How Attack Surface Management Works?

The attack surface refers to all the hardware, software, SaaS services, and cloud assets that process or store organization's data and are accessible from the Internet.

Attack surface management follows five steps:

1 Asset Discovery

It involves enlisting all internet-facing assets including web applications, services, APIs, cloud storage, email servers, etc.

2 Inventory & Classification

The assets are discovered & labeled based on type, technical properties, business criticality, compliance requirements, & ownership.

3 Risk Scoring & Security Ratings

The risk factor of each asset is identified & ratings are derived from objective and verified information.

4 Continuous Security Monitoring

Regular monitoring is done for newly discovered security vulnerabilities, weaknesses, misconfiguration, and compliance issues.

5 Malicious Asset & Incident Monitoring

This step involves monitoring for infamous cyberattacks such as spear phishing websites, email spoofing, ransomware, etc.

www.thecentexitguy.com

Centex Technologies

CENTEX TECHNOLOGIES

13355 Noel Road, Suite # 1100, Dallas, TX 75240
Phone: (972) 375 - 9654

501 N. 4th Street, Killeen, TX 76541
Phone: (254) 213 - 4740

1201 Peachtree St NE, Suite 200, Atlanta, GA 30361
Phone: (404) 994 - 5074

Capital Factory, 701, Brazos Street, Austin, TX 78701
Phone: (512) 956 - 5454