – Android Mobile App Pentest – (NOPcon)

2012 – Android Malware Analysis – (Euroforensics)

2011 – 2019 How to Become an Ethical Hacker / Penetration Tester – (Universities)

Blog Hakkında

2009 yılında “Bilgi güçtür ve paylaşıldıkça artar!” mottosu ile hayata geçirdiğim blogumda bugüne kadar gerçekleştirmiş olduğum 200’den fazla siber güvenlik araştırmasının çıktılarına yer verdim.

Emek, zaman ve kaynak ayırarak yaptığım araştırmalar sonucunda yazdığım bu makalelerin, siber güvenlik alanında kendini geliştirmek isteyenler için faydalı olması dileklerimle…

Hakkımda

Mert SARICA, alanında tanınmış ve saygın bir Siber Güvenlik Araştırmacısı, Konuşmacı ve Blogger’dır. 2022 yılının Ekim ayından bu yana kariyerini EB-1A vizesi (Yeşil Kart) ile Amerika Birleşik Devletleri’nde sürdürmektedir.

SARICA, 2023 yılının Şubat ayı itibariyle SOCRadar Siber Tehdit İstihbaratı

firmasında Güvenlik Araştırmaları ve Operasyonları Başkanı olarak görev yapmaktadır. SOCRadar, siber tehdit istihbaratı alanında yüzlerce ülkede binlerce şirkete üst düzey siber güvenlik çözümleri sunan ve misyonu gereği her büyüklükteki kuruluşa siber tehditlere karşı koymak için ihtiyaç duydukları araçları sağlayan bir siber güvenlik şirketidir.

SARICA şu anki pozisyonunda, şirketin misyonu ve hedefleriyle uyumlu stratejik planlar ve stratejik kararlar konusunda CEO'ya danışmanlık yapmakta ve ayrıca stratejik girişimlerin şirketin genel hedefleriyle uyumlu olmasını sağlamaktadır.

Buna ek olarak, yeni fikirleri ve özellikleri teşvik ederek ürün genelinde inovasyonu desteklemekte ve genellikle ürün geliştirme, satış ve pazarlama gibi çeşitli departmanlarla yakın çalışarak stratejik girişimlerin yürütülmesini denetlemektedir.

Bunun yanı sıra, siber tehditler, güvenlik açıkları ve trendler hakkında derinlemesine güvenlik araştırması yapan bir tehdit araştırmacıları kadrosuna liderlik etmekte, mentorluk yapmakta ve desteklemekte ve ayrıca verimlilik, kalite, hizmet ve kaynakların uygun maliyetli yönetimini sağlamak için Güvenlik Analisti ve Destek ekiplerinin günlük operasyonlarını denetlemektedir.

Ekim 2020 – Eylül 2022 yıllarında DenizBank'ın iştiraki olan Intertech firmasında BT Güvenlik ve Risk Yönetimi Grubu'ndan sorumlu Genel Müdür Yardımcısı / CISO olarak görev yapmıştır.

Ocak 2018 – Eylül 2020 yıllarında ise Siber Saldırı Tespit ve Müdahale, Siber Güvenlik Mühendisliği, Siber Tehdit İstihbaratı ve Zafiyet Yönetimi Ekipleri'nden sorumlu Müdür olarak Akbank Siber Güvenlik Merkezi (SGM)'nde görev yapmıştır.

SARICA, 2007 – 2017 yıllarında QNB Finansbank'ın bilgi teknolojileri iştiraki olan IBTech firmasında sızma testi, zararlı yazılım analizi ve bilgisayar olayları tespit ve müdahale alanlarından sorumlu olan Tehdit ve Zafiyet Yönetimi Ekibi'nde Teknik Lider olarak görev yapmıştır.

Kurumsal iş hayatının yanı sıra akademik kariyeri 2014 – 2016 yıllarında Bahçeşehir Üniversitesi, Siber Güvenlik Yüksek Lisans Programı'nda öğretim görevlisi olarak verdiği "Zararlı Yazılım Analizi Eğitimleri" ile devam etmiştir.

Yüksek lisansını, 2010 yılında “Yeditepe Üniversitesi İngilizce İşletme (MBA) Programı” üzerine yapan SARICA’nın kariyer hayatının başlangıcı, lisans eğitimini tamamladığı üniversite olan Yeditepe Üniversitesi, Bilişim Sistemleri ve Teknolojileri Bölümü‘nde olmuştur.

SARICA, lisans eğitimine devam ettiği yıllarda Yeditepe Üniversitesi’nin elektronik ders seçme uygulaması üzerinde keşfetmiş olduğu kritik güvenlik zafiyetini üniversite yönetimi ile paylaşmış; bu paylaşım üzerine üniversite yönetimi tarafından başarı bursu ile ödüllendirilmiş ve “Etik Hacker” olarak işe alınmıştır.

2011 yılından bu yana 30’dan fazla siber güvenlik etkinliğine konuşmacı olarak davet edilmiş, Türkiye genelinde 40’a yakın üniversite etkinliğinde ise öğrencilere “Etik Hacker” mesleğini tanıtmaya yönelik sunumlar gerçekleştirmiştir.

Sertifikalar
2020 – CCISO (Certified Chief Information Security Officer)
2013 – CEREA (Certified Expert Reverse Engineering Analyst)
2010 – CREA (Certified Reverse Engineering Analyst)
2009 – OPST (OSSTMM Professional Security Tester)
2009 – OSCP (Offensive Security Certified Professional)
2007 – CISSP (Certified Information Systems Security Professional)
2006 – SSCP (Systems Security Certified Practitioner)

Eğitimler
2021 – Cyber Threat Intelligence (SANS – FOR 578)
2020 – Certified Chief Information Security Officer (EC-Council)
2020 – Risk Management Approach & Practices (EC-Council)
2020 – Certifed Project Manager (EC-Council)
2020 – SIEM with Tactical Analytics (SANS – SEC 555)
2020 – Blue Team Fundamentals: Security Operations and Analysis (SANS – SEC 450)
2019 – Security Strategic Planning, Policy, and Leadership (SANS – MGT 514)
2018 – The Security Automation Lab (Black Hat USA 2018)
2017 – Advanced Digital Forensics, Incident Response, and Threat Hunting (SANS – FOR 508)
2016 – Hardware Hacking With Hardsploit Framework (Black Hat USA 2016)
2015 – Exploit Laboratory: Black Belt (Black Hat USA 2015)
2014 – Advanced Penetration Testing, Exploits, and Ethical Hacking (SANS –

SEC 660)
2013 – Advanced Reverse Engineering Malware (InfoSec Institute)
2012 – Reverse-Engineering Malware (SANS – FOR 610)
2011 – Computer Forensic Investigations – Windows In-Depth (SANS – FOR 408)
2010 – Reverse Engineering: Malware, Binary Analysis and Software Vulnerabilities (InfoSec Institute)
2009 – OSSTMM Professional Security Tester (ISECOM – OPST)
2009 – Pentesting with BackTrack (Offensive Security – OSCP)
2008 – Oracle Anti Hacker Training (Red-Database-Security)
2007 – ISO 27001 Lead Auditor (BSI)
2006 – ISO 27001 Implementation of Information Security Management (BSI)
2005 – Certified Ethical Hacker (EC-Council)

Sunumlar
2023 – Akıllı Izgaramı Nasıl Hackledim ? (BSidesNoVA Conference)
2011 – 2019 Nasıl Etik Hacker Olunur ? (40+ Üniversite)
2019 – Kumhavuzu Tespiti (NOPcon Hacker Conference)
2019 – Arka Kapı Avı (IstSec Information Security Conference)
2016 – 2017 Tuzak Sistem ile Hacker AVI – (Bilisim Zirvesi, Istanbul & Cyprus Cyber Security Conferences)
2016 – Zararlı JavaScript Analizi – (Netsec)
2016 – Sızma Testi Uzmanlığı ve Kariyer (Cyber Security Winter Camp)
2015 – Ev Yapımı CryptoLocker Engelleme Çözümü – (IstSec Information Security Conference)
2015 – Siber Saldırı & Savunma (International Internal Audit Conference (TIDE))
2015 – Donanım Yazılımı Analizi – (Hacktrick Information Security Conference)
2014 – Donanım Yazılımı Analizi – (IstSec Information Security Conference)
2013 – Anti Zararlı Yazılım Analizi – (IstSec Information Security Conference)
2013 – Ofansif Zararlı Yazılım Analizi – (Euroforensics, Cyprus, IstSec Information Security Conference)
2012 – Sızma Testinin Önemi – (Netsec)
2012 – Android Mobil Uygulama Sızma Testi – (NOPcon)
2012 – Android Zararlı Yazılım Analizi – (Euroforensics)