

Keto AppSec: It's All About the FATS

David Lindner, Director, Application Security

March 27, 2020

WHO IS THIS GUY?



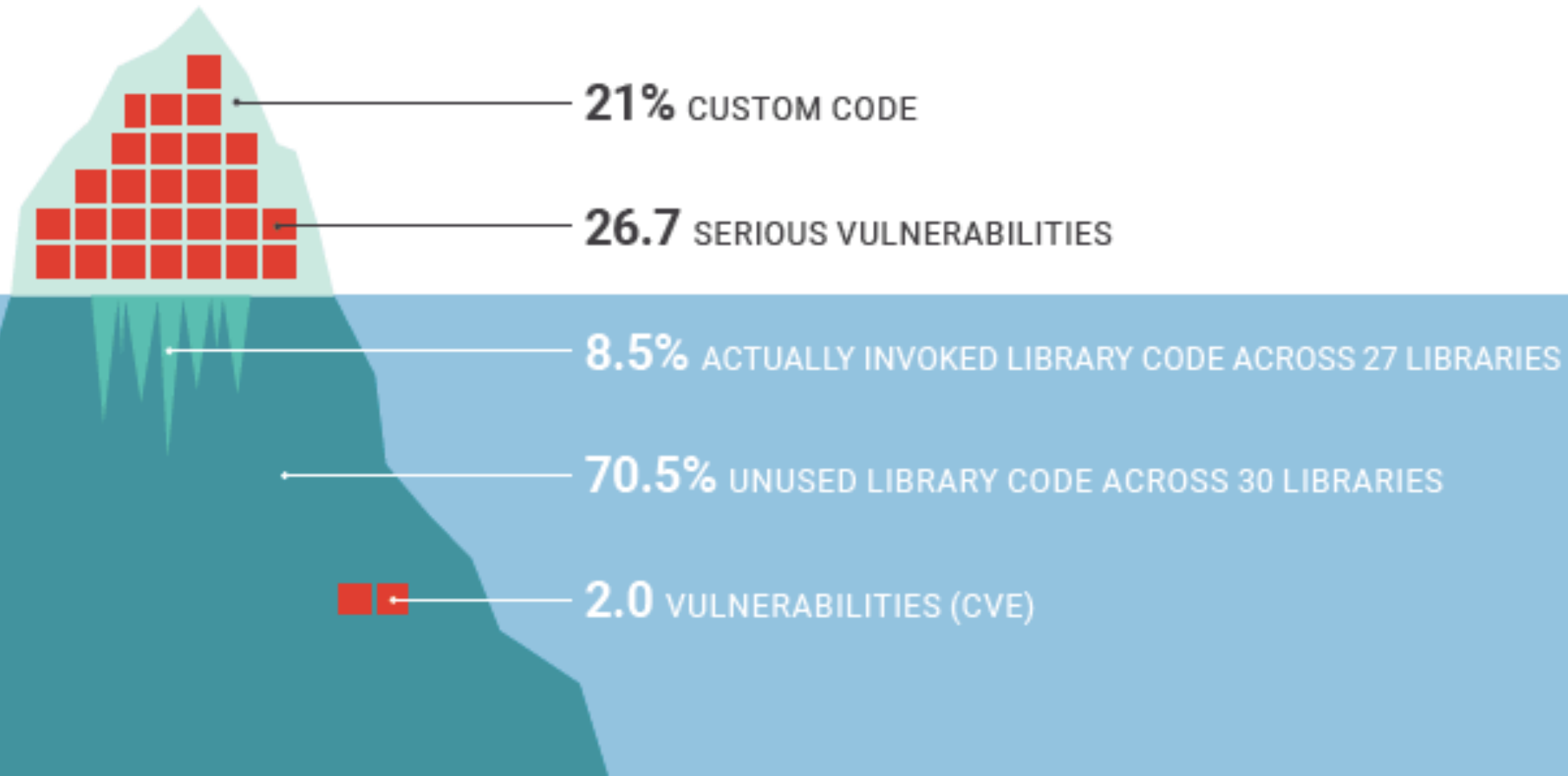
```
class Speaker {  
    let name = "David Lindner"  
    let title = "Director, Application Security"  
    let company = "Contrast Security"  
    let twitter = "@golfhackerdave"  
    var hobbies = ["Dadding", "Golfing", "IoT/Mobile",  
        "Fishing", "Hawkeyes"]  
}
```


A close-up, high-angle shot of a shark's head as it breaks the surface of the water. The shark's mouth is wide open, revealing a row of sharp, white teeth. The water is dark and turbulent, with white foam and splashes around the shark's head. The shark's skin is a mottled grey-brown color.

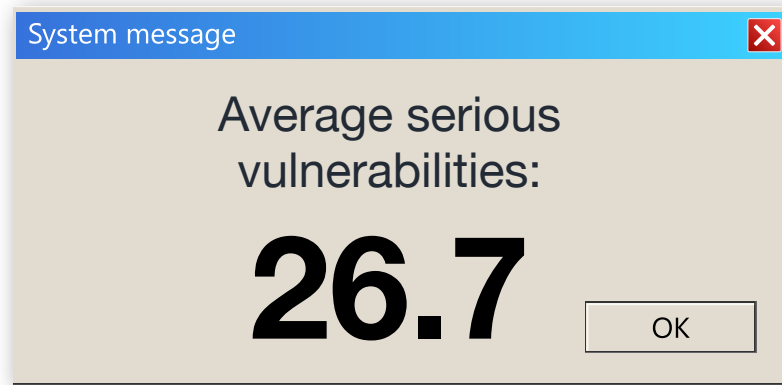
Not so breaking news

Software Applications are vulnerable...and they are being attacked.

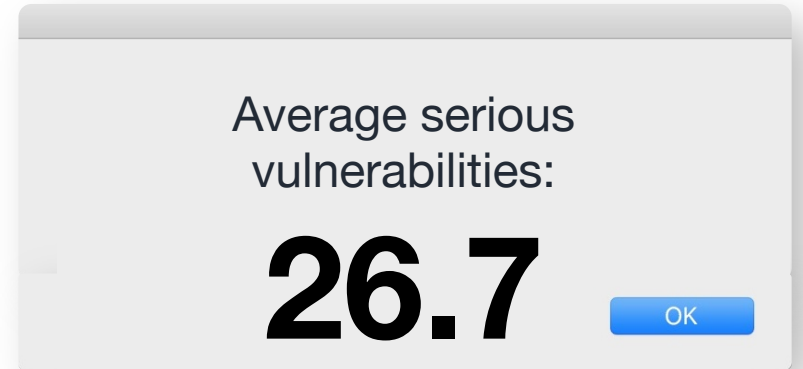
The Average Application



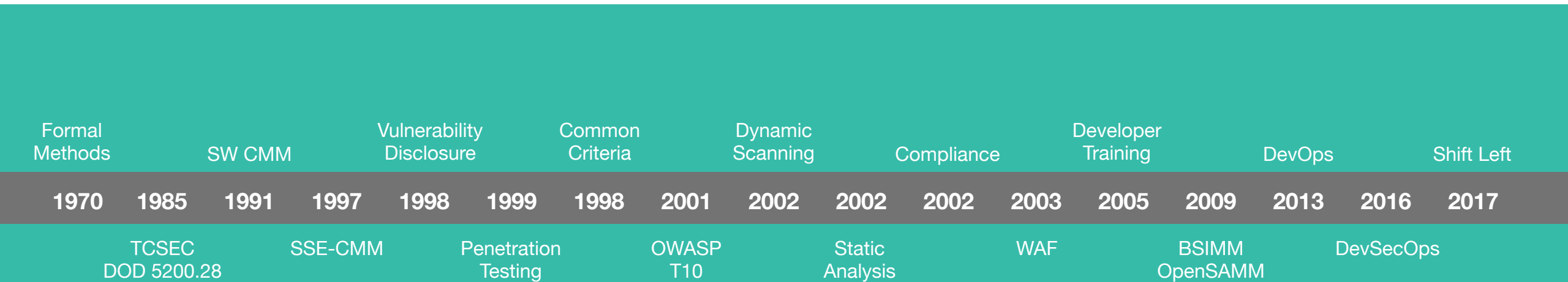
Software Security Crisis



2000

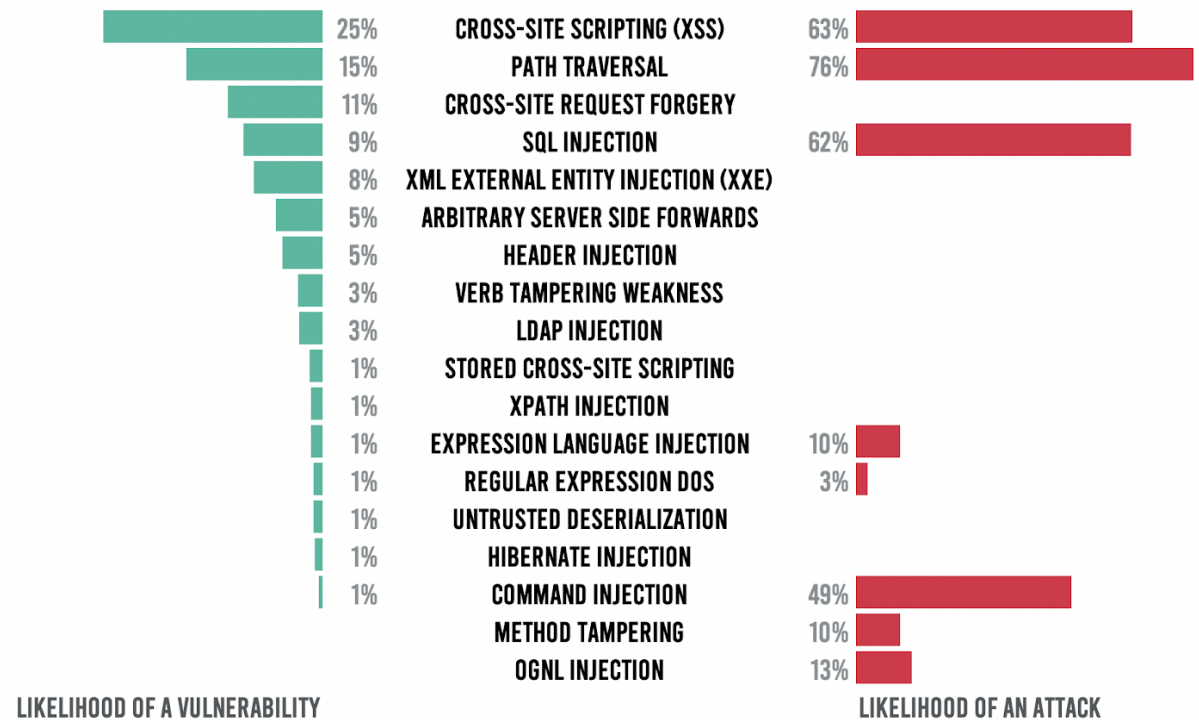


2019



Likelihood your application/api gets attacked

Jan/Feb 2020



Hackers are Exploiting the Lag...

How Fast Can you Respond?

March 7
CVE-2017-5638
Disclosed, Apache
releases fixed version

Mid-May
Equifax
breach
occurs

July 29
Equifax
learns of
breach

Sept 7
Equifax discloses,
Four more Struts2
CVEs disclosed

No Updates

No Detection

Disaster

March 8
Widespread attack
probes observed

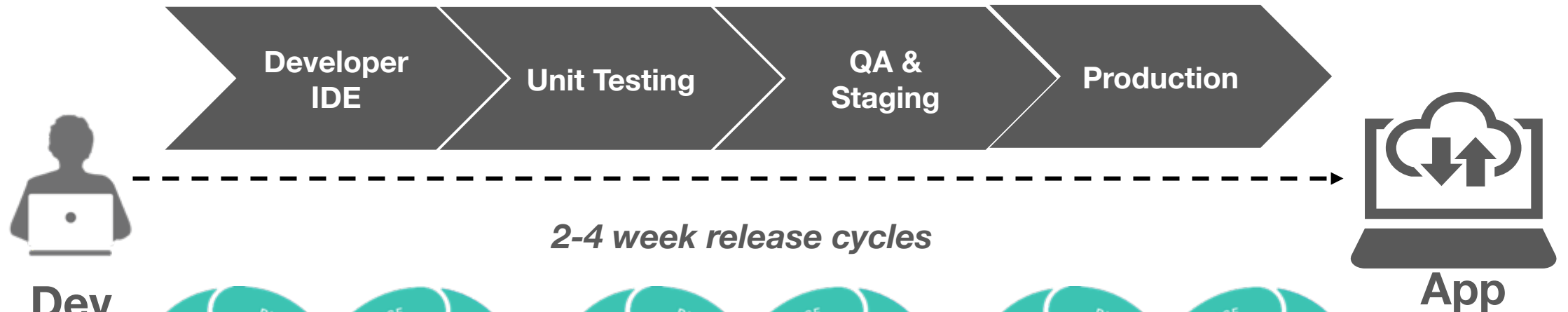


Software
development
continues to
accelerate...and
leverage new
approaches.

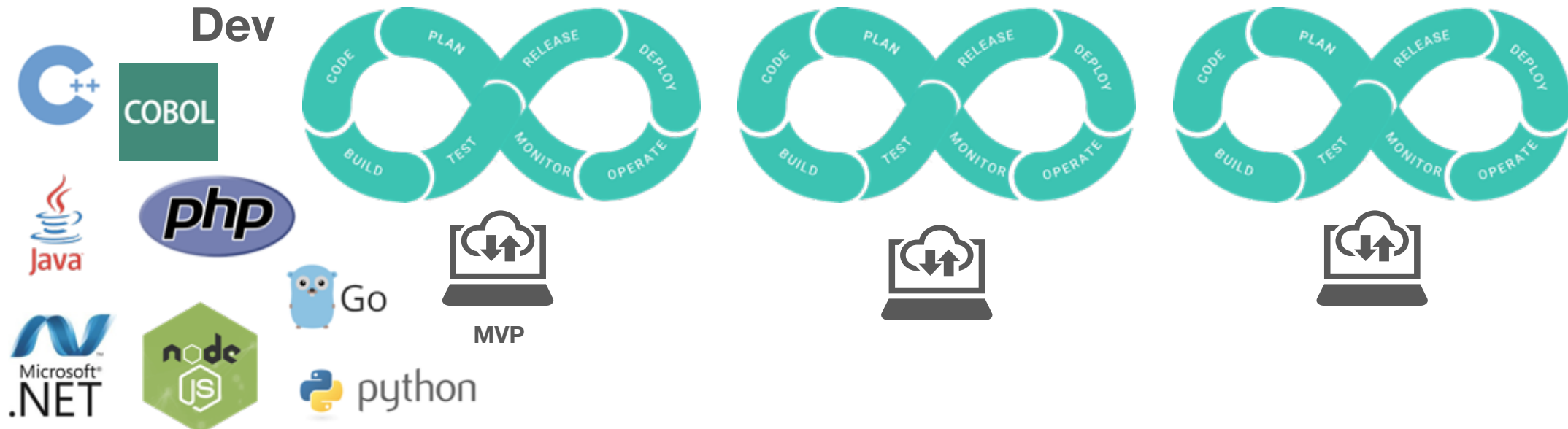
Not so breaking news #2

Fundamental change on the path to an application

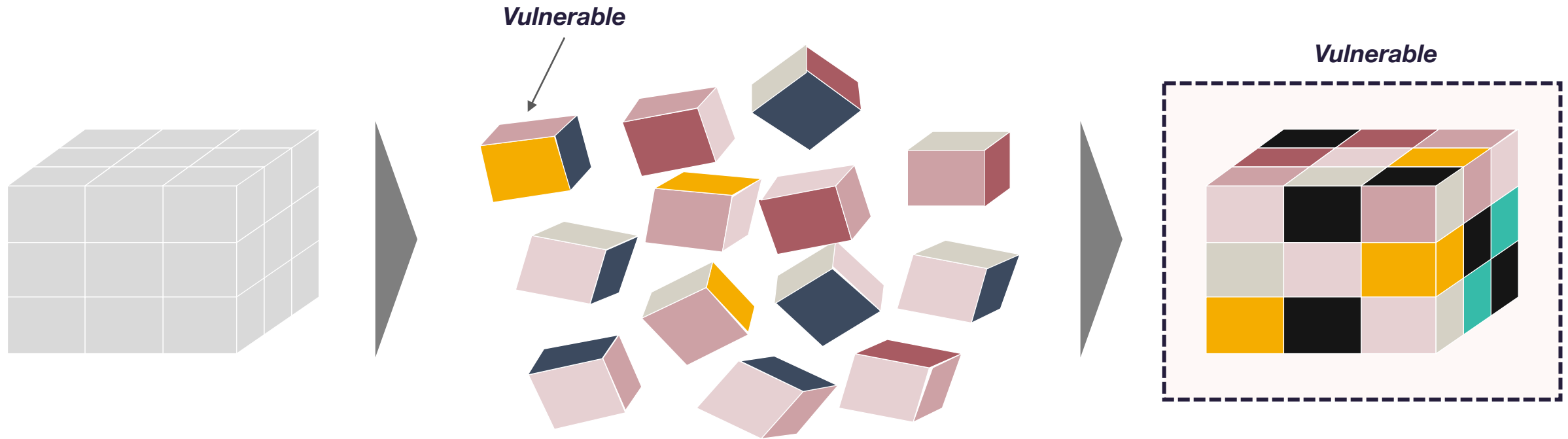
3-12 month release cycles



2-4 week release cycles

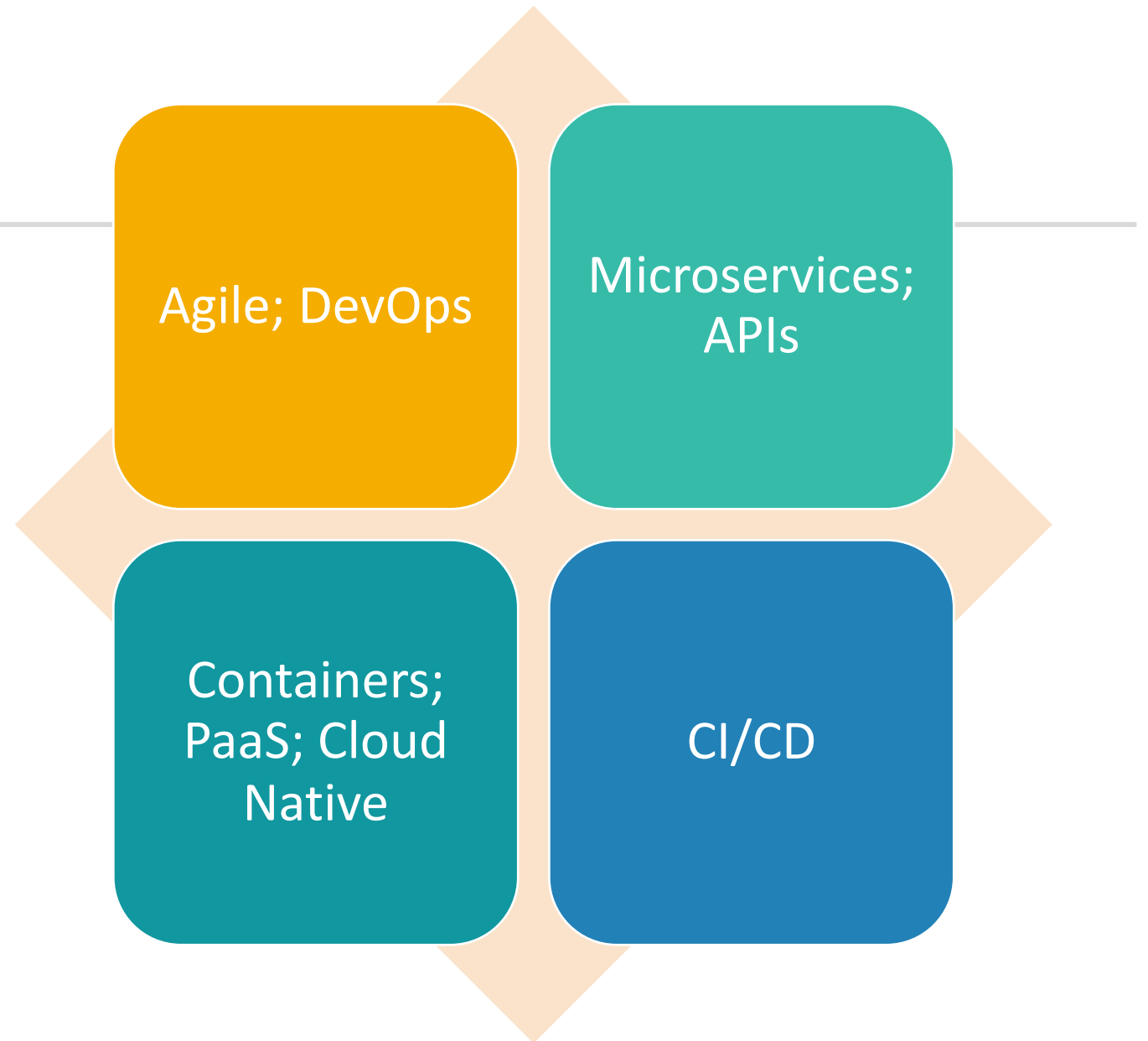


The (other) reality of software today



Vulnerable components = exposed software = higher (inherited) risk

Software Approaches Change Rapidly

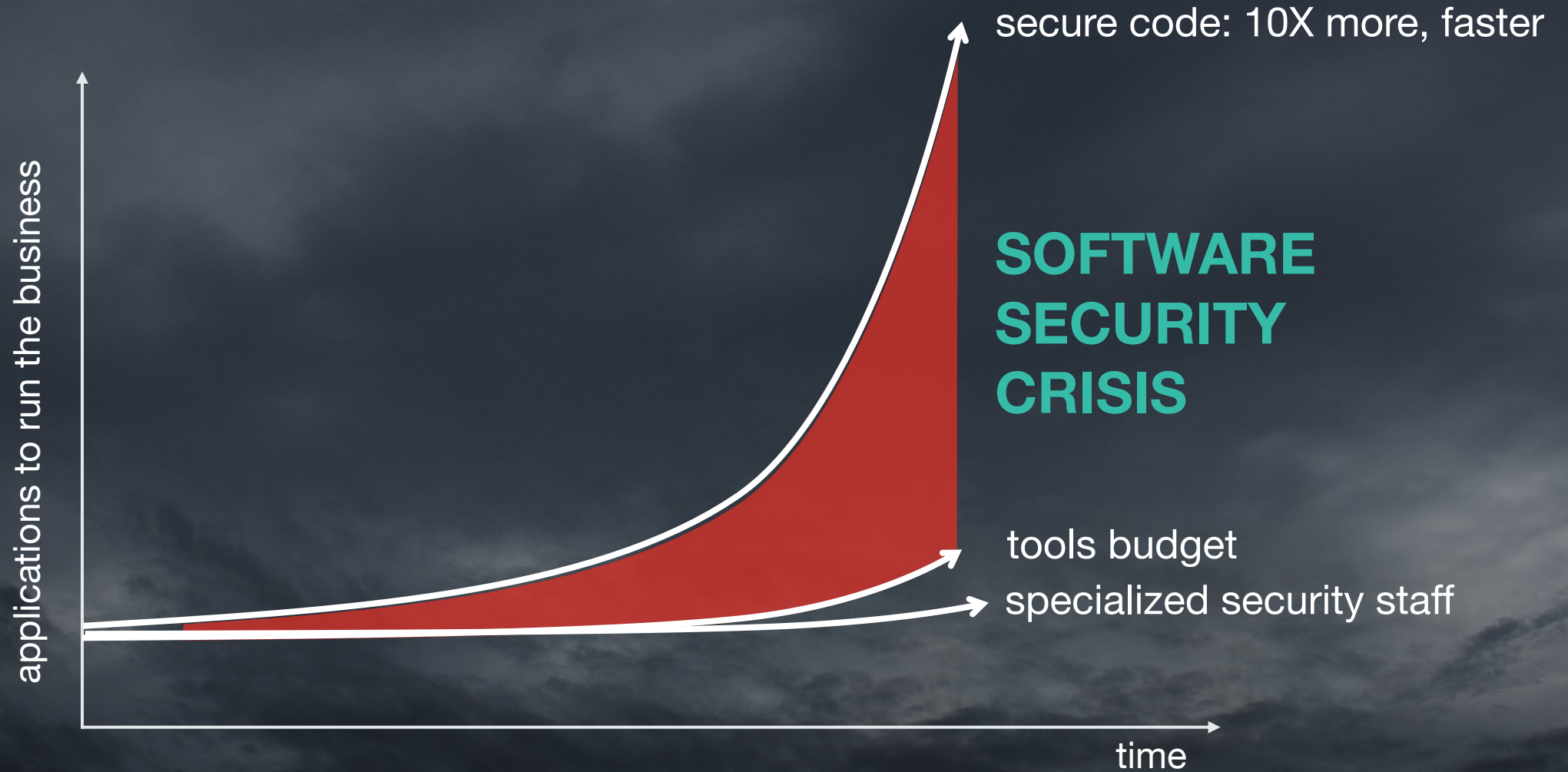


Out of 122 BSIMM 10 organizations



- 1.37% software security group to developers
- That's 1 software security professional to every 73 developers

IMPOSSIBLE ECONOMICS: SOFTWARE SECURITY



A scenic photograph of a waterfall cascading over a mossy cliff. A vibrant rainbow is visible in the lower-left foreground, partially obscured by mist rising from the base of the waterfall. The text "The OLD way" is centered over the image in a white, serif font.

The OLD way

The OLD way



I have 1500 applications



THEY ALL MUST BE
TESTED

Manual tests
SAST/DAST



Stop development
while we find
problems

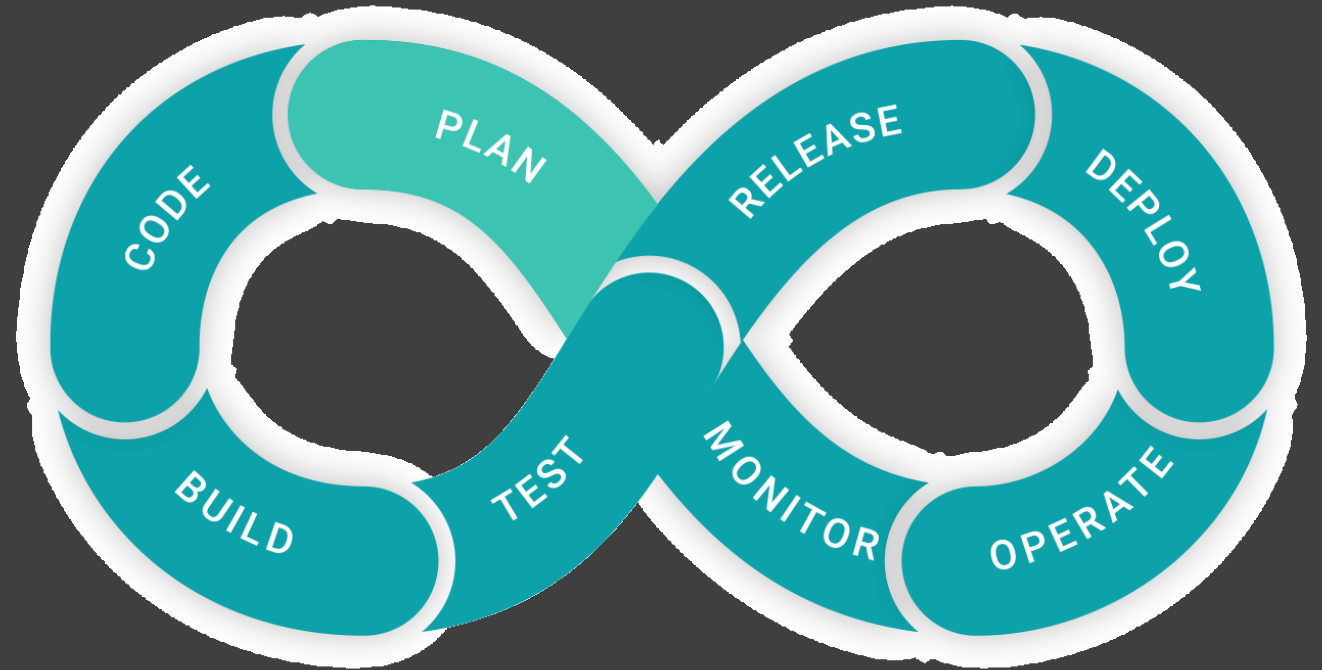
Where could
we go wrong
with this?

7-(11)-7

The OLD way

- Security is seen as a blocker
- Everything is fought
- Reports go “missing”
 - Security debt increases
- Security posture is unknown except when report was created

The OLD way





Result of the OLD way - Gating

Security has the exact problems development had

- **Problem:** **software** is poor quality, late, slow, and doesn't provide business value.
- **Proven Approach:** DevOps
- **Result:**
 - 5x lower change failure rate
 - 96x faster MTTR service
 - 2x likely to exceed business goal

- **Problem:** **security** is poor quality, late, slow, and doesn't provide business value.
- Possible Approach: DevSecOps
- **Desired Result:**
 - 10x increase in portfolio coverage?
 - 80% reduction in vulns to prod?
 - 0x increase in time to market



The existence of insecure software has so far helped society far more than it has harmed it.

- Daniel Miessler
- <https://danielmiessler.com/blog/the-reason-software-remains-insecure/>

WHY SOFTWARE REMAINS INSECURE

The societal gains
provided by all software

EXCEL
THE INTERNET
MOBILE PHONES
GPS
ONLINE SHOPPING
CLOUD COMPUTING
VIDEO CONFERENCING
GOING TO THE MOON
MAINFRAMES
ARTIFICIAL INTELLIGENCE
LINUX
WORD PROCESSING
WINDOWS
ANDROID
IOS
EXPLORING THE SOLAR SYSTEM
NETFLIX
AWS

SOFTWARE'S WIN/LOSS LEDGER

BENEFIT TO HUMANITY	UNFATHOMABLE
PEOPLE KILLED BY BAD SOFTWARE	BASICALLY ZERO
TIMES THE INTERNET CRASHED	BASICALLY NEVER
CHANCE OF LIVING WITHOUT IT	ZERO
NUMBER OF PEOPLE HELPED	BILLIONS

The societal problems
caused by bad software

ANNOYANCE
OCCASIONAL DDOS
SLIGHT PROFIT IMPACT



How can we deliver 10X
more secure code that
protects the integrity of
the business?



How can we focus and do things securely faster?

A modern office interior with a teal overlay. The scene shows a long conference table with several chairs, a wall with a grid pattern, and large windows in the background. The text "FATS" and "F is for Frameworks" is centered in the image.

FATS

“F is for Frameworks”



What do frameworks do for us?

- REACT and Angular
 - XSS Protections by default
- Node
 - helmet
 - csrf
- Ruby on Rails
 - protect_from_forgery with: :exception
 - Mass assignment is pretty much fixed
 - devise or authlogic password storage
- Go
 - gorilla/csrf
 - gorilla/securecookie
 - crypto.random
 - html/template
- PHP Laravel
 - Salted/hased passwords with bcrypt
 - Prepared Statements
 - Mass Assignment protections

What does it mean?



- Know your frameworks
- Customize your testing
- Focus on the things that you aren't protected from

A modern office interior with a teal overlay. The scene shows a long conference table with several chairs, a wall with a grid pattern, and large windows in the background. The text "FATS" and "A is for Automation" is centered in the image.

FATS

"A is for Automation"



LEGACY TOOL QUAGMIRE

Disparate, static, disconnected, inaccurate; requires an army of specialists to interpret results



IDE
Spellcheckers



SCA



SAST
Full Scan



Manual
Pentesting



NGWAF



Manual
Code
Review



SAST
Quick Scan



DAST



Fuzzing



WAF



IPS

Modern software tools work differently

Collaborative, real-time, full lifecycle, integrated, and social

YOUR SOFTWARE PROCESS AND PIPELINE

BUILD



QUALITY



PERFORMANCE



COLLABORATION

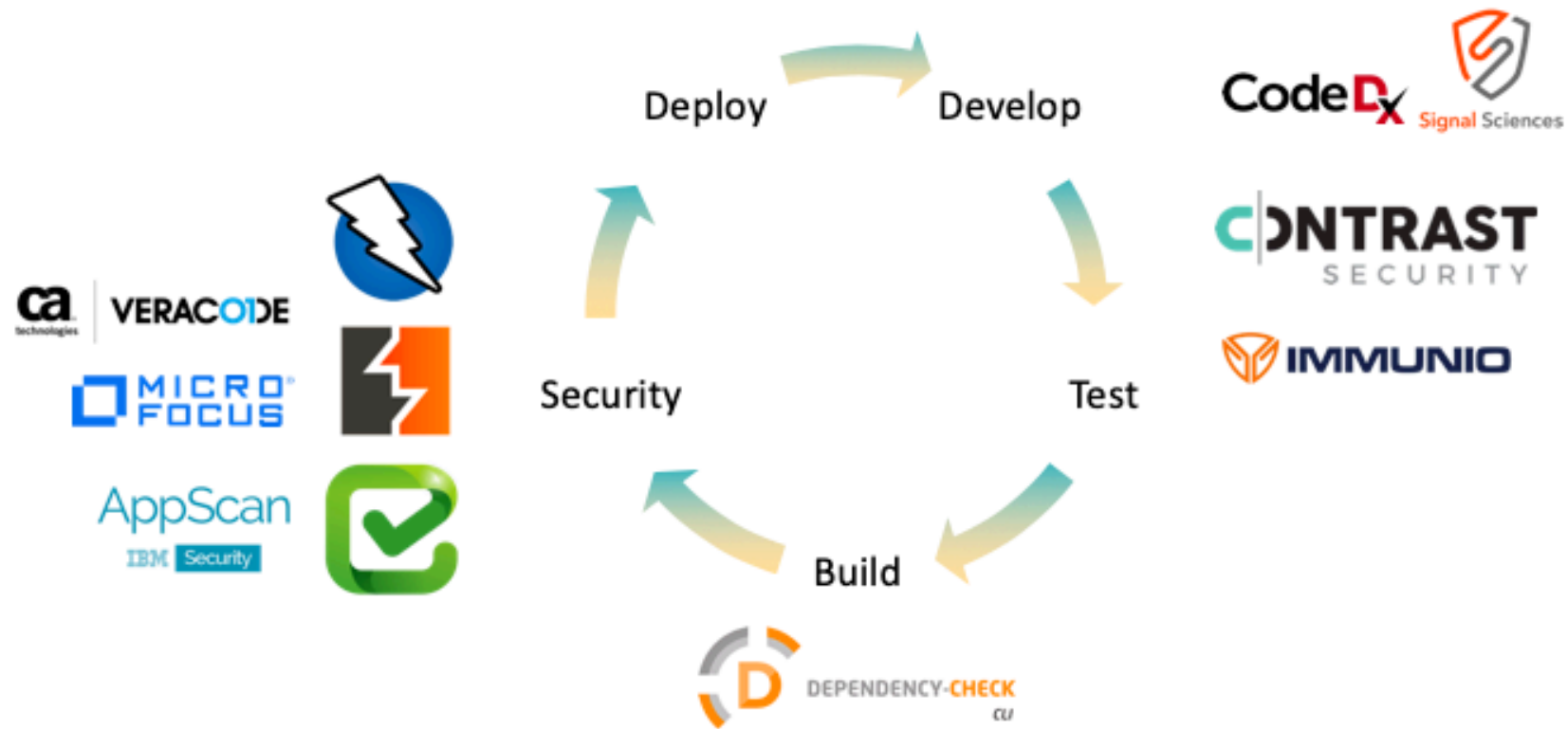


ANALYTICS



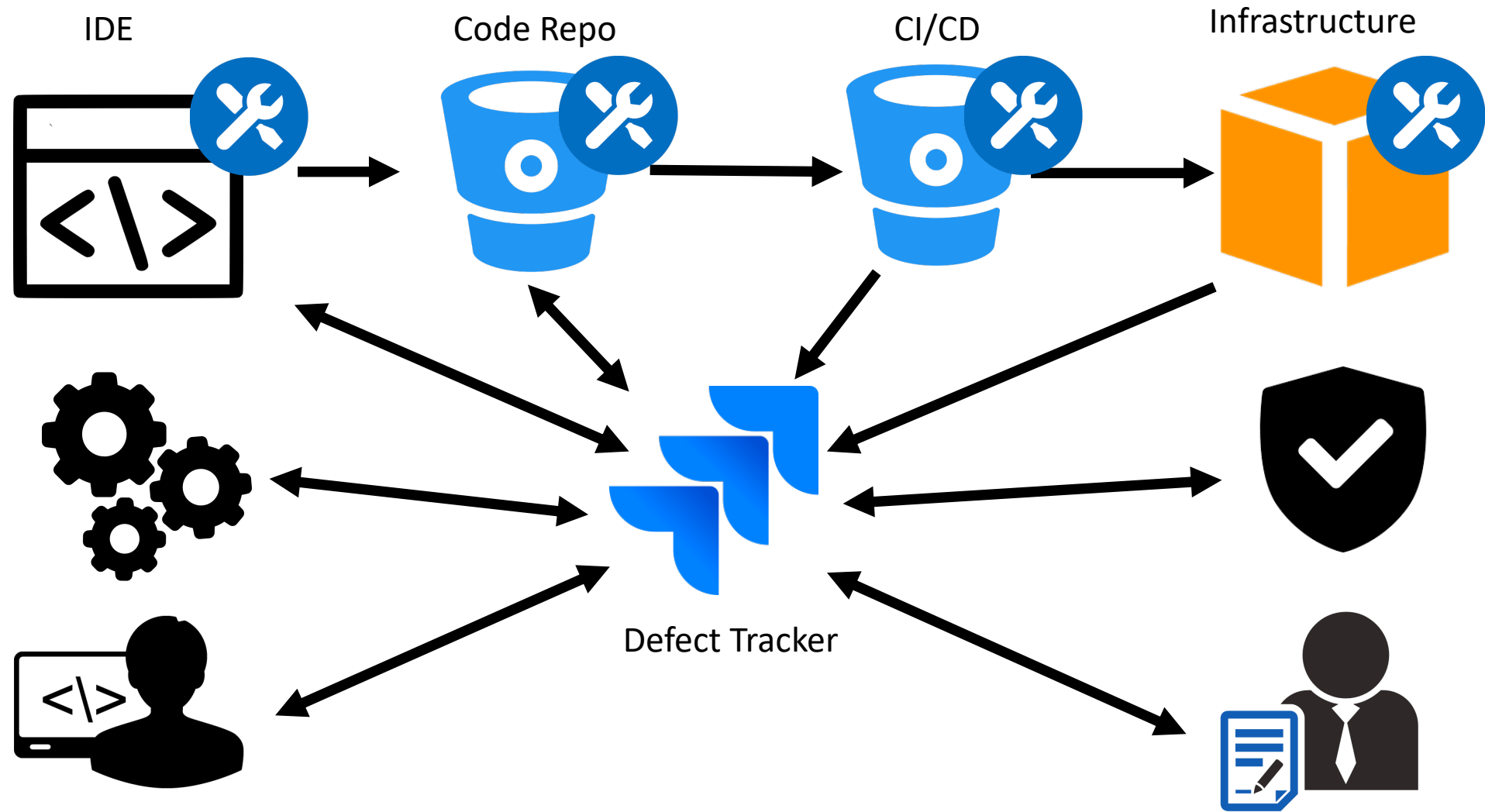
**SOFTWARE
SECURITY**





Lots of security tooling

Need to Streamline



Dev: how we use tools and automation to secure code



Our dev setup

PHILOSPHY

- Automated from the Beginning, Keep it Small, Boring Releases

TOOLING

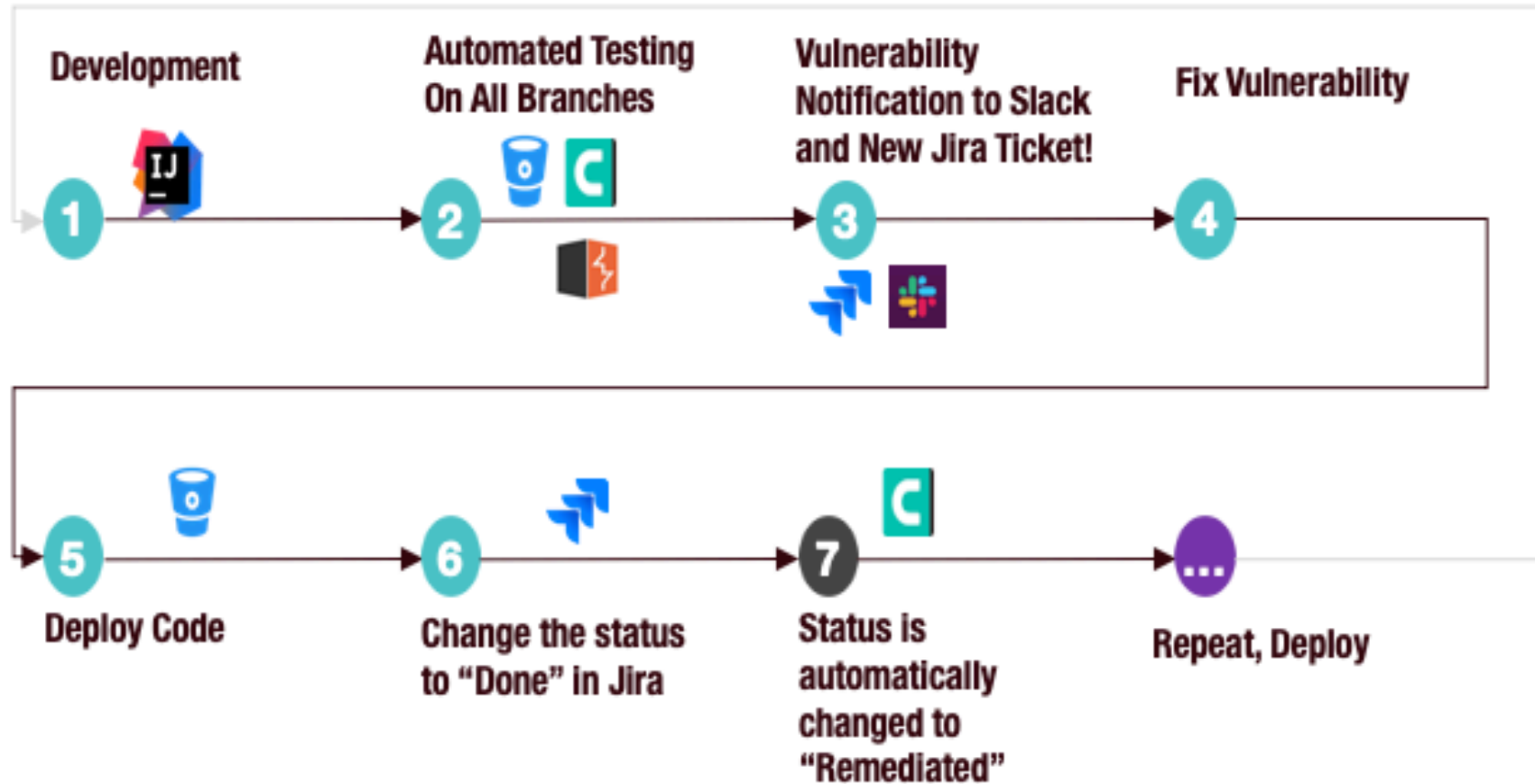
- IDE: IntelliJ
- CI/CD/SCM: Bitbucket Pipelines
- Artifact Repository: Artifactory
- ChatOps: Slack
- Automated Scans: Burp Enterprise (COMING SOON)
- Bug tracking: JIRA
- AppSec: Contrast Assess and Protect

SETUP

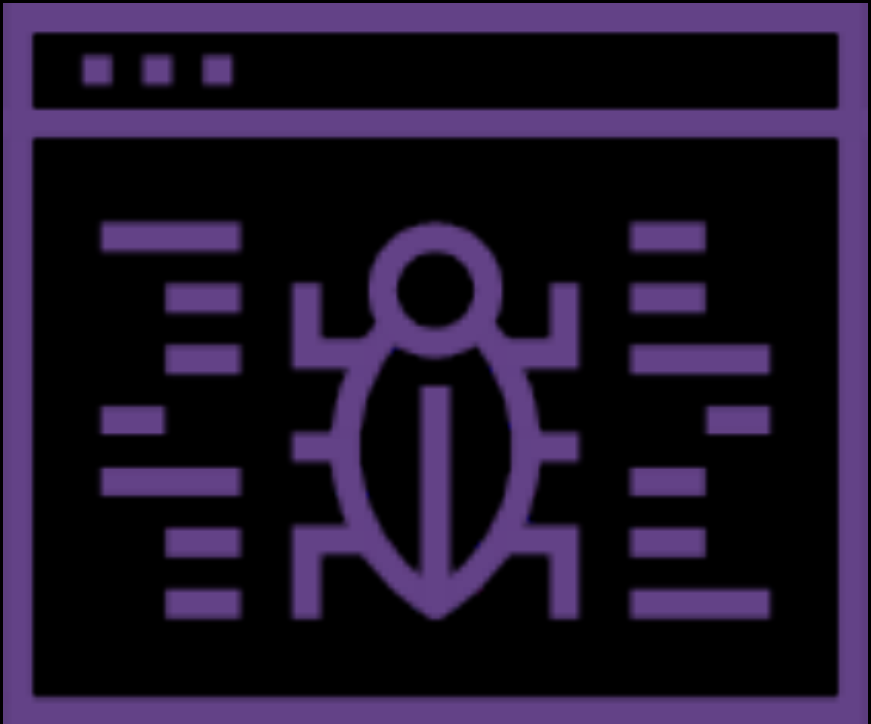
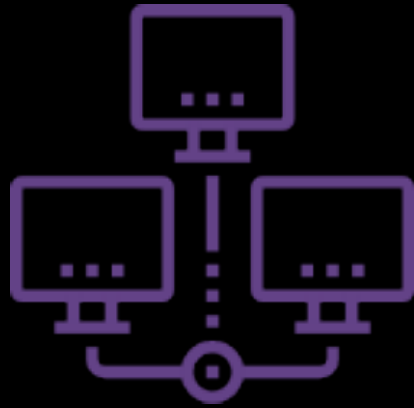
- Run pipeline on all branches; Maven plugin to configure and include Java Agent



Our dev workflow



What are we trying to achieve



- Identify vulnerabilities at DevOps speed
- Accurate results
- Simplified and integrated AppSec
- Continuous coverage
- Automation
- Application intelligence
- Smart response and 0-day protection
- Security anywhere





What if you could kill entire vulnerability classes with automation?

- XSS
- SQL/NoSQL Injection
- Command Injection
- CSRF
- EL/OGNL Injection
- Untrusted Deserialization
- XXE
- Padding Oracle



Empower Development to Weave Security In

- Expanding Security beyond the InfoSec/AppSec team
 - Security Champions within Development, Architecture & Leadership
- Keys to Success:
 - Self-selection
 - Visibility & Praise
 - Incentives

A modern office interior with a teal overlay. The scene shows a long conference table with several chairs, a wall with a grid pattern, and large windows in the background. The text "FATS" and "T is for Threats" is centered in the image.

FATS

"T is for Threats"



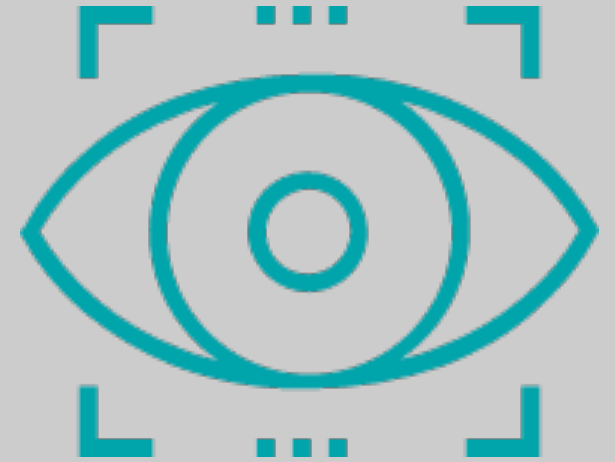
Managing Risks/Threats/Attacks

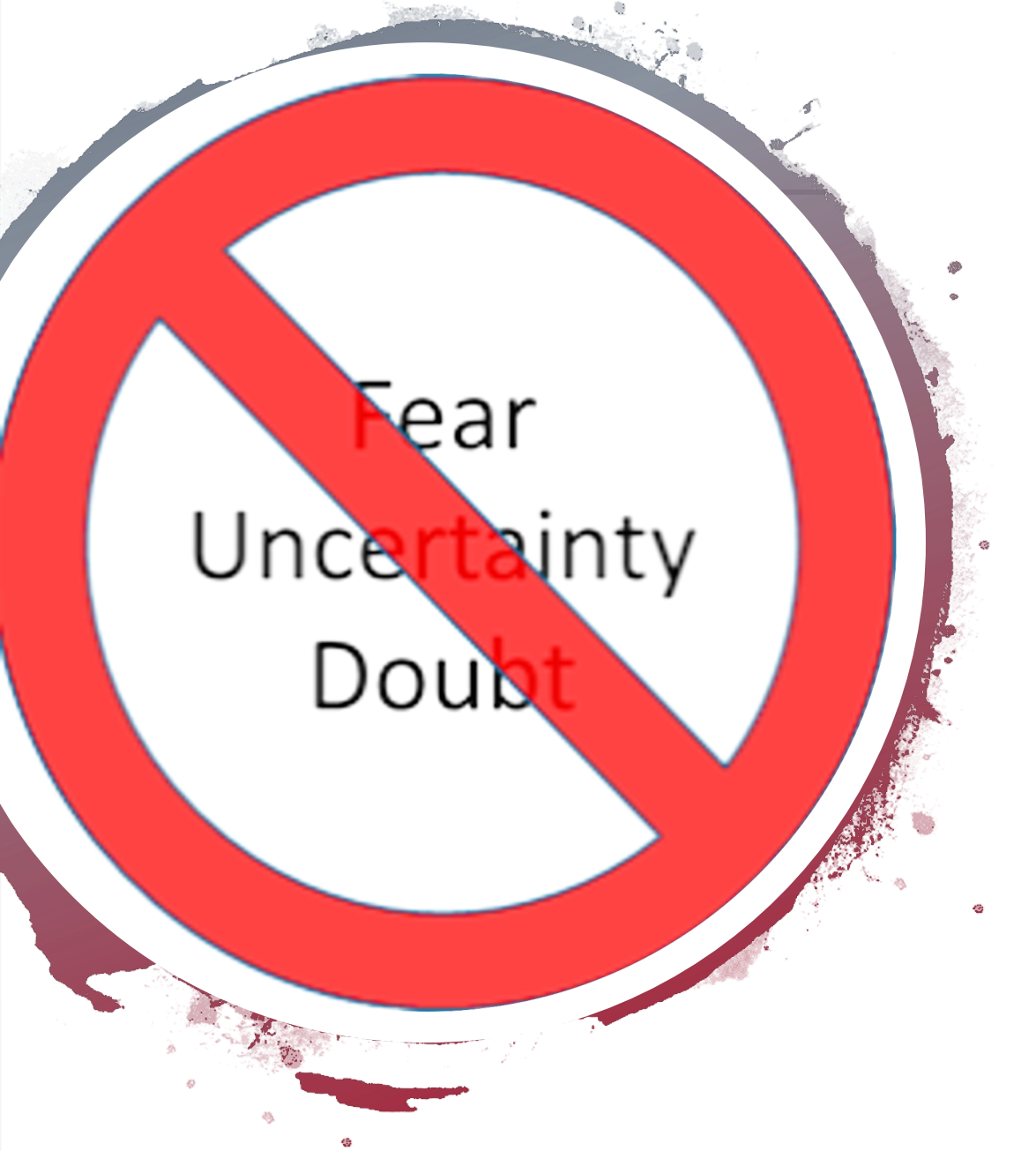
- Risk rating
- ASVS – helps with rigor
- CVE and issues monitoring
- Threat Intelligence



Software Composition Analysis (SCA)

- Fully automated solution
- Runtime assessment and protection
- Continuous visibility
- Self updating risk intelligence
- Single solution for all your code





Manage REAL Threats

- FUD no more
- Threat Intelligence
 - WAF or RASP data
 - Intelligence tools?
 - Other indicators
- Predictive Analysis
- For instance XSS

What's not FUD?

SQL Injection

- https://en.wikipedia.org/wiki/SQL_injection#Examples

Untrusted Deserialization

- WebLogic RCE - <https://nvd.nist.gov/vuln/detail/CVE-2019-2725>
- Struts 2 - <https://nvd.nist.gov/vuln/detail/CVE-2017-9805>
 - Equifax

OGNL Injection

- Struts 2 - <https://nvd.nist.gov/vuln/detail/CVE-2018-11776>

XSS - .09% CVSS 5 and up

Security Vulnerabilities Related To CWE-79

Scores Greater Than: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[Results](#) [Download Results](#)

CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication
CVE-2019-1020019	79		XSS	2019-07-29	2019-07-31	4.3	None	Remote	Medium	Not required
rio-previewer before 1.0.0a12 allows XSS.										
CVE-2019-1020010	79		XSS	2019-07-29	2019-09-05	4.3	None	Remote	Medium	Not required
key before 10.102.4 allows hijacking a user's token.										
CVE-2019-1020008	79		XSS	2019-07-29	2019-07-31	4.3	None	Remote	Medium	Not required
table.js before 1.0.4 allows XSS.										
CVE-2019-1020007	79		XSS	2019-07-29	2019-07-30	3.5	None	Remote	Medium	Single system
endency-Track before 3.5.1 allows XSS.										
CVE-2019-1020005	79		XSS	2019-07-29	2019-08-01	3.5	None	Remote	Medium	Single system
rio-communities before 1.0.0a20 allows XSS.										
CVE-2019-1020003	79		XSS	2019-07-29	2019-08-01	3.5	None	Remote	Medium	Single system
rio-records before 1.2.2 allows XSS.										
CVE-2019-1010314	79		XSS	2019-07-11	2019-07-12	4.3	None	Remote	Medium	Not required
a 1.7.2, 1.7.3 is affected by: Cross Site Scripting (XSS). The impact is: execute JavaScript in victim's browser, when the vulnerable repo page is loaded. The component is: repository's descr or is: victim must navigate to public and affected repo page.										
CVE-2019-1010307	79		XSS	2019-07-15	2019-07-18	3.5	None	Remote	Medium	Single system
GLPI Product 9.3.1 is affected by: Cross Site Scripting (XSS). The impact is: All dropdown values are vulnerable to XSS leading to privilege escalation and executing js on admin. The comp /ajax/getDropDownValue.php. The attack vector is: 1- User Create a ticket , 2- Admin opens another ticket and click on the "Link Tickets" feature, 3- a request to the endpoint fetches js and										
CVE-2019-1010287	79		Exec Code XSS	2019-07-17	2019-07-22	4.3	None	Remote	Medium	Not required
sheet Next Gen 1.5.3 and earlier is affected by: Cross Site Scripting (XSS). The impact is: Allows an attacker to execute arbitrary HTML and JavaScript code via a "redirect" parameter. The form: login.php, lines 40 and 54. The attack vector is: reflected XSS, victim may click the malicious url.										
CVE-2019-1010261	79		XSS	2019-07-18	2019-07-19	4.3	None	Remote	Medium	Not required
a 1.7.0 and earlier is affected by: Cross Site Scripting (XSS). The impact is: Attacker is able to have victim execute arbitrary JS in browser. The component is: go-get URL generation - PR to s://github.com/go-gitea/gitea/pull/5905. The attack vector is: victim must open a specifically crafted URL. The fixed version is: 1.7.1 and later.										
CVE-2019-1010247	79		XSS	2019-07-19	2019-08-23	4.3	None	Remote	Medium	Not required
rtZone IAM mod_auth_openidc 2.3.10.1 and earlier is affected by: Cross Site Scripting (XSS). The impact is: Redirecting the user to a phishing page or interacting with the application on bel onent is: File: src/mod_auth_openidc.c, Line: 3109. The fixed version is: 2.3.10.2.										
CVE-2019-1010237	79		Exec Code XSS	2019-07-22	2019-10-09	4.3	None	Remote	Medium	Not required
5.3 before 5.3.12; 5.2 before 5.2.21 is affected by: Cross Site Scripting (XSS) - CWE-79 Type 2: Stored XSS (or Persistent). The impact is: Execute code in the victim's browser. The compo QuestionPool. The attack vector is: Cloze Test Text gap (attacker) / Corrections view (victim). The fixed version is: 5.3.12.										
CVE-2019-1010235	79		XSS	2019-07-22	2019-07-23	3.5	None	Remote	Medium	Single system
CMS 1.1 is affected by: Cross Site Scripting (XSS). The impact is: Cookie stealing, Alert pop-up on page, Redirecting to another phishing site, Executing browser exploits. The component is:										
CVE-2019-1010207	79		XSS	2019-07-23	2019-07-29	4.3	None	Remote	Medium	Not required
stechsolutions Pie Register 3.0.15 is affected by: Cross Site Scripting (XSS). The impact is: Stealing of session cookies. The component is: File: Login. Parameters: interim-login, wp-lang, an k vector is: If a victim clicks a malicious link, the attacker can steal his/her account. The fixed version is: 3.0.16.										



SQL Injection - 97% CVSS 6 and up

Security Vulnerabilities Related To CWE-89

CVSS Scores Greater Than: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-1010259	89		Sql	2019-07-18	2019-08-13	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
SaltStack Salt 2018.3, 2019.2 is affected by: SQL Injection. The impact is: An attacker could escalate privileges on MySQL server deployed by cloud provider. It leads to RCE. The component is: The mysql.user_chpass function from the MySQL module for Salt. The attack vector is: specially crafted password string. The fixed version is: 2018.3.4.														
2	CVE-2019-1010248	89		Sql	2019-07-18	2019-07-23	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Synetics GmbH I-dolt 1.12 and earlier is affected by: SQL Injection. The impact is: Unauthenticated mysql database access. The component is: Web login form. The attack vector is: An attacker can exploit the vulnerability by sending a malicious HTTP POST request. The fixed version is: 1.12.1.														
3	CVE-2019-1010201	89		Sql	2019-07-23	2019-07-24	4.0	None	Remote	Low	Single system	Partial	None	None
Jeesite 1.2.7 is affected by: SQL Injection. The impact is: sensitive information disclosure. The component is: updateProcInsIdByBusinessId() function in src/main/java/com.thinkgem.jeesite/modules/act/ActDao.java has SQL Injection vulnerability. The attack vector is: network connectivity,authenticated. The fixed version is: 4.0 and later.														
4	CVE-2019-1010191	89		Sql	2019-07-24	2019-07-29	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
marginallia < 1.6 is affected by: SQL Injection. The impact is: The impact is a injection of any SQL queries when a user controller argument is added as a component. The component is: Affects users that add a component that is user controller, for instance a parameter or a header. The attack vector is: Hacker inputs a SQL to a vulnerable vector(header, http parameter, etc). The fixed version is: 1.6.														
5	CVE-2019-1010153	89		Sql	2019-07-23	2019-07-24	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
zcms 8.3 and earlier is affected by: SQL Injection. The impact is: sql inject. The component is: zs/subzs.php.														
6	CVE-2019-1010148	89		Exec Code Sql	2019-07-23	2019-07-24	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
zcms version 8.3 and earlier is affected by: SQL Injection. The impact is: zcms File Delete to Code Execution.														
7	CVE-2019-1010104	89		Sql	2019-07-18	2019-07-23	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
TechyTalk Quick Chat WordPress Plugin All up to the latest is affected by: SQL Injection. The impact is: Access to the database. The component is: like_escape is used in Quick-chat.php line 399. The attack vector is: Crafted ajax request.														
8	CVE-2019-1010034	89		Sql	2019-07-15	2019-08-21	4.0	None	Remote	Low	Single system	Partial	None	None
Deepwoods Software WebLibrarian 3.5.2 and earlier is affected by: SQL Injection. The impact is: Exposing the entire database. The component is: Function "AllBarCodes" (defined at database_code.php line 1018) is vulnerable to a boolean-based blind sql injection. This function call can be triggered by any user logged-in with at least Volunteer role or manage_circulation capabilities. PoC : /wordpress/wp-admin/admin.php?page=weblib-circulation-desk&orderby=title&order=DESC.														
9	CVE-2019-17429	89		Sql	2019-10-10	2019-10-11	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Adhouma CMS through 2019-10-09 has SQL Injection via the post.php p_id parameter.														
10	CVE-2019-17419	89		Sql	2019-10-09	2019-10-10	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
An issue was discovered in MetInfo 7.0. There is SQL injection via the admin/?n=user&c=admin_user&a=doGetUserInfo id parameter.														
11	CVE-2019-17418	89		Sql	2019-10-09	2019-10-10	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
An issue was discovered in MetInfo 7.0. There is SQL injection via the admin/?n=language&c=language_general&a=doSearchParameter appno parameter, a different issue than CVE-2019-16997.														
12	CVE-2019-17319	89		Sql	2019-10-07	2019-10-09	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Emails module by a Regular user.														
13	CVE-2019-17318	89		Sql	2019-10-07	2019-10-09	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the pmse_Inbox module by a Regular user.														
14	CVE-2019-17298	89		Sql	2019-10-07	2019-10-09	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Administration module by a Developer user.														
15	CVE-2019-17297	89		Sql	2019-10-07	2019-10-09	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Quotes module by a Regular user.														
16	CVE-2019-17296	89		Sql	2019-10-07	2019-10-09	6.5	None	Remote	Low	Single system	Partial	Partial	Partial

CMD Injection 95% CVSS 6 and up

Security Vulnerabilities Related To CWE-77

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

Total number of vulnerabilities : **489** Page : **1** (This Page) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#)

[Cvov Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access
1	CVE-2019-1010306	77		Exec Code	2019-07-15	2019-07-30	7.5	None	Remote
Slanger 0.6.0 is affected by: Remote Code Execution (RCE). The impact is: A remote attacker can execute arbitrary commands by sending a crafted request. The attack vector is: Remote unauthenticated. The fixed version is: after commit 5267b455caeb2e055cccd2b6a22727c111f5c3.									
2	CVE-2019-1010179	77		Exec Code	2019-07-24	2019-08-01	7.5	None	Remote
PHPK including commit 88fd9cdf14ea4b6ac3e3967f6ea7bcaabb6f03b is affected by: Improper Neutralization of Special Elements used in a Command ('C0ggg-keys or execute commands remotely. The component is: function pgg_exec() php.php:98. The attack vector is: HKP-API: /pks/lookup?search.									
3	CVE-2019-1010174	77			2019-07-25	2019-09-28	7.5	None	Remote
Cimg The Cimg Library v.2.3.3 and earlier is affected by: command injection. The impact is: RCE. The component is: load_network() function. The attack lead to command injection, because no string sanitization is done on the url. The fixed version is: v.2.3.4.									
4	CVE-2019-1000018	77		Exec Code	2019-02-04	2019-04-11	4.6	None	Local
rsch version 2.3.4 contains a CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in allowscp pe attack appear to be exploitable via An authorized SSH user with the allowscp permission.									
5	CVE-2019-15954	77		Exec Code +Priv	2019-09-05	2019-09-06	9.0	None	Remote
An issue was discovered in Total.js CMS 12.0.0. An authenticated user with the widgets privilege can gain achieve Remote Command Execution (RCE) on a tag containing JavaScript code that will be evaluated server side. In the process of evaluating the tag by the back-end, it is possible to escape the sandbox total>global.process.mainModule.require(child_process).exec(RCE);</script>									
6	CVE-2019-15949	77		Exec Code	2019-09-05	2019-09-06	9.0	None	Remote
Nagios XI before 5.6.6 allows remote command execution as root. The exploit requires access to the server as the nagios user, or access as the admin user downloading a system profile (profile.php?cmd=download), is executed as root via a passwordless sudo entry; the script executes check_plugin, which is permissions to modify plugins, or the nagios user on the server, can modify the check_plugin executable and insert malicious commands to execute as root									
7	CVE-2019-15530	77			2019-08-23	2019-08-27	9.0	None	Remote
An issue was discovered on D-Link DIR-823G devices with firmware V1.0.2B05. There is a command injection in HNAPl (exploitable with Authentication) via									
8	CVE-2019-15529	77			2019-08-23	2019-08-27	9.0	None	Remote
An issue was discovered on D-Link DIR-823G devices with firmware V1.0.2B05. There is a command injection in HNAPl (exploitable with Authentication) via									
9	CVE-2019-15528	77			2019-08-23	2019-08-27	9.0	None	Remote
An issue was discovered on D-Link DIR-823G devices with firmware V1.0.2B05. There is a command injection in HNAPl (exploitable with Authentication) via SetStaticRouteSettings.									
10	CVE-2019-15527	77			2019-08-23	2019-08-27	9.0	None	Remote
An issue was discovered on D-Link DIR-823G devices with firmware V1.0.2B05. There is a command injection in HNAPl (exploitable with Authentication) via SetWanSettings.									
11	CVE-2019-15526	77			2019-08-23	2019-08-27	9.0	None	Remote
An issue was discovered on D-Link DIR-823G devices with firmware V1.0.2B05. There is a command injection in HNAPl (exploitable with Authentication) via related issue to CVE-2019-13482.									
12	CVE-2019-15107	77			2019-08-15	2019-09-16	10.0	None	Remote
An issue was discovered in Webmin <=1.920. The parameter old in password_change.cgi contains a command injection vulnerability.									
13	CVE-2019-15029	77		Exec Code	2019-09-05	2019-09-06	9.0	None	Remote
FusionPBX 4.4.8 allows an attacker to execute arbitrary system commands by submitting a malicious command to the service_edit.php file (which will insert command, one needs to call the services.php file via a GET request with the service id followed by the parameter a=start to execute the stored command.									
14	CVE-2019-15027	77		Exec Code	2019-08-14	2019-08-27	10.0	None	Remote

Security Vulnerabilities Related To CWE-78

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

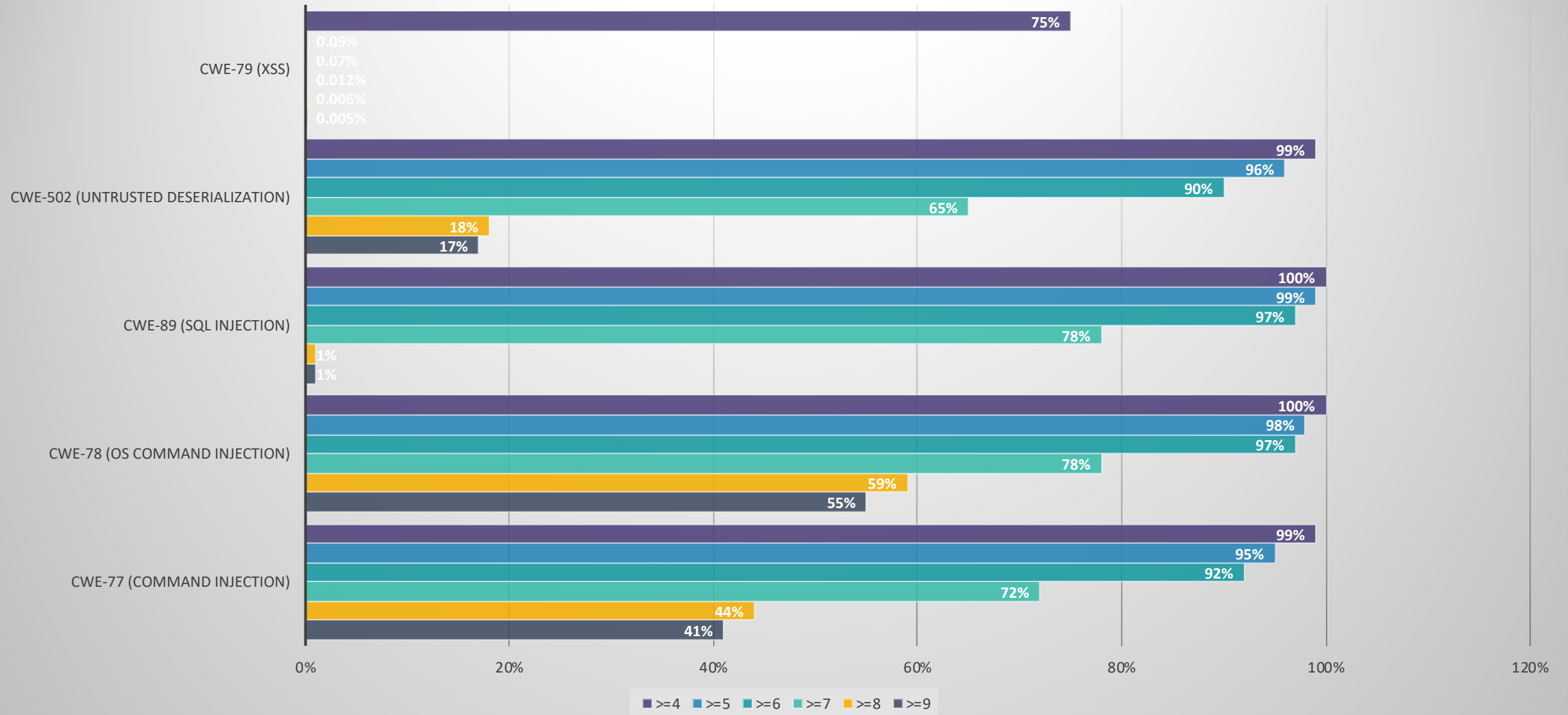
Total number of vulnerabilities : **788** Page : **1** (This Page) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#)

[Cvov Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access
1	CVE-2019-1010200	78		Exec Code	2019-07-23	2019-10-09	10.0	None	Remote
Voice Builder Prior to commit c145d4604d67e6fc625992412ee0fb9a85e26b and f6660e6d8f0d1d931359d591dbdec580fef36d36 is affected by: CWE-78 Command ('OS Command Injection'). The impact is: Remote code execution with the same privileges as the servers. The component is: Two web server accessed remotely. The endpoints are defined at: - /ts: https://github.com/google/voice-builder/blob/3a449a3e8d5100ff323161c89b897f6d5ccdb6f9/m https://github.com/google/voice-builder/blob/3a449a3e8d5100ff323161c89b897f6d5ccdb6f9/festival_model_server/api.js#L28 - /ts: https://github.com/builder/blob/3a449a3e8d5100ff323161c89b897f6d5ccdb6f9/festival_model_server/api.js#L65. The attack vector is: Attacker sends a GET request to the parameter. The fixed version is: After commit f6660e6d8f0d1d931359d591dbdec580fef36d36.									
2	CVE-2019-17510	78		Exec Code	2019-10-11	2019-10-15	10.0	None	Remote
D-Link DIR-846 devices with firmware 100A35 allow remote attackers to execute arbitrary OS commands as root by leveraging admin access and sending metacharacters to /squashfs-root/www/HNAPl/control/SetWizardConfig.php.									
3	CVE-2019-17509	78		Exec Code	2019-10-11	2019-10-15	10.0	None	Remote
D-Link DIR-846 devices with firmware 100A35 allow remote attackers to execute arbitrary OS commands as root by leveraging admin access and sending metacharacters to /squashfs-root/www/HNAPl/control/SetMasterWlanSettings.php.									
4	CVE-2019-17269	78		Exec Code	2019-10-06	2019-10-09	10.0	None	Remote
Intellian Remote Access 3.18 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the Ping Test field.									
5	CVE-2019-16920	78		Exec Code	2019-09-27	2019-10-10	10.0	None	Remote
Unauthenticated remote code execution occurs in D-Link products such as DIR-655C, DIR-866L, DIR-652, and DHP-1565. The issue occurs when the attacker gateway interface that could lead to common injection. An attacker who successfully triggers the command injection could achieve full system compromise affected: DIR-855L, DAP-1533, DIR-862L, DIR-615, DIR-835, and DIR-825.									
6	CVE-2019-16718	78		Exec Code	2019-09-23	2019-09-23	6.8	None	Remote
In radare2 before 3.9.0, a command injection vulnerability exists in bin_symbols() in lib/core/cbin.c. By using a crafted executable file, it's possible to execute a victim. This vulnerability is due to an insufficient fix for CVE-2019-14745 and improper handling of symbol names embedded in executables.									
7	CVE-2019-16701	78			2019-09-25	2019-09-25	9.0	None	Remote
pSense through 2.3.4 through 2.4.4-p3 allows Remote Code Injection via a methodCall XML document with a pfsense.exec.php call containing shell metacharacters.									
8	CVE-2019-16293	78		Exec Code	2019-09-13	2019-09-13	6.5	None	Remote
The Create Discoveries feature of Open-Audit before 3.2.0 allows an authenticated attacker to execute arbitrary OS commands via a crafted value for a									
9	CVE-2019-16057	78			2019-09-16	2019-09-16	10.0	None	Remote
The login_mgr.cgi script in D-Link DNS-320 through 2.05.B10 is vulnerable to remote command injection.									
10	CVE-2019-15701	78		Exec Code	2019-08-27	2019-08-30	6.8	None	Remote
components/Modals/HelpModal.jsx in BloodHound 2.2.0 allows remote attackers to execute arbitrary OS commands (by spawning a child process as the autocomplete feature is used. The victim must import data from an Active Directory with a GPO containing JavaScript in its name.									
11	CVE-2019-15503	78		Exec Code	2019-08-26	2019-08-30	10.0	None	Remote
cgi-cpn/xcoding/prontus_videoedit.cgi in AltaVista Prontus (aka ProntusCMS) through 12.0.3.0 has "Improper Neutralization of Special Elements used in an input via an HTTP GET parameter.									
12	CVE-2019-15498	78		Exec Code	2019-08-23	2019-08-27	9.3	None	Remote
cgi-bin/cmhy/webcam.sh in Vera Edge Home Controller 1.7.4452 allows remote unauthenticated users to execute arbitrary OS commands via --output an bin/cmhy/webcam.sh.									
13	CVE-2019-15036	78		Exec Code	2019-10-02	2019-10-03	9.0	None	Remote
An issue was discovered in JetBrains TeamCity 2018.2.4. A TeamCity Project administrator could execute any command on the server machine. The issue									



% of CVE by CVSS Score



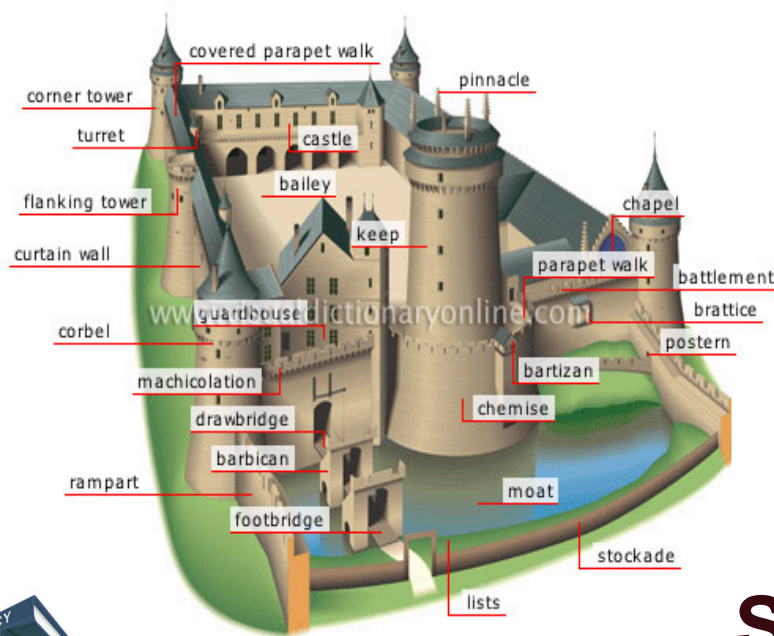


FATS

“S is for Speed and Sophistication”




Don't blame speed



SECURING FAST-CHANGING THINGS IS DIFFERENT

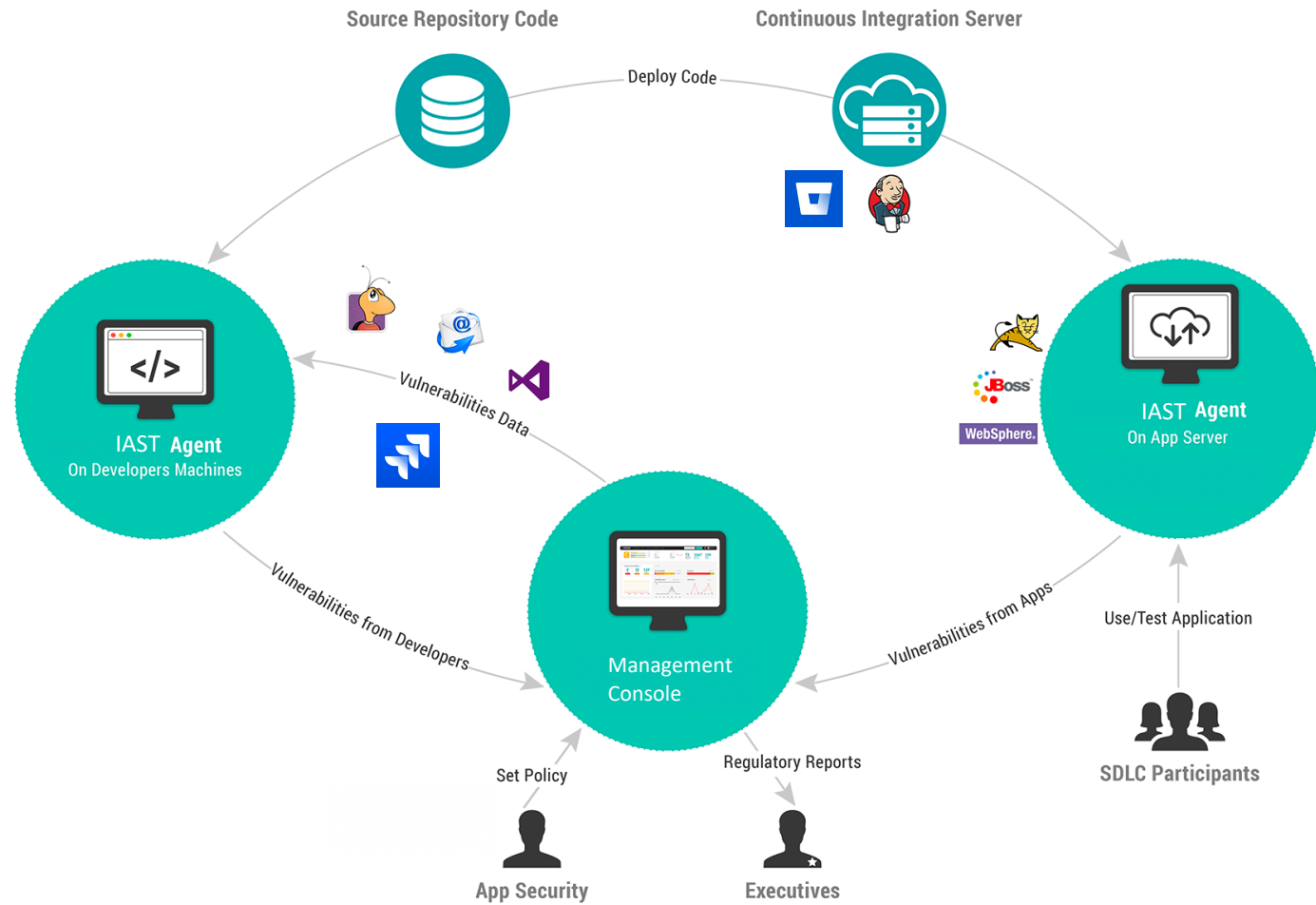




**DevOps speed is held back
by a 15-year-old, scan and perimeter-
based software security model**

Built for the pre-cloud era

Continuous Integration and Delivery



Time for Sophisticated Things

- Cyber talent shortage is real
 - Frameworks won't solve everything
 - Tools can't find everything, especially the extremely complex or custom security controls
 - So focus on the hard stuff with your expensive cyber security assets
-



Examples of Sophisticated things



Authorization



Integrations



Cloud Native / Micro Services / Serverless



Threat modeling



Secure Design



When to train/when to do

A modern office interior with a teal overlay. The scene shows a long conference table with several chairs, a wall with a grid pattern and plants, and large windows in the background. The text "What does this all mean?" is centered in white.

What does this all mean?



~~Shift~~ **EXTEND** left, right, and everywhere!



SECURITY IN
DEVELOPMENT

EMPOWER

- Have some trust in frameworks
- Real time test 1st party and 3rd party code
- Realtime feedback through my tools
- Don't slow me down



SECURITY IN
INTEGRATION

ASSURE

- Don't slow down my builds
- Integrate with my testing tools
- Critical vulns break my build



SECURITY IN
OPERATIONS

PROTECT

- Tell me who is attacking and how
- Stop vulnerabilities from being exploited
- Don't create alert fatigue

APPSEC IN THE MODERN DEV WORLD

Evolve Tools to Secure Modern Software

Automated application security distributed across all software development and delivery pipelines; assess and protect microservices/APIs; native support for cloud-native apps

Enable Developer Self Sufficiency

Self-service application security integrated into the developer workflow; developers automatically find and fix vulnerabilities, without reliance on security experts

Automate Open Source Risk Management

Open source security and compliance controls automatically embedded in CI/CD; teams stay on top of risk introduced by use of open source; always on monitoring and protection

Accelerate Digital Transformation; Protect Legacy Portfolio

A single solution to secure on-premises, cloud and hybrid apps at scale; drive cloud adoption and app modernization, while defending your legacy application portfolio

Optimize Penetration Testing

Strategically focus investment in manual penetration testing on complex security weaknesses; Increase fidelity and action-ability of results

Ensure Continuous Visibility

Real-time visibility into security posture across the enterprise; continuous monitoring and intelligence across the SDLC; streamlined compliance

Thanks! Ask me anything!



David Lindner - @golfhackerdave