VIEW POINT

DECEPTION: THE CYBERSECURITY STRATEGY THAT YOU NEED

Abstract

Being at an all-time war with the adversaries, the SOCs with their cyber controls need to display the highest form of resilience. Deception-based cyber intelligence, as the primary cybersecurity strategy, is here to outwit the attackers duping them into their own trap. By laying decoys across perimeter, network and endpoints, deception obstructs the occurrence of major cyber events causing the threat actors to expose their tactics, techniques and procedures (TTPs). With the new age cyber solutions disrupting the zone, the deception market is seeing an unwavering growth and is expected to rise high serving major use cases in sectors of Defense, Healthcare, BFSI, etc.

Infosys®
Navigate your next

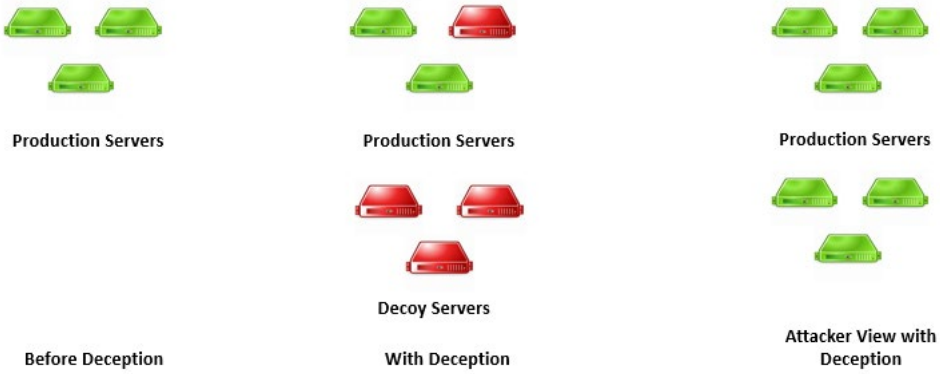
The cybersecurity strategy of an enterprise needs to constantly identify and bolster the chinks in the armor which, when not addressed, can bring down an enterprise like a house of cards, causing immeasurable and irrecoverable damage to resources, assets, and the brand value of the organization.

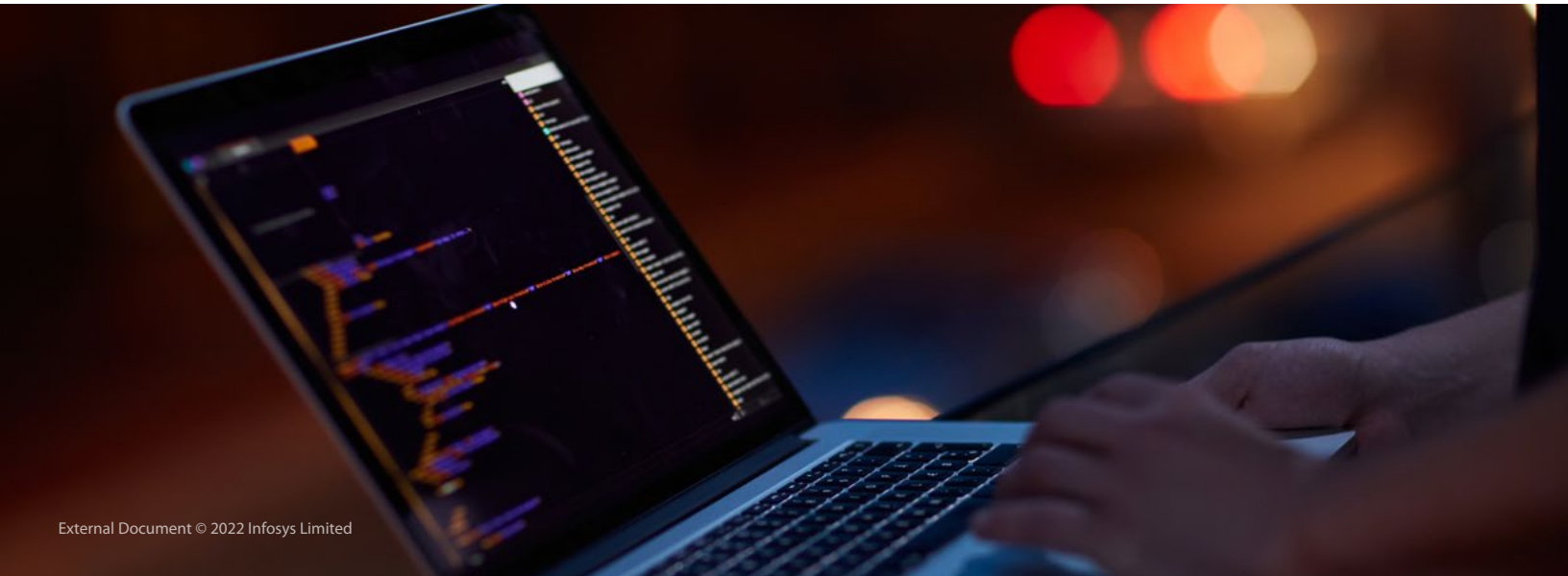
The ongoing pandemic has marked the onset of the digital era and has caused a paradigm shift in the functioning of the IT landscape. Today, technology has become imperative. With the exponential increase in the adoption of innovative technologies and enablement of the remote workforce, the corporations are reimagining and re-evaluating their IT security framework and adhering more to the agile approach. More than 60% of the companies in North America, Europe, and Asia have been predicted to face a higher celerity in the digital transformation between 2020 and 2023. The number of cybersecurity complaints the FBI receives has also surged from 1000 calls a day in the pre-pandemic world to a whopping 4000 at present. Industries like Healthcare, Financial Services, Government Organizations, and Manufacturing have become the primary target of hackers.

With the increased number of end-user devices and the unprecedented pace of the digital transformation, cybersecurity has taken the center stage for the Chief Information Security Officers around the globe, wanting to leave no stone unturned to plug in the digital holes. Across the cybersecurity landscape, thinking ahead of the curve and routinely evaluating the hacker's evolving mindset, and combating it with equal, if not greater, might have become a necessity.

Be on Your Guard with Deception

Deception is an active defense strategy using which an enterprise can potentially succeed in defending itself from cyber-attacks every time, safeguarding it from the attackers the one crucial time. It acts as a reliable cyberweapon that elevates an organization's active defense capability by laying down a blanket across the enterprise network, planting fake cues that serve best when the network perimeter falls short on the controls and suspects a breach. This strategy gives the good guys an edge over the bad guys by luring them towards the askew assets of the enterprise, engaging them, and alerting the Security Operations Center with a prompt and legitimate warning allowing them to devise an adequate response plan facilitating timely aversion of a crisis.





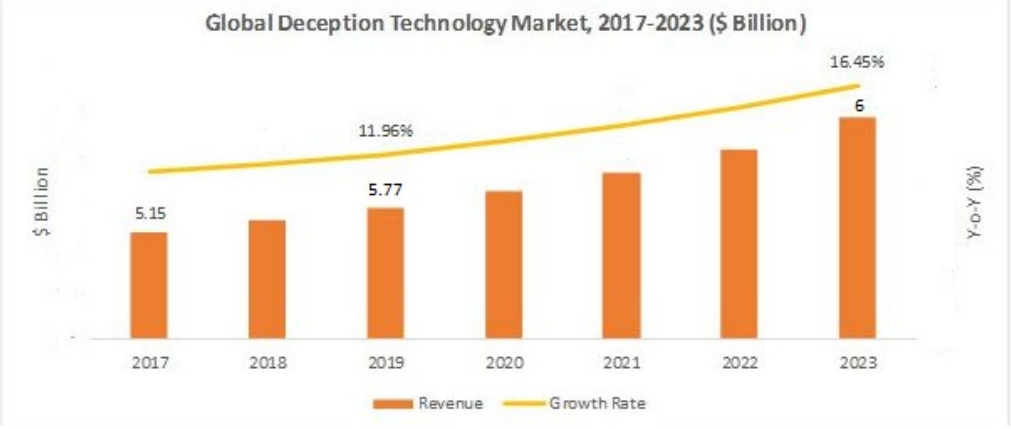
A large part of the existing security solutions can effectively identify the deviation from the standard state of the network leading to false positives and wastage of resources with no details on the extent of the risk and the underlying intent. Unlike other strategies, the most prominent advantage of deception is to set up a playing field for the threat actors where their entire attack campaign can be simultaneously tracked and monitored in a contained environment to analyze the TTPs they apply and assess the intent behind the attack. This is the most rewarding learning for the Security Operations Center that imparts them the knowledge to thwart similar campaigns in the future.

What the Future Holds

As per recent research, the Global Deception Technology Market, that was valued at USD 1.19 billion in 2019, has been predicted to arrive at USD 2.48 billion by 2025, logging a CAGR of 13.3%.

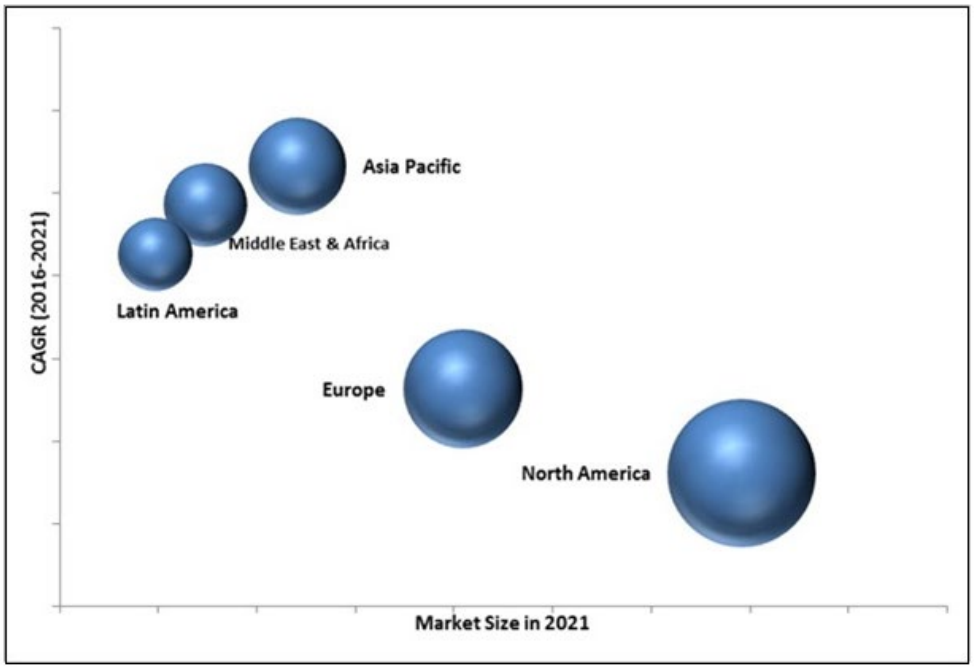
Recently, a promising Deception-tech player got acquired by Zscaler, a cloud security company. The Mumbai-based startup empowers organizations by laying down decoys with enhanced features like alerts, forensics, and root cause analysis.

Furthermore, equipped with the best deception technology in the market, Zscaler is all set to take down the threat actors with an accelerated threat perusal and containment strategy, thereby capitalizing on the global deception technology market.



Source: Infoholic Research

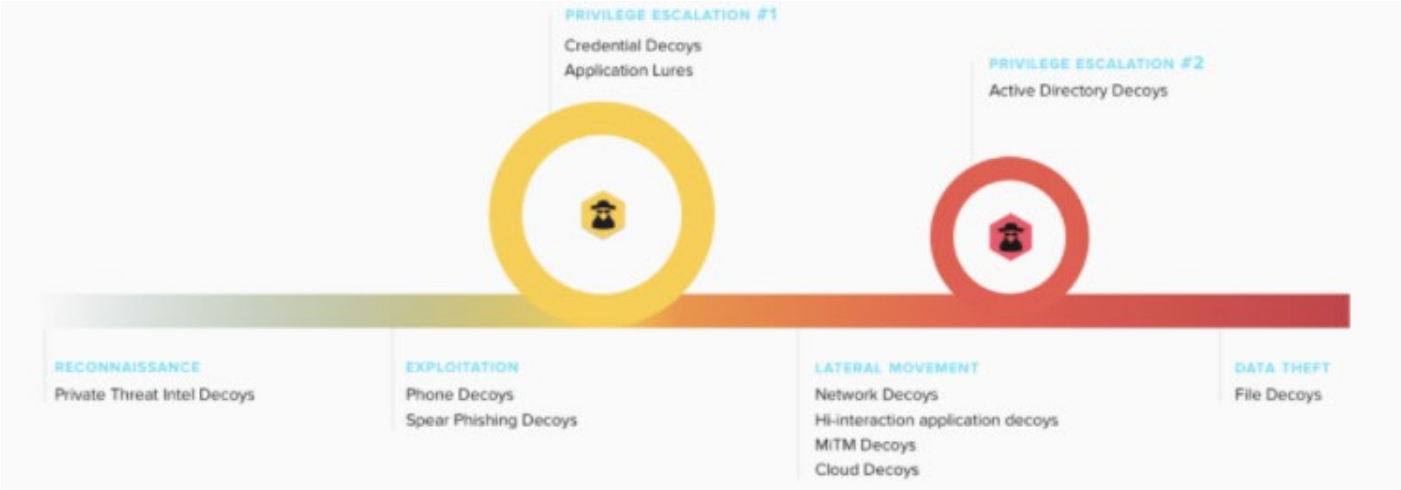
The deception technology market is witnessing highest growth in the areas of North America, Europe, APAC, the Middle East and Africa and Latin America. In recent years, the region of North America has been the highest revenue generator of the market, with Europe being the next in the queue. The apparent factor that drives this trend is the inclination of the developed world towards innovation Theincrease in the IoT and BYOD-related technological advancements within the organizations, is set to drive the deception technology market growth in the APAC region. . The increased number of cyber-attacks in the healthcare sector is expected to further fuel the market in the APAC region.
The deception technology market is forecasted to enable the regions of Latin America, the Middle East, and Africa to log a comparatively higher CAGR by the end of 2028.



Source: MarketsandMarkets.com

Applied Deception

The Deception Technology market finds widespread use cases across industries like BFSI, Healthcare, Defense, IT, Government, Telecommunication, and others across domains of network security, application security, endpoint security and data security.



Source: Smokecreen.io

The disruption brought about by Cloud Computing has boosted the availability of computing resources like VMs and containers, and the increased number of cloud accounts users has resulted in bulky threat noise.

The **Perimeter Deception Controls** effectively deploy the fake assets that imitate the vulnerable infrastructure and create high fidelity alerts helping in determining the attack attempts from the likes of the WAF logs.

If the attacker successfully enters the premises evading all the perimeter controls, the **Network Deception Controls** come into play. The hoax workstations and servers deployed at various locations confuse the threat actors who end up exposing themselves.

The Network Deception is considered most effective when even the legitimate users get baffled while performing their daily tasks coupled with the **Endpoint Deception Controls** capturing not just the deflected behavior on the network but also the regular behavior of the users in the event of getting tricked by a decoy leading to invalid location on a certain endpoint at a time.

Industry Use Cases

Healthcare: The technological revolution in the healthcare landscape with increasingly interconnected medical devices has made it a hot spot for cybercriminals. The dynamic and distributed nature and continuously fed critical PII and PHI IoTs takes the healthcare industry out of the gamut of human expertise, making it difficult to track, detect and respond in the event of a breach. Perimeter-based solutions are quite popular, but they are not very robust and require frequent policy and access mechanism renewal to stay pertinent. All major deception players offer automated deceptions that redirect the attackers away from the production hosts resulting in early detection of sophisticated ransomware attack campaigns.

Financial Services: The ripples of damage to a Financial Institution caused by a cyber-attack reach far beyond what meets the eyes. Its implications are not only confined to the monetary impact - the loss of investors' trust in the organization also erodes years of goodwill built. Other factors like continuous business innovation, frequent mergers & acquisitions, and rapid cloud transition add fuel to the fire, resulting in increased susceptibility to attacks and swelling up the need for robust defense protocols. Advanced Persistent Threats (APTs) frequently target the BFSI sector. Another factor keeping the industry vulnerable to attacks is the Society for Worldwide Interbank Financial Telecommunication (SWIFT) services. Popular deception solutions deploy decoy SWIFT credentials to mislead the attackers into engaging and inhibiting the attack.

In a Nutshell

It is the ever-expanding nature of the attack surfaces that leads towards the ever-emerging attack TTPs. While it is the need of the hour to tighten the grip on the perimeter controls, the security professionals too need to be on their toes, being watchful of any possible perforation. Deception, emerging as a potential primary cybersecurity strategy, is set to turn the tables around in the event of a breach by empowering the Security Operations Center with desired contingency accompanied by visibility and insight into the attacker's every move.

Bibliography

- Steve Lasky (Jan 5, 2021). It will be the year of deception in the cybersecurity world say the experts, retrieved from SecurityInfoWatch
- Dan Woods (Jun 22, 2018). How Deception Technology Gives You The Upper Hand In Cybersecurity, retrieved from Forbes
- Infolic Research LLP (May 2018). Global Deception Technology Market to grow at a CAGR of 12.8% to aggregate $2.4 billion by 2023, retrieved from Infolic Research
- Deception Technology Market, retrieved from Markets and Markets
- Laura Wood (April 29, 2020), Global Deception Technology Market: Growth, Trends and Forecast to 2025, retrieved from Research and Markets
- Heather Pemberton Levy (March 23, 2016). Riding the Deception Wave, retrieved from Gartner
- Deception Technology Market Size, Share and Industry Analysis, retrieved from Fortune Business Insights
- Three Use Cases for Deception Technology in Financial Services, retrieved from Golllusive.com
- Deception Use Cases for Financial Institutions, retrieved from Attivonetworks

About the Authors

Manish Kumar (CYBER-SEC)

Manish Kumar is a Principal Consultant at Infosys Cybersecurity and heads CyberNext Platform Engineering at Infosys, responsible for building Threat, Vulnerability & Risk Detection and Response platform, onboarding customers to platform & Platform Operations. Holds certifications like CISSP, CISM, GCIH, and ISO 27001:2013 LA.

Shivani Sharma (iCETS)

Shivani Sharma is a Senior Associate Consultant at Infosys. She has a noteworthy contribution towards significant implementations in the project management space. She is currently engaged in research and partnership activities at Infosys Center of Emerging Technology Solutions and actively scouts for innovations in emerging technologies, including Cybersecurity.

About Us

The incubation center of Infosys called 'Infosys Center for Emerging Technology Solutions' (iCETS) focuses on the incubation of NextGen services and offerings by identifying and building technology capabilities to accelerate innovation. The current areas of incubation include AI & ML, Blockchain, Computer Vision, Conversational interfaces, AR-VR, Deep Learning, Advanced Analytics using video, speech, text, and much more.

To know more, please reach out to iCETS@infosys.com

For more information, contact askus@infosys.com

Infosys®
Navigate your next