TECH
mahindra

Strategize to Reduce Attack Surface with Agility

WHITEPAPER

The growing security breaches has made it important for an organization to look at managing the attack surface in an effective manner. Traditionally managing attack surface was very limited to performing exploratory nature of detection and protection techniques around external attack surface. Increased cloud adoption, continued hybrid nature of work, organizations failing to identify the unknown assets and the people being a major actor has brought in the need to expand the scope of attack surface management and strategize to reduce the attack surface with agility.

Abstract

This whitepaper helps you understand how people, process, and technology play a very important role in reducing the attack surface and how the principles of Agile can be effectively applied to attack surface management. Further on, the content also presents you insights on why the traditional way of managing the attack surface is not just enough. While reducing the attack surface every contributor such as external attack surface, internal attack surface, third party vendors, supply chain play their own part in the security ecosystem.

Key Takeaways

Some of the key takeaways of this whitepaper include

- Application of principles of Agile to respond to possibility of breaches, incidents in a faster manner
- Adoption of strategic cybersecurity initiatives by the organizations
- Insights into the vectors that define attack surface comprising of external, internal, and vendor management ecosystem
- A perspective into attack surface management is not just about technology, but a combination of people, process, and technology
- Effective risk quantification, prioritization, grouping of vulnerabilities to act with agility
- Analytics to help in Agile cybersecurity decision making

Introduction

This whitepaper provides an overview of managing the attack surface effectively with various methods and processes and brings in the aspect of Agile phases which will help organizations strategize to reduce the attack surface with agility. This paper is intended for those looking for a holistic solution around managing the attack surface in a faster manner.

Listed below are some of the key challenges most the organizations face and the reason why paying close attention to attack surface management is necessary

- Increased cloud adoption
- Continued remote working
- Shadow IT assets in the organization both external and internal
- Increased targeted social engineering attacks
- Lack of effective detect and respond controls
- Fixation towards external attack surface management rather than looking at aspects like internal attack surface management, attack surface generated by lack of knowledge by employees and so on

Understanding Attack Surface and Application of Agile Methodology

It is important to see attack surface with agility. There are multiple factors that contribute for reduction of organizations attack surface are covered in this whitepaper as depicted below

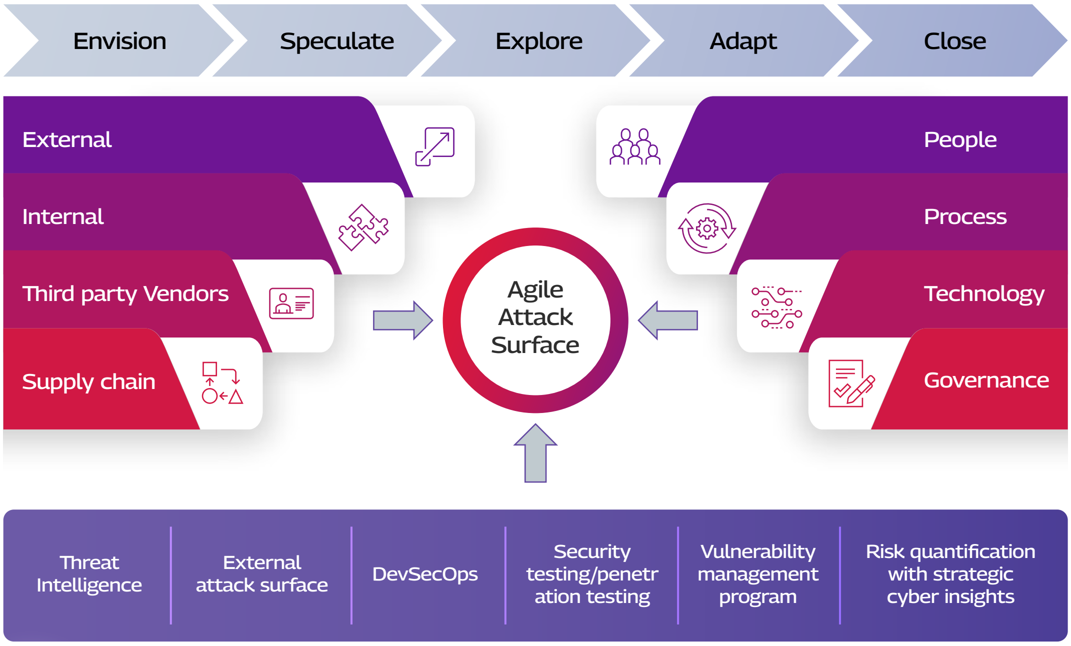


Figure1: Depiction of Agile attack surface with phases of Agile project management and various vectors contributing to managing attack surface with agility

Attack Surface - An Understanding

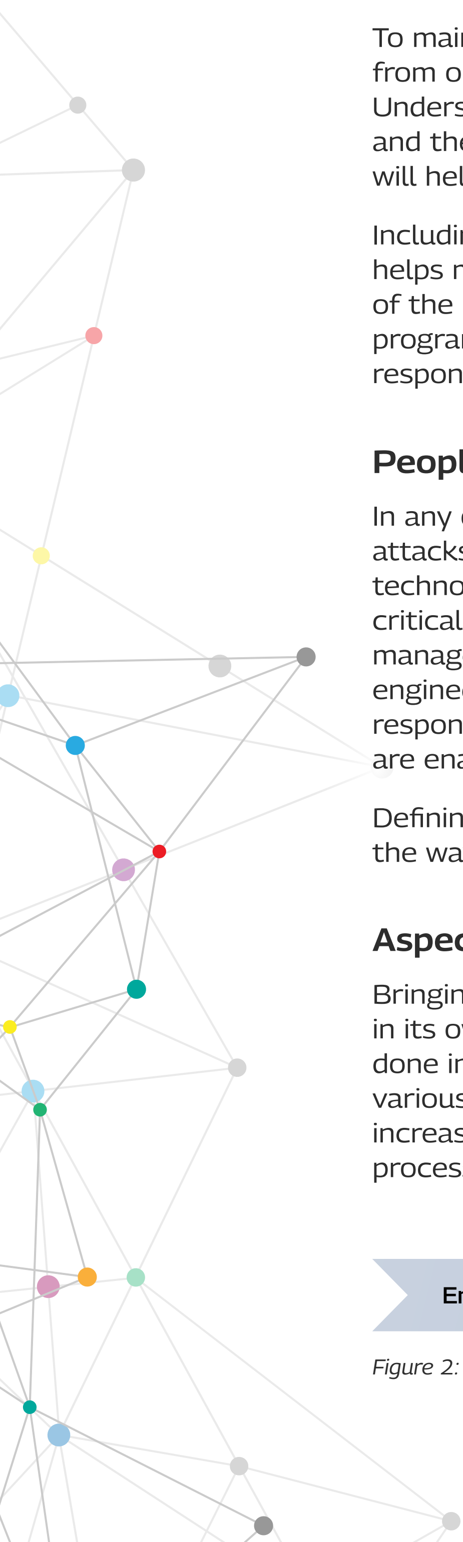
Organizational Ecosystem

At the core, let's try to understand what an attack surface comprises for an organization. Attack surface comprises the following

- External attack surface
- Third party vendor management
- Internal attack surface
- Supply chain

To maintain the attack surface effectively the organizations, must move away from one time security testing kind of programs to continuous security testing. Understanding the attack surface from an external perspective is necessary and the organizations need to have periodic red teaming kind of exercise which will help gauge the security control effectiveness.

Including security in the CI/CD pipeline in DevSecOps kind of implementation helps minimize the attack surface to a great extent. Leveraging the capabilities of the platforms which provides threat intel, vulnerability management program status, SIEM/SOC systems will help reduce the attack surface and respond to a breach or an incident in a quick manner.



People, Process, and Technology - Contributors to Attack Surface

In any organization, people are always the first line of defense against any attacks. Reducing the attack surface is not limited to enablement of technology with various tools and techniques, but ensuring People also play a critical role in reduction of attack surface. In internal attack surface management people play a significant role and always at the risk of social engineering attacks. It is necessary that there are right set of roles and responsibilities identified to manage the cyber security incidents so that they are enabled to act with agility.

Defining the set of maker checker kind of processes, right SOPs are some of the ways to put a process around the attack surface to manage it with agility.

Aspects of Agility in Attack Surface Management

Bringing in the Agile way of doing the software development was revolutionary in its own way where a software which would take months to go live would be done in weeks and product is ready to be consumed. In Agile, it's all about how various teams / sources come together to work in a seamless manner and increase the speed by 2X. The core principles of Agile include ensuring people, process, and technology work in absolute tandem and with speed.

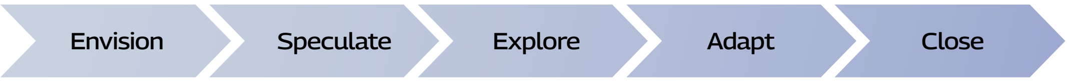


Figure 2: Understanding the phases of Agile

Let's now apply these phases of Agile to managing the organizations attack surface effectively.

We will understand this with an example.

Envision

In this phase, as defined earlier, knowing your attack surface can be through the various threat intel from different platforms, continuous attack surface scanning, implementation of DevSecOps to name a few. This is how organizations have a better view of the current security posture and how breach resilient it is against any attacks. Understanding the cyber strategy of the organization and putting in the context of the same around attack surface management provides a key insight.

Speculate

Once the organizations know their attack surface and the weaknesses, it's important to put the required controls in place to fix the same so that they are ready in case of any incident. Enabling people, processes, and the required technology in place will ensure that the teams act with agility in case of an incident. The ability to bring in analytical and contextual insights along with the principle of 80-20 rule helps organizations focus on issues that matter.

Explore

Understanding the risk with appropriate quantification either with strategic cyber insights or operational insights will help explore the various controls or techniques to be applied to mitigate the same in an agile manner. It's all about risk prioritization and quantification and preparedness by the organizations to act quickly in case of an incident.

Adapt

In agile way of doing things, people play a very important role. Enabling them with the right skillset, technology and platforms will help them adapt better and respond quickly. The ability to adapt to various situations allows the teams to be prepared for anything. Having the right root cause analysis and governance model helps organizations to sustain the agile manner of managing the attack surface.

Close

This is the final phase where the teams will continue manage the attack surface powered by governance and applying various threat intel received through different defensive mechanisms. While this stage enables to mitigate individual attack surface vectors, this entire process must be performed in a cyclic manner while continuing to envision, speculate, explore, adapt, and close.

Benefits

- Organizations have an opportunity to move away from traditional attack surface management that was limited to dark web kind of monitoring alone
- People who are the first line of defense for any organization are well equipped to act with agility
- Applying the principles of agile to respond quicker to threats identified through the ASM process
- Consolidating the threat feeds from different systems makes it easy for organizations to prioritize the risk and strategize mitigation

The Way Forward

While the current techniques focus a lot on technology aspects of ASM, TechM's approach helps organizations look at ASM in a holistic manner. Currently the tools techniques available in the marketplace have limitations to cover the entire scope of Agile attack surface management TechM believes that while fragmented components of agile ASM exist a combination of using the right tools, processes and analytics would ensure that objective of Agile ASM is met.

Authors

Maninder Bharadwaj

Global Head, Cybersecurity and Risk Management, Tech Mahindra

Maninder has over two decades of experience in cyber risk and risk advisory consulting serving diverse clients located in Asia, Americas, and Europe. He has consulted in various industries including consumer business, life sciences, manufacturing, oil and gas, and BFSI.

Maninder has gained a well-rounded management experience by being in roles of risk advisory CTO, risk advisory clients and industries leader, practice COO, leader of large firm accounts, and regional leader.

Suchitra Krishnagiri

Suchitra has 15+ years of information security experience with expertise in application security and devsecOps . In her experience, she has led global delivery for penetration testing services, by being a solution architect on large programs and currently heading the centre of excellence for application security at Tech Mahindra.

Disclaimer. Brand names, logos and trademarks used herein remain the property of their respective owners.