PRAETORIAN

WHITE PAPER

Continuous Offensive Security

Partnering to Proactively Protect the Digital Frontier

INSIDE THIS REPORT

A robust cybersecurity program continuously identifies vulnerabilities and proactively secures critical assets.

INTRODUCTION

The Evolution of Security Testing

As organizations embrace new technologies, their attack surfaces expand, creating opportunities for threat actors to exploit vulnerabilities. Traditional security measures are no longer sufficient to protect against advanced cyber-attacks.

Instead, in an age of digital transformation, businesses must adapt to the rapidly-evolving threat landscape. Continuous Offensive Security (COS) addresses this challenge by proactively and continuously identifying and mitigating threats, securing critical assets, and ensuring a robust cybersecurity posture at all times.

> **Key Principle:** A robust cybersecurity program continuously identifies vulnerabilities and proactively secures critical assets—not just during annual assessments, but every day.

UNDERSTANDING COS

What Is Continuous Offensive Security?

COS is a proactive and ongoing approach to cybersecurity that focuses on identifying and mitigating threats in real-time. COS goes beyond traditional defensive security measures, such as firewalls and antivirus software, to actively engage with potential threats, identify weaknesses in systems and applications, and remediate vulnerabilities before attackers can exploit them.

COS is most effective when it is a managed service, which means that a third-party partner has committed to proactively monitor and manage an organization's security posture. The partner integrates several security solutions into a single managed offering that includes:

- **Attack surface management** - Continuous discovery and monitoring of assets
- **Red teaming and penetration testing** - Simulated attacks to identify vulnerabilities
- **Vulnerability triage and prioritization** - Risk-based assessment of findings
- **Exploit intelligence** - Real-time awareness of emerging threats
- **Adversary emulation** - Testing defenses against real-world attack techniques

Risk-Based Approach

At the core of COS is a risk-based approach to security testing. This involves prioritizing vulnerabilities based on their impact on an organization's business objectives and allocating resources to address the most critical vulnerabilities first.

THE NEED

The Need For Continuous Offensive Security

The increasing complexity of IT ecosystems, adoption of SaaS and PaaS, and the ever-expanding attack surface has created the perfect environment for sophisticated attackers.

This change in threat environment necessitates a shift from reactive to proactive security measures and from point-in-time security assessment to continuous security testing.

The End Results of a COS Program

1. **Resilient Response**
   A more resilient and agile response to emerging threats
2. **Greater Visibility**
   Greater visibility into an organization's risk exposure and potential attack vectors
3. **Improved Posture**
   Improved security posture through constant discovery of unknown material risks
4. **Business Alignment**
   Better alignment of security practices with business objectives

$4.35M
GLOBAL AVERAGE COST OF A DATA BREACH

80%
OF ORGANIZATIONS WITH PROACTIVE TESTING REPORTED IMPROVED CONFIDENCE

According to the Ponemon Institute's 2022 Cost of a Data Breach Report, the global average cost of a data breach in 2021 was $4.35 million. By adopting a more proactive and continuous approach to security testing, organizations can reduce the risk of a successful cyber-attack and potentially avoid the high costs associated with a data breach.

A 2020 survey by Forrester Consulting found that 80% of organizations that adopted a proactive approach to cybersecurity testing reported improved confidence in their security posture.

DIFFERENTIATION

Why Choose COS Over Other Solutions?

The market offers several different approaches to cybersecurity testing and validation, including bug bounty programs and separate point products for attack surface management, breach and attack simulation, and continuous automated red teaming. A COS managed service solution is a better option for several reasons.

First and Foremost: A Partnership, Not a Product.

A successful COS program is not just about the technology, but also about the people and processes that support it. That's why we take a partnership approach with our clients to help them achieve their cybersecurity goals.

Our Partnership Principles

1. **Trust**

   We believe that trust is essential to a successful partnership. Our clients trust us to provide them with the best possible cybersecurity solutions and to act in their best interests at all times.

2. **Collaboration**

   We work closely with our clients to develop a deep understanding of their security needs and objectives. This collaboration helps us to develop tailored solutions that are specifically designed to meet their unique requirements.

3. **Expertise**

   Our team of security experts has years of experience in the cybersecurity industry. We leverage this expertise to provide our clients with the best possible guidance and advice.

4. **Continuous Improvement**

   Cybersecurity threats are constantly evolving, and so are our solutions. We are committed to continuous improvement and work closely with our clients to ensure that our solutions are always up-to-date and effective.

DIFFERENTIATION

Other Key Differentiators of COS

Extends Your Team With External Experts

Since COS is a managed service, it includes security experts who have the expertise to identify and remediate vulnerabilities. They also can provide actionable insights to improve security posture. In contrast, point products often require in-house expertise to operate effectively, which can be a significant challenge for organizations that do not have dedicated security teams.

Focuses on Comprehensive and Customized Testing

COS offers a comprehensive and customized approach to security testing, which integrates attack surface management, red teaming, penetration testing, vulnerability management, exploit intelligence, and adversary emulation. This ensures evaluation and validation for all aspects of an organization's cybersecurity posture.

Provides Proactive Defense

COS keeps organizations several steps ahead of attackers by continuously identifying and mitigating potential vulnerabilities and attack vectors before attackers can exploit them. In contrast, point products such as bug bounty and breach and attack simulations focus on identifying vulnerabilities after an attack has already occurred.

Includes Full Scope

COS challenges industry norms around applying an artificial "scope" to testing. Traditionally, organizations have focused on testing a specific subset of their systems based on predefined criteria. This approach can result in blind spots and cause organizations to miss material exposures.

USE CASES

Common Use Cases for Continuous Offensive Security

Mergers and Acquisitions

During M&A activities, organizations must assess the cybersecurity posture of the target company. COS techniques like red teaming and penetration testing can help identify vulnerabilities, assess security risks, and ensure a smooth integration of digital assets.

Supply Chain Risk Management

As organizations rely on third-party vendors and service providers, they must ensure that these partners maintain strong security practices. COS can evaluate the security posture of third parties, identify potential risks, and develop strategies to mitigate these risks.

FDA Premarket Submission and Postmarket Monitoring

In the healthcare industry, the FDA requires medical device manufacturers to ensure the security of their devices. COS validates medical device security as part of the premarket submission and then continuously monitors security post-market, protecting patient safety and data privacy.

Securing Digital Transformation

As organizations increasingly migrate to the cloud, they must ensure that their cloud-based assets are secure. COS can help identify misconfigurations, vulnerabilities, and potential attack vectors in cloud environments.

CONCLUSION

Conclusion

Overall, Continuous Offensive Security can be a valuable tool for any organization that wants to proactively defend its digital assets against cyber threats. By employing COS techniques, organizations can identify vulnerabilities, assess risks, and remediate security gaps before attackers successfully exploit them.

> **The results:** A more resilient and agile security posture, better alignment of security practices with business objectives, and improved compliance with regulatory frameworks.

Additional Use Cases

- **Satisfying Regulatory Compliance** - COS satisfies compliance annual penetration testing requirements for frameworks such as GDPR, HIPAA, and PCI DSS
- **Validating Incident Response** - COS helps organizations develop and test their incident response plans, ensuring readiness

Resources

"The State of Network Security, 2020-2021."
Homes, David and Shey, Heidi. Forrester Consulting. 2 August 2021.

"2022 Cost of a Data Breach Report."
Ponemon Institute. 2022.