TRUSTEDSEC CASE STUDY

TrustedSec
Evolve beyond threats

Creating a More Holistic Security Program by

Addressing Adversary Tactics and Techniques

A global company was looking for cutting-edge insights over and above traditional security assessments. While there is tremendous value in security program maturity reviews and penetration testing activities, reviewing the range of adversary tactics and techniques helped develop more robust analytics, increased tool coverage, saved money, and allowed the organization to better detect and respond to adversary behaviors.

Challenge

The organization needed a global assessment to report to executive management concerning the current state of the security posture and spending activities after recent changes in leadership and management structure.

As the organization's security posture had significantly improved over the last several years (with tremendous effort and cost), they found themselves receiving the same general recommendations and maturity scores, keeping their security efforts stagnant with no clear path for improvement. This is because traditional program assessments take an inside-out approach by looking at an organization's policies, procedures, technology, and vulnerabilities to identify areas for improvement, thus only looking at security from one particular angle.

PERSONNEL PROFILE

Engagement Lead (L):
Rockie Brockway,
Practice Lead, Office of the CSO

Rockie leads the Office of the CSO team at TrustedSec with 25 years of experience in IT and Information Security.

Engagement Lead (C):
Rick Yocum,
Senior Security Consultant

Rick has been helping organizations elevate their security and compliance practices for more than 16 years.

Engagement Lead (R):
Stephen Marchewitz,
Director of Practice Development

Stephen has been in the security and risk industry for over 13 years and in IT for over 20 years.

Solution

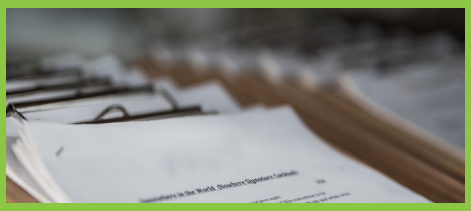
To overcome these limitations, TrustedSec provided an outside-in look at how real-world attackers could potentially breach the organization, supplementing common control reviews and penetration tests. TrustedSec leveraged the MITRE ATT&CK™ framework—"a globally accessible knowledge base of adversary tactics and techniques based on real-world observations."

By including this framework in an attack path effectiveness determination, TrustedSec was not only able to assess the maturity of the program and current vulnerabilities, but also reviewed the technology that the company had in place, the skills and institutional knowledge within the organization, and the completeness of coverage provided by various tools and resources to defend against an adversary's tactics and techniques.

Key Benefits

TrustedSec's approach assisted in reducing the likelihood of adversary success, advising on control investment and resource prioritization, and determining relevant metrics of performance and effectiveness. The organization was then able to verify progress in a repeatable way, align their budget to bridge gaps in control coverage, and reduce spending on redundant tool capabilities (which saved over $400,000). In addition, TrustedSec worked with the organization to determine gaps in tool knowledge and resource constraints that reduced the effectiveness and efficiency of the security team to detect and respond to attack tactics and techniques.

RECOMMENDATIONS INDEX



Program Maturity

- Educated the organization, including leadership, around appropriate security best practices
- Provided a roadmap with operationalized recommendations to rapidly mature the organization

Control Maturity

- Provided an independent baseline on the safeguards to ensure that the current environment meets the organization's security expectations and requirements

OpSec Performance

- Assisted in improving the overall security posture by measuring and providing feedback on tactical performance through people, process, and technology

Attack Path Effectiveness

- Determined tool coverage, overlap, and holes in the defenses
- Analyzed the effects of integrating new or 'next generation' technology with existing infrastructure, software operations, and security management procedures

About TrustedSec

TrustedSec is an Information Security consulting team at the forefront of attack simulations with a focus on strategic risk-management. Our goal is to help organizations defend against threats of all kinds and change the security industry for the better.

With a team handpicked not only for expertise and technical skill, but for ethical character and dedication, TrustedSec is committed to increasing the security posture of organizations around the world.

TrustedSec INFO@TRUSTEDSEC.COM 877.550.4728