SANS Zero Trust & Deception Solutions Forum

August 28, 2020 | Live Online - Eastern U.S. | SANS Chairperson: Ismael Valenzuela

Sponsored by: Cyberinc Akamai Cyolo

AGENDA

10:00 - 10:30am	**Join Slack Workspace (https://join.slack.com/t/sans-zero-trust-forum/shared_invite/zt-gvddt44k-0K~F_fqZpm_DjWbIvYN2eA) & Virtual Event (https://www.sans.org/webcasts/112770)**
10:30 - 10:50am	**Welcome & Keynote** Traditional methods of cyber defense, like perimeter-based network security, have always emphasized the need of keeping adversaries out of our networks, building a fortress that would stop attackers while allowing secure access to legitimate users. In such a model, trust is typically binary: either the user is authenticated (trusted) or not. Once access is granted to a user, that level of trust is hardly re-evaluated, and when it is, it is usually as a result of an incident, when it is often too late. Although modern client-side attacks have made evident that the old perimeter security model based on moats and castles is clearly insufficient, this architecture is still the most commonly deployed today. With this in mind, back in 2011, Forrester published a report on a new model called Zero Trust, a data-centric approach that promotes a new way to think about cyber threats, one that assumes that the adversary is already on the network, that you have been already compromised. While this model has been known for some time, it seems that Zero Trust has only gained major popularity recently. The increasing use of cloud and the adoption of BYOD (Bring Your Own Device) policies are contributing to the strong appeal that zero-trust architectures have for both commercial and government organizations. Furthermore, the release of the Draft Publication on Zero Trust by NIST in late 2019 guarantees that this will be one of the most discussed topics by the infosec community in 2020. But is Zero Trust just a new marketing buzzword, a simple iteration over the well-known least privilege mindset, or a truly innovative strategy? Is Zero Trust truly attainable? If so, how do you get started and what are some of the tools and technologies that are available to implement it? **Ismael Valenzuela, @aboutsecurity, Forum Chairperson & SANS Instructor**
10:50 - 11:25am	**Zero Trust: How trustworthy is my endpoint?** According to a survey by Security Insiders, nearly 80% of organizations are either looking to or have embraced Zero Trust. Where do you stand? Zero Trust as a concept has existed for decades. The term itself was coined by Forrester in 2010 and in the last couple of years it has become a buzzword of sorts. Forrester defines it as security by design to overcome the gaps in the traditional "trust but verify" models, with the implementation of methods to localize and isolate threats through microcore, micro-segmentation, and deep visibility. With remote working becoming the new normal and cloud applications taking center stage, tools like the browser increasingly acts as an initial point of entry for attackers (including some very recent high-profile attacks). And once they're in, attackers move laterally looking for appropriate targets to maximize their value. With several technologies coming under the umbrella of Zero Trust, is there a good place to start? How does Zero Trust address the ever-morphing threats you see everyday? Can you do something about the plethora of threats that impact your end user and lead to breaches? What are the key considerations to ensure success? **Rajiv Raghunarayan, @raraghun, SVP, Products and Marketing, Cyberinc**
11:25am - 12:00pm	**2020 Vision: Zero Trust Frameworks** Traditional Perimeter Security models have come under pressure in 2020 as they have been challenged by evolving attack techniques and the explosion in remote work. Join Patrick Sullivan from Akamai in a discussion that will explore some of these challenges and share some ideas for leveraging Zero Trust Access models to respond to these changes. **Patrick Sullivan, @Akamai, CTO, Security Strategy, Akamai Technologies**

SANS Zero Trust & Deception Solutions Forum

August 28, 2020 | Live Online - Eastern U.S. | SANS Chairperson: Ismael Valenzuela

Sponsored by: Cyberinc Akamai Cyolo

AGENDA

12:00 - 12:35pm	**The Zero-Trust Journey from Vision to Execution** Today's working environment is smart, connected and complex. Organizations struggle to provide employees and contractors with efficient, fast and secure access, while dealing with security challenges and budget constraints. The zero-trust model aims to ensure no trust is given to any entity inside or outside of the perimeter, at any time and that no transitive trust is allowed. Organizations are required to secure, manage and monitor every device, user, app and network used to access business data. In this session we will discuss why the zero-trust model is the best security model to adopt, especially when preparing your business for 2021. We will de-buzz the term and see how the zero-trust model can benefit any organization, as it is designed to fit specific needs and use cases. We will take you through a zero-trust journey and review how to implement zero-trust to ensure secure connectivity for the following three use cases: • Working from Home (WFH) - securely connecting remote employees, using managed or unmanaged devices to the organization's applications and servers, to ensure business continuity with a remote workforce. • Suppliers/Third Party Access – ensure secure external access of a logistic supplier using an unmanaged device, with explicit real-time approval from someone within the organization, granting specific access. • Privileged Access Management (PAM) – secure access from within the network only, for specific devices, no servers' passwords required, with biometric authentication and recording for supervision. **Almog Apirion, @AlmogAp, CEO and Co-Founder, Cyolo**
12:35 - 12:45pm	**Closing Statement & $125 Gift Card Trivia Winner Announced** **Ismael Valenzuela, @aboutsecurity, Forum Chairperson & SANS Instructor**