A MODERN APPLICATION SECURITY PLAYBOOK

8 ESSENTIAL STEPS FOR CREATING A SECURITY STRATEGY ACROSS DEVELOPMENT AND OPERATIONS

CONTRAST SECURITY

INTRODUCTION

CREATE A UNIFIED APPLICATION SECURITY STRATEGY THAT EMPOWERS DEVELOPERS WITH THE ABILITY TO BUILD AND DEPLOY SOFTWARE RELEASES QUICKLY AND SECURELY

Business success today depends on developing great software, faster than ever. It drives commerce and innovation, enabling businesses to thrive, or conversely, collapse if defective. Software has become ubiquitous in almost everything we interact with; from ordering groceries to filing taxes, morphing into the digital DNA of contemporary living, omnipresent in nearly every facet of our lives.

The movement to modern software Agile and DevOps, microservices/APIs, containers, etc. is essential to achieve the velocity required to feed our growing digital appetite and drive to automation

As a result, insecure code has become a leading security risk and, increasingly, the leading business risk as well. It’s irresponsible at every level to ignore this risk while doubling-down on anti-virus solutions and firewalls — neither of which protects applications.

> “ REMEMBER, THE GOAL IS TO BE THE ATTACKER’S NIGHTMARE, NOT BE THE DEVELOPER’S NIGHTMARE OR BUSINESS PEOPLES’ NIGHTMARE.”
>
> — GUNNAR PETERSON, ARCTEC GROUP MANAGING PRINCIPAL

STEP 1

THREAT INTELLIGENCE

WHY THIS IS **CRITICAL**

Without continuously monitoring the attack surface, understanding who is attacking apps, and what techniques they are using, companies will be blindsided by attacks and waste money and time on the wrong priorities.

ASK **YOURSELF**

Are new threats, novel vulnerabilities, or new defense strategies identified by the team or the news?

What is the time between a vulnerability announcement and portfolio-wide protection? Is it getting longer or shorter?

The application security attack surface is constantly changing. New applications, new third-party products, new code, new libraries, new frameworks, and new environments make attaining a basic understanding of the application portfolio extremely challenging. Organizations should always be aware of their attack surface.

Application “Threat Intelligence” ensures the organization is continuously aware of application attackers and vulnerabilities, using both external sources of information and real data about what the organization is actually experiencing.

> “ THE TRADITIONAL HACK YOUR WAY SECURE APPROACH DOESN’T WORK AND ENGENDERS A FALSE SENSE OF SECURITY. SECURITY INVESTMENT MUST BE MADE STRATEGICALLY OVER TIME, NOT AS A KNEE-JERK RESPONSE TO THE LATEST THREAT.”
>
> — JOHN PAVONE, ASPECT SECURITY CEO

STEP 2

SECURITY ARCHITECTURE

WHY THIS IS **CRITICAL**

Without a clear definition of what security actually means and a structure to organize security priorities, security cannot be measured and will never be achieved.

ASK **YOURSELF**

Can you easily answer "How do we protect against X?"

Do you have a line-of-sight from every defense to the business reason for that defense?

Application Security Architecture manages a unified set of primary and secondary security defense strategies. Without a structure to organize application security priorities, organizations will never be able to improve. This step unifies security practices known as "business threat modeling," "application threat modeling," "security policy," "security requirements," "security test cases," and "security guidance."

There are multiple ways to organize an application Security Architecture. The simplest approach is a list that captures each high-level business concern, attack techniques, defense strategy, defense implementation, and verification technique. To ensure coverage, it may be helpful to organize these defenses and all their details into categories or into a full matrix. A more sophisticated, long-term approach is to build a hierarchical security story, organized by business threat, that captures the complexity of the company's application Security Architecture.

> “ CONTRAST SECURITY’S APPROACH TO EMBED APPLICATION SECURITY LEVERAGING INSTRUMENTATION THROUGHOUT THE SOFTWARE LIFECYCLE REPRESENTS THE FUTURE OF DEVSECOPS.”

— DAVE MCKINSTRY, SR. PROGRAM MANAGER, MICROSOFT CORPORATION

STEP 3

SECURITY RESEARCH

WHY THIS IS **CRITICAL**

If defenses aren't tested like an adversary, it will never be known whether they are strong enough to withstand real attacks.

ASK **YOURSELF**

Are researchers finding novel security issues and improvements?

Are new sensors being created and added to your Security Architecture?

Security Research actively searches for novel risks and turns them into "security as code" - automated sensors that continuously monitor and protect against these risks. Security Research focuses on expanding application coverage, code coverage, and vulnerability coverage across the entire software supply chain, including third-party software and products.

The goal is to seek out gaps, weaknesses, simplifications, and optimizations and make improvements. But Security Research isn't for managing "known" vulnerabilities. Those are already part of the Security Architecture, having been instrumented with sensors. Security Research uses techniques like the following to find "novel" security issues:

- Penetration testing
- Red teams
- Security instrumentation
- Fuzzing
- Static analysis
- Vulnerability scanning
- Policy analysis
- Bug Bounty Programs

"IF YOU HAVE CODE THAT'S IMPORTANT ENOUGH TO DEPLOY, YOU HAVE CODE THAT'S IMPORTANT ENOUGH TO INSTRUMENT."

— GENE KIM, AUTHOR, RESEARCHER, DEVOPS PIONEER AND FOUNDER OF TRIPWIRE CORPORATION

STEP 4

SECURITY INTEGRATION

WHY THIS IS **CRITICAL**

Only with vigorous monitoring can vulnerabilities across your portfolio get fixed early, when they are significantly cheaper to fix.

ASK **YOURSELF**

Are all of the applications in the portfolio automatically analyzed for vulnerabilities in code, libraries, architecture, and configurations?

Are vulnerabilities discovered and fixed as a part of normal software development, and integrated with normal development tools without security expert involvement?

Is the number of vulnerabilities being introduced more or less than the number of vulnerabilities remediated each month?

Application Security Integration ensures that software development projects are using security sensors and standard defenses to develop, deploy, and operate secure applications and APIs.

With the explosion of components, frameworks, and other libraries, gaining assurance in the software supply chain has never been more important. The challenge is ensuring that all third-party software, and how it is used, is consistent with the expected security architecture.

Contrast's vulnerability analysis is done automatically by instrumenting the running application during development, integration, or testing. The vulnerability analysis happens "in the background," and produces immediate notification of any discrepancies between the organization's security architecture and the actual implementation. When a new vulnerability is identified, Contrast automatically notifies developers using the tools they use to do their normal work. This could include a variety of channels:

- Alert or notification via Slack, HipChat, or other messaging (ChatOps)
- Email notification and status messages
- Bug report filed with JIRA, TFS, and other platforms
- Live, always up-to-date application security dashboard
- Other dashboards via REST API

> “TRYING TO BUILD SECURE APPLICATIONS WITHOUT A SET OF STRONG STANDARD DEFENSES IS LIKE TRYING TO BUILD A CAR WITH A BUNCH OF STUFF YOU FOUND AT THE JUNKYARD.”
>
> — JEFF WILLIAMS, CONTRAST SECURITY CTO

STEP 5

STANDARD DEFENSES

WHY THIS IS **CRITICAL**

Complexity is the enemy of security, and establishing strong standard defenses is the best way to reduce the mind-bending complexity of application security.

ASK **YOURSELF**

Is there an active project to build and maintain a set of standard enterprise security defenses?

Do the standard defenses cover the major security threats to the enterprise?

Are the standard defenses thoroughly security tested and easy to use?

What percentage of the application portfolio uses all the standard defenses?

Standard Defenses means that defense mechanisms like authentication, session management, access control, encryption, input validation, output escaping, error handling, and logging are correctly implemented, easy to use, resilient against attack, and kept up-to-date..

Most organizations have recognized that they should not write their own encryption. Instead, vetted implementations are used that have been scrutinized and tested by experts. This same principle applies to all application security defenses - including controls as seemingly simple as input validation, encoding, and logging - as they are critically important to stopping attacks and can be quite difficult to get correct.

By centralizing these controls and externalizing them from the application, they can be tested, managed, and maintained at the high level of quality that they require.

Defenses must:

- Be correctly implemented
- Be resistant to bypass or tampering
- Be easy for developers to find, configure, and invoke properly
- Be easy for end users to configure and use properly
- Come with sensors that verify their correct use

> “ATTACK-AWARE SOFTWARE APPLICATIONS PROVIDE ATTACK DETECTION AND REAL-TIME DEFENSIVE RESPONSE WITH A VERY LOW FALSE-POSITIVE RATE. THIS TECHNIQUE ALLOWS AN APPLICATION TO DETECT AND NEUTRALIZE A THREAT BEFORE THE ATTACKER EXPLOITS A KNOWN OR UNKNOWN VULNERABILITY.”
>
> — MICHAEL COATES, OWASP CHAIR

STEP 6

ATTACK PROTECTION

WHY THIS IS **CRITICAL**

If applications can't detect and block attempted attacks, the likelihood of a successful breach increases significantly, and nobody will ever know it happened.

ASK **YOURSELF**

Are you able to deploy defenses quickly to every application?

Can you identify and pinpoint evidence of attempted and blocked attacks down to the line of code?

Attack Protection means that the organization is continuously monitoring for attacks and has established the ability to block them. In addition, the organization has established the ability to respond to breaches quickly and thoughtfully.

Applications are going to be continuously attacked. Hence, modern applications must have the ability to detect and block their own attacks. Attempts to detect attacks outside the application at the network perimeter simply cannot hope to understand enough of the protocols, data formats, and application logic to identify anything but the most trivial attacks.

Attack Protection informs existing alerting and logging infrastructure, such as syslog, SIEM, and alerting channels to ensure an appropriate response when a successful attack is detected. Attack Protection also must prepare a plan that covers forensics, evidence preservation, public relations, notification, meeting legal requirements, insurance, data recovery, and remediation. Being ready to respond quickly can minimize much or all of the reputation damage associated with a breach, while a poorly executed response can magnify the damage.

“WITHIN DEVELOPMENT, ESPECIALLY ITERATIVE AGILE DEVELOPMENT, YOU REALLY NEED TO HAVE SECURITY BLEED INTO THE ECOSYSTEM.”

— JUSTIN SOMAINI, CHIEF TRUST OFFICER AT BOX

STEP 7

SECURITY ORCHESTRATION

WHY THIS IS **CRITICAL**

Without coordinating application security across development, operations, management, and the Board of Directors, informed decisions can't be made about risks and investments may be wrongly prioritized.

ASK **YOURSELF**

Is the Board able to understand and meaningfully contribute to security decisions?

Is there clear justification for improvement projects?

Security Orchestration is charged with making sure that the application security program is running smoothly and producing great results. There are two main parts of Security Orchestration, ensuring that the Board of Directors is aware and involved with application security, and managing priorities for the other seven steps.

Application security data should be available for reporting to senior management and the Board of Directors. The Security Orchestration group is responsible for translating this data into recommendations and prioritized initiatives to improve security for the organization.

The second priority for Security Orchestration is to manage the budget, staffing, and scheduling the initiatives chosen by management. These projects should be executed and managed like any other initiative, with a clear plan, success criteria, and appropriate resources.

“THERE IS NO TEACHER BUT THE ENEMY. NO ONE BUT THE ENEMY WILL TELL YOU WHAT THE ENEMY IS GOING TO DO. NO ONE BUT THE ENEMY WILL EVER TEACH YOU HOW TO DESTROY AND CONQUER. ONLY THE ENEMY SHOWS YOU WHERE YOU ARE WEAK. ONLY THE ENEMY TELLS YOU WHERE HE IS STRONG.”

—ORSON SCOTT CARD, ENDER’S GAME

STEP 8

SECURITY TRAINING

WHY THIS IS **CRITICAL**

Security is often quite counter-intuitive, so it's unfair to expect development and operations teams to create and operate security applications without training in how to do that.

ASK **YOURSELF**

What percentage of the development and operations team has been trained in secure coding?

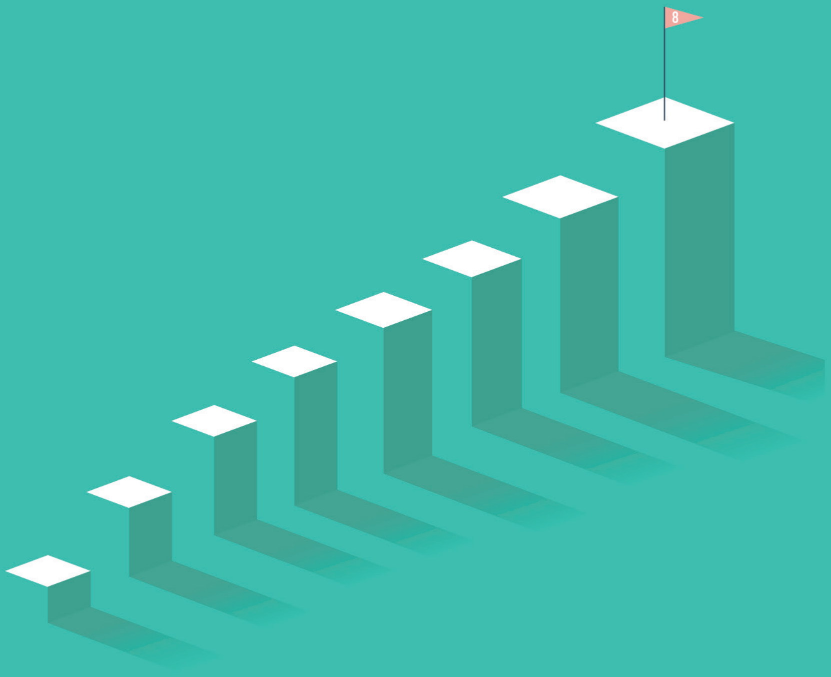
What are the average scores students receive on post-training tests?

What is the average delta between pre-and post-training tests?

Security Training ensures everyone understands why application security is important to the business, how the application security program actually works, and what everyone's individual responsibilities are. In addition, training is a good way to familiarize staff with the organization's Security Architecture and to ensure that they know when to use defenses and how to use them correctly.

The first level of Security Training happens automatically as Contrast Enterprise with IAST provides instant feedback as developers do their normal work. This "micro-training" happens directly in people's work environments, such as a developer's IDE, QA environment, or bug tracker. Automated analysis and instant notifications allow development and operations to adjust their behavior and correct security mistakes when they cost almost nothing to fix. Notification leverages the organization's existing infrastructure, such as email, Slack, HipChat, and PagerDuty.

New additions are being made to the security architecture all the time. Getting an expert to do a briefing, video, or blog about the new threat, vulnerability, or defense is a great way to keep the staff up to date on the latest security information. Briefings should be tailored to the organization and must include defense details in addition to threat and vulnerability information. An occasional memo or speech emphasizing the importance of security should be published by a senior executive to keep everyone aligned.



CONTRAST SECURITY

240 3rd Street
Los Altos, CA 94022
888.371.1333

Contrast Security is the world's leading provider of security technology that enables software applications to protect themselves against cyberattacks, heralding the new era of self-protecting software. Contrast's patented deep security instrumentation is the breakthrough technology that enables highly accurate assessment and always-on protection of an entire application portfolio, without disruptive scanning or expensive security experts. Only Contrast has sensors that work actively inside applications to uncovervulnerabilities, prevent data breaches, and secure the entire enterprise from development, to operations, to production.

11/12/19