Protect Against Breaches

Understand if Your Organization is Secure

DEMAND FOR INFORMATION SECURITY PROFESSIONALS WILL GROW

31%

FROM 2019 TO 2029,

much faster than the average for all occupations[3] including other information technology staff. As demand increases, getting qualified expertise to help stop breaches will be a top priority for teams that are likely to be overworked and understaffed. It's time to PREPARE.

Threat Landscape: User Accounts

- Session Hijacking
- Phishing
- Malicious Insiders

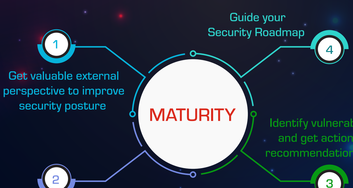
READINESS

Evaluate your threat detection and response capabilities. How prepared are you to stop a breach or respond to an event?

THE THREE PILLARS TO A GOOD BREACH READINESS PROGRAM ARE:

1. Incident Response Plans
2. Disaster Recovery Plans
3. Business Continuity Plans

TOP REASONS TO GET AN EXTERNAL SECURITY PERSPECTIVE



Most IT Security Teams spend their time identifying potential security threats, but this leaves less time to gather information about incidents and resolve them[1]. Having detailed policies and procedures to protect data, along with regular validation of those practices will help ensure that organizations can protect their assets.

PENETRATION TESTS

are designed to identify and assess security risks in several areas — internal, external, web applications. Internal IT teams are aware of the test and have prepared, patched, etc.

Penetration Tests can help secure your company passwords! GoSecure Pen Testers still find **1 in 4 users** have elected to use one of the All-Star passwords (i.e. Password123, CompanyName123,).[2]

RESPONSE

CHOOSE YOUR TEAM!

Red | **Blue** | **Purple Teams** engage in exercises to determine how exposed you are to attacks and improve your organization's security posture. Purple Team exercises are the most innovative and will rapidly test and improve security use cases.

Threat Landscape: Data Infrastructure

- Ransomware
- Malware
- Advanced Persistent Threats
- Botnet & Trojans

PREPARE

www.gosecure.net/advisory-services

GoSecure

[1] – 2019 Osterman Research Inc. [2] – Cybersecurity Perceptions vs Reality [3] – Bureau of Labor Statistics, United States