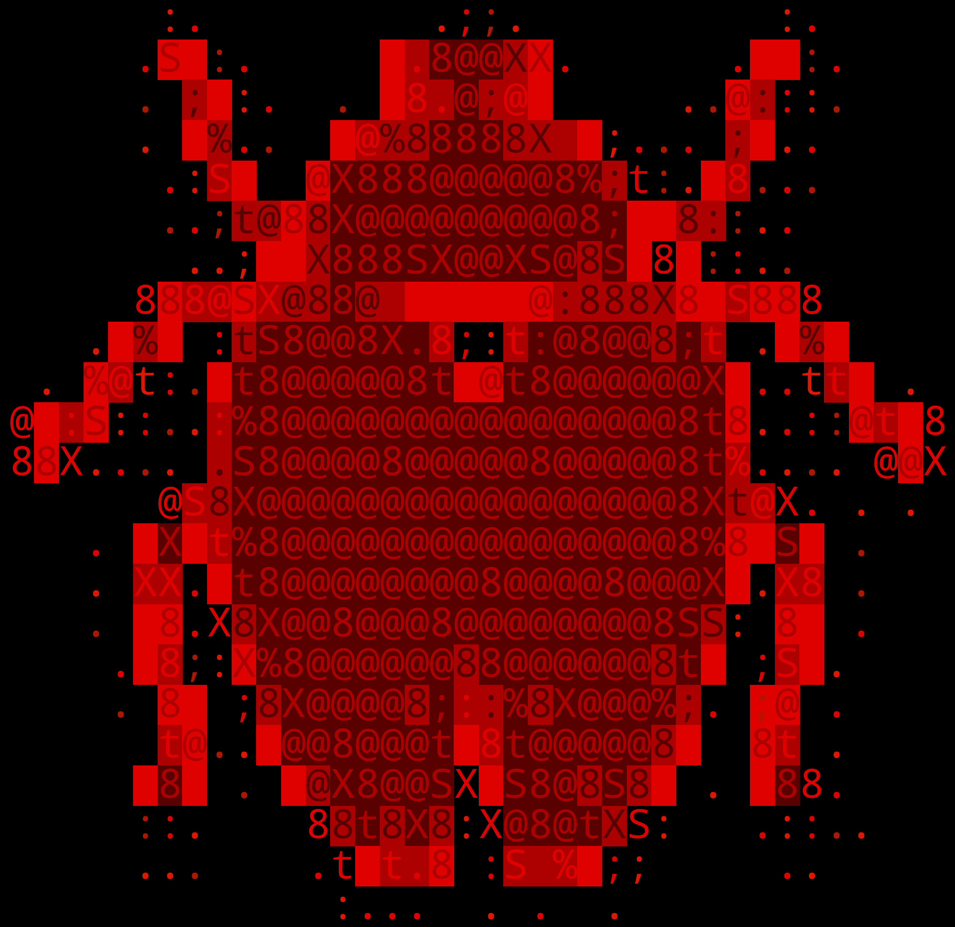
LTIMindtree



Point of View

Eliminate Blind Spots in Your Network with Continuous Breach Attack Simulation

Index

The Modern Cybersecurity Landscape

Organizations invest and deploy a plethora of software and hardware tools for securing their IT network like firewalls, IPS, AV, anti-virus, anti-phishing, IAM, EPS, etc. However, this conventional approach is failing to safeguard organizations as news of cyber-attacks keeps popping up frequently.

Modern day hackers use sophisticated techniques with a data-focused approach. They are very patient and remain dormant for months inside the network, which helps them to avoid various security scans. This helps them leverage various vulnerabilities, IT misconfiguration, user behaviour, and IT hygiene checks to move laterally towards the targeted data asset. Organizations need a proactive approach to deal with such type of sophisticated cyber criminals.

Data Security is the Key

The primary concern of cyber security leaders is to identify whether critical IT assets, which directly service a large number of customers or internal employees, are susceptible to external threats. A cyber security breach might result in irrevocable brand reputation loss in addition to significant financial loss. The average cost of data breach reported in the US stood more than USD 8.64 million in 2020. What's interesting to note is 43% of these breaches occurred in small businesses. Key responsibilities of cyber security teams include security, availability, and performance of IT assets. Moreover, CISOs have to achieve and maintain these KRAs within approved IT Security budget.

Shortfall of Conventional Cyber Defense Approach

Traditionally, vulnerability assessment and red teaming/penetration testing is conducted periodically, within a scheduled time frame. However, the IT network vulnerability, attacker's approach, and mindset are dynamic. Hence, organizations remain prone to new vulnerabilities.

Drawbacks of VA Tools

VA scan outlines many vulnerabilities to be remediated, but it does not prioritize them with respect to protection of critical IT assets, nor provides inter-relation among those vulnerabilities.

Inefficient use of cyber security and IT support team for such remediation.

These tools overlook IT misconfiguration and hygiene.

Moreover, vulnerabilities emanating due to user behavior are left out of such tools.

Drawbacks of Red Teaming/ Manual Penetration Testing

Since Red/Blue teams consist of highly skilled security professionals, ethical hackers acting either as adversaries or protector of security landscape, Red/Blue teaming/and penetration testing proves very costly as organizations have to hire skilled manpower as internal employee or on a contract basis.

Scalability always remains a challenge for traditional Red Teaming.

Test findings and remediation loses relevance after few months as IT infra and network is dynamic.

Experienced and skilled manpower is in short supply and costly to retain.

Risk of exposing network topology to personnel of different organizations.

CBAS - The Way Forward

In order to cope-up with challenges posed by cybercriminals, organizations must keep a continuous vigil at their IT landscape and augment thesecurity teams think from a hacker's perspective.

The Continuous Breach Attack Simulation solution helps security teams to gain visualization of all attack vectors as the hacker moves from one node to another within the organization network. Once simulation of particular attack scenarios end, all the vulnerabilities and compromised assets are compiled. This solution shows critical findings and recommends the prioritized, actionable remediation items. The process runs 24x7, 365 days providing continuous visibility and protection.

CBAS Solution: Advantages and Unique Features

Stops exposing customer network to external pen testing personnel.

Provides complete awareness of all possible attack paths to your critical IT assets at any given time.

Protects on-Premise, cloud or hybrid networks with an integration of existing SIEM tools used by customers.

Remains a step ahead of hackers with up-to-date attack techniques in our software updates.

Significant saving every year on cost of hiring pen testing teams internally or externally.

Increased efficiency of cyber security and IT support manpower as they have to focus on and remediate far lesser vulnerabilities.

The Bottom Line

Cyber attackers and their methodologies have evolved dramatically in the past couple of decades. They capitalize on human errors like misconfigurations, shadow IT, and lack of user awareness to breach an organization's network. Attackers employ legitimate tools and leverage user behavior to infiltrate networks and compromise assets, making any enterprise vulnerable to attacks even with modern security controls and processes in place.

In order to tackle this situation, enterprises need to be one step ahead of the attackers by gaining real-time snapshot of their security posture - which includes visibility of infrastructure configuration, network vulnerabilities, and risk exposure of their critical assets. CBAS simulates, validates, and remediates every hacker's path to the critical assets within the network and eliminates the most critical blind spots in the enterprise network with detailed visual display of potential threats, attack path, and actionable remediation insights, CBAS helps organizations to increase awareness of its security personnel, increases cost-effectiveness of potential remediation efforts, captures overall risk score and changes over time, and thus bolsters overall security posture.

About the author

Manoj Devendrappa

Specialist – Cybersecurity, **LTIMindtree**

Manoj is a consultant in the cybersecurity domain, having 10+ years of experience with proven track record in helping customer organisations meet their security goals and objectives by delivering core Blue team and Red Team functionalities. He has also been involved as a security solution architect and assist organizations in devising security strategy and roadmap planning, infrastructure design, and innovation. At LTIMindtree, Manoj is responsible for Technical Service Delivery management, implementing strong governance across accounts, infrastructure outsourcing for information security, identifying customers' technical and business requirements to design cyber security solutions as per industry standards.

LTIMindtree