

## **Collaborative Discussion 1 – Received Response – Ying Chan**

It is an informative post about preventing brute force attacks and denial of service (DoS) attacks, Michael. Especially pointed out a useful approach, deception-based security.

Deception technology is second only to Zero Trust (ZT) technology in the top listed security tools according to IDG's 2020 Security Priorities Study (IDG, 2020), the majority of security executives has added to their organization since last year. Despite the weakness that needs for in-network deceptions to continuously outsmart extremely complex attackers, as well as the ability for organizations to deploy, manage, renew, and respond to deception warnings. The average time it takes for a corporation to notice a successful network breach is 200 days. Users of deception technology report that they respond to deception-based notifications 12 times faster than they do to other warnings, resulting in significant cost savings for enterprises and it is worth considering. (Naveena, 2021)

The ZT architecture was developed by John Kindervag in 2010 (John, 2010). The concept is to pretend all interfaces and users are untrusted, and all traffic is encrypted. However, the implementation can be painful for the existing organization.

There is no doubt that ZT is a great concept, though it is obvious that just because a device is authenticated does not mean it is not compromised. Deception is more pragmatic in the sense that it does not presume that it will be able to characterize all the endpoints and legitimate data flows. To sum up, the implementation of deception and ZT in parallel could lead to a more effective defence.

### **References:**

IDG (November 19, 2020) 2020 IDG Security Priorities Study. Tools For Marketers. Available from: [https://f.hubspotusercontent40.net/hubfs/1624046/2020\\_Security%20Priorities%20Executive%20Summary\\_final.pdf](https://f.hubspotusercontent40.net/hubfs/1624046/2020_Security%20Priorities%20Executive%20Summary_final.pdf) [Accessed 21 November 2021].

Naveena. (August 05, 2021) Is deception technology a security strategy worth considering?. IT Security. Available from: <https://insights.manageengine.com/it-security/deception-technology/> [Accessed 21 November 2021].

John, K. (September 17, 2010) No More Chewy Centers: Introducing The Zero Trust Model Of Information Security. For Security & Risk Professionals. Available from: <https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf> [Accessed 21 November 2021].