Cybersecurity News

NEWS AND INFORMATION TO HELP PROTECT COMPANIES AND EMPLOYEES

OCTOBER 2020

UNDERSTANDING APPLICATION SECURITY TESTING (AST) OPTIONS

The need to integrate security into all levels of a business extends into the organization's own software. The security of these applications can be tested in development and production using application security testing (AST). By making AST a priority, an organization builds more secure code and applications and lets clients know that it is focused on providing a secure end product. To help in understanding the options and considerations, Help Net Security asked global experts for their guidance on selecting AST solutions.

Assess the current environment

Look at the staffing, approach, and tools that are already in place within your organization. The current approach and staffing may apply a continuous integration and continuous delivery (CI/CD) workflow process with security. Consider how security can be woven seamlessly into the workstream using the best tools for the situation.

Avoid the one-size-fits-all approach: establish testing for the environment and needs

Choose the AST testing that fits the particular needs of your corporation, bearing in mind budget, technology infrastructure, source code availability for analyses, and open-source components that make up the environment to be tested.

Review true-positive and false-positive vendor rates

Taking time to determine if results are valid is expensive in terms of staff time and undermines the AST product itself. Understanding true- and false-positive rates helps you gauge the real-world usability of a given AST product.

Assess viability within your unique workflow

Can the AST product function in your workflow? If not, development teams will be reluctant to embrace it.

Consider implementation time

How quickly can the AST product result in security improvements that are measurable, beyond just finding security issues?

THE AST TOOLS

Static application security testing (SAST)	Scans code early
Software composition analysis (SCA)	Scans code for open source software usage
Dynamic application security testing (DAST)	Tests in production
Interactive application security testing (IAST)	Analyzes code when an automated or human tester is working with the application
Runtime application self-protection (RAST)	A specific type of IAST that operates from within applications

Source: Lemos, Robert. *SAST, DAST, IAST, and RASP: Pros, cons and how to choose*, TechBeacon. https://techbeacon.com/sast-dast-iast-rasp-pros-cons-how-choose.

(continued)

DevSecOps: EMBEDDING SECURITY INTO RAPID-RELEASE APPLICATION CYCLES

DevSecOps engrains security into the application development and deployment by fully integrating security testing into the continuous integration and continuous delivery (CI/CD) pipelines. It also increases the knowledge and skills of the development teams to enable them to manage testing and fixes.

Source: Constantin, Lucian. *What is DevSecOps? Why it's so hard to do well*, CSO, July 23, 2020. https://www.csoonline.com/article/3245748/what-is-devsecops-developing-more-secure-applications.html.

Apply a variety of approaches and consider consultant qualifications

Beyond the types of testing (e.g., SAST, DAST, IAST) specifically needed, consider that business logic, authorization, and identity management in testing can be missed by automated testing. Professional services can help support these needs, but look for qualified consultants who are certified and have practical experience.

Source: Zorz, Mirko. *How do I select an application security testing solution for my business?*, Help Net Security, July 8, 2020. https://www.helpnetsecurity.com/2020/07/08/select-application-security-testing-solution/.

NEW MUFG CISO DISCUSSES THREATS AND REDUCING CYBER RISK

As the new MUFG Union Bank, N.A., Chief Information Security Officer (CISO), Devon Bryan brings extensive cybersecurity experience to leading the security efforts at MUFG. In a new MUFG video, Devon addresses the following topics:

- The importance of cybersecurity
- The greatest cybersecurity threats
- Considerations for reducing cyber risk

Visit MUFG's YouTube channel to view the first video in a series and learn more about Devon's thoughts and approach to cybersecurity.

> *"Cybersecurity is truly a team sport and each employee in the organization plays an important role as a part of the overall defensive strategy."* — *Devon Bryan, CISO, MUFG*

OCTOBER IS NATIONAL CYBERSECURITY AWARENESS MONTH: DO YOUR PART. #BECYBERSMART

Every October, the United States Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA) and National Cyber Security Alliance (NCSA) lead observance of National Cybersecurity Awareness Month (NCAM).

Because our online and offline lives are becoming more indistinguishable, this year's theme is focused on individuals and organizations protecting their parts of cyberspace by:

- Implementing stronger security practices
- Raising community awareness, and
- Training employees and educating vulnerable audiences

For more information about how to promote Cybersecurity Awareness month, visit the NCSA Stay Safe Online site: https://staysafeonline.org/.

Source: National Cyber Security Alliance. *Stay Safe Online.* https://staysafeonline.org/.

COVID-19 AFFECTING CYBERSECURITY AND SPENDING

The pandemic created opportunities for cybercriminals to exploit a sense of fear and urgency through their scams. Meanwhile, people spent more time online at home, and organizations were in a crucial situation requiring them to adapt to the all-remote reality.[1]

For many organizations, prioritizing employee uptime at home may have resulted in a lack of security with more permissive virtual private network (VPN) access policies and quickly built infrastructures. In addition, employees are working in home environments that are vulnerable due to loosened security policies, shared WiFi passwords, and internet of things (IOT) device use.[1]

It's not fully clear how COVID-19 affects current and future spending on security, but security remains a priority. In a recent Microsoft study of 800 global business leaders of companies with more than 500 employees in India, Germany, the United Kingdom, and the U.S., 58% of these organizations reported increased security spending. For spending through the end of 2020, nearly 40% of respondents indicated that they are prioritizing cloud security. Organizations are also prioritizing investments in data and information security, network security, anti-phishing tools, and endpoint detection and response (EDR).[2]

For more insights on security spending, see the Microsoft study results.

[1] Marozas, Leonardas. *We need to rethink cybersecurity for a post-pandemic world. Here's how*, World Economic Forum, August 13, 2020. https://www.weforum.org/agenda/2020/08/rethink-cybersecurity-post-pandemic-world/.

[2] Conway, Andrew. *New data from Microsoft shows how the pandemic is accelerating the digital transformation of cyber-security*, Microsoft, August 19, 2020. https://www.microsoft.com/security/blog/2020/08/19/microsoft-shows-pandemic-accelerating-transformation-cyber-security/.

The information above is provided as a convenience, without warranties of any kind and MUFG Union Bank, N.A. disclaims all warranties, express and implied, with respect to the information. You are solely responsible for securing your systems, networks, and data. You should engage a qualified security expert to advise on your specific needs and requirements.

This *Cybersecurity News* contains news and information designed to help protect your company and employees.