SUSTO: Systematic Universal Security Testing Orchestration

Opportunity for a new OWASP project

Who am I?

Luis Saiz

Innovation in Security @BBVA-Labs

https://bbvalabs.gitbook.io/oss/bbva_labs_security

CC0 https://pxhere.com/es/photo/792065

Testing - NIST 800-53rev5

A **requirement** is a statement that translates or expresses a **specific need** including associated **constraints and conditions**

Security and privacy **controls** for information systems and organizations **help satisfy** security and privacy **requirements**

Common controls are security or privacy controls whose implementation results in a **capability** that is **inheritable** by multiple information systems or programs. Controls are deemed inheritable when the information system or program receives protection from the implemented control but the control is developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or program

Organizations consider the **inherited risk** from the use of **common controls** [....] It is therefore important that both internal and external **common control providers keep common control status information current**

QUESTION

How many of you think your organization

keep control status information current?

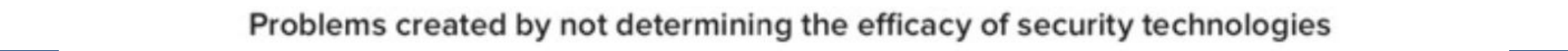
https://pixabay.com/illustrations/hands-raised-raised-hands-arms-up-1768845/

Help Net Security
July 31, 2019

Share this article

53% of enterprises have no idea if their security tools are working

The majority of organizations don't know if the security tools they deploy are working, and are not confident they can avoid data breaches, according to AttackIQ.



“SotA”: Security in CI/CD pipelines

“SotA”: Security in CI/CD pipelines

- (Static/Dynamic) Application Security Testing

“SotA”: Security in CI/CD pipelines

- (Static/Dynamic) Application Security Testing
- SW Composition Analysis

“SotA”: Security in CI/CD pipelines

- (Static/Dynamic) Application Security Testing
- SW Composition Analysis
- Container Security

“SotA”: Security in CI/CD pipelines

- (Static/Dynamic) Application Security Testing
- SW Composition Analysis
- Container Security
- Vulnerability Correlation

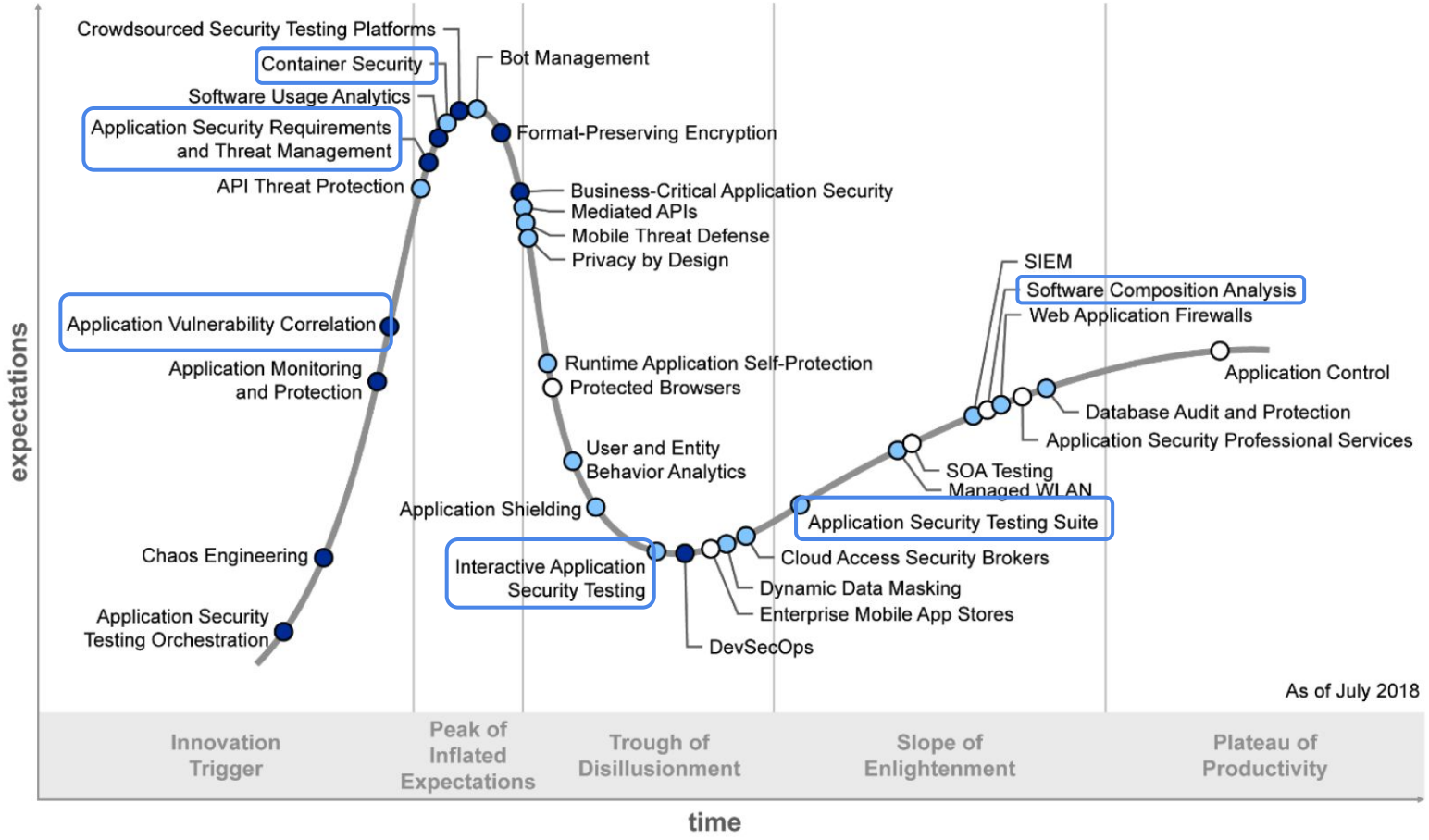
“SotA”: Security in CI/CD pipelines

- (Static/Dynamic) Application Security Testing
- SW Composition Analysis
- Container Security
- Vulnerability Correlation
- Security Requirements & Threat Management

“SotA”: Security in CI/CD pipelines

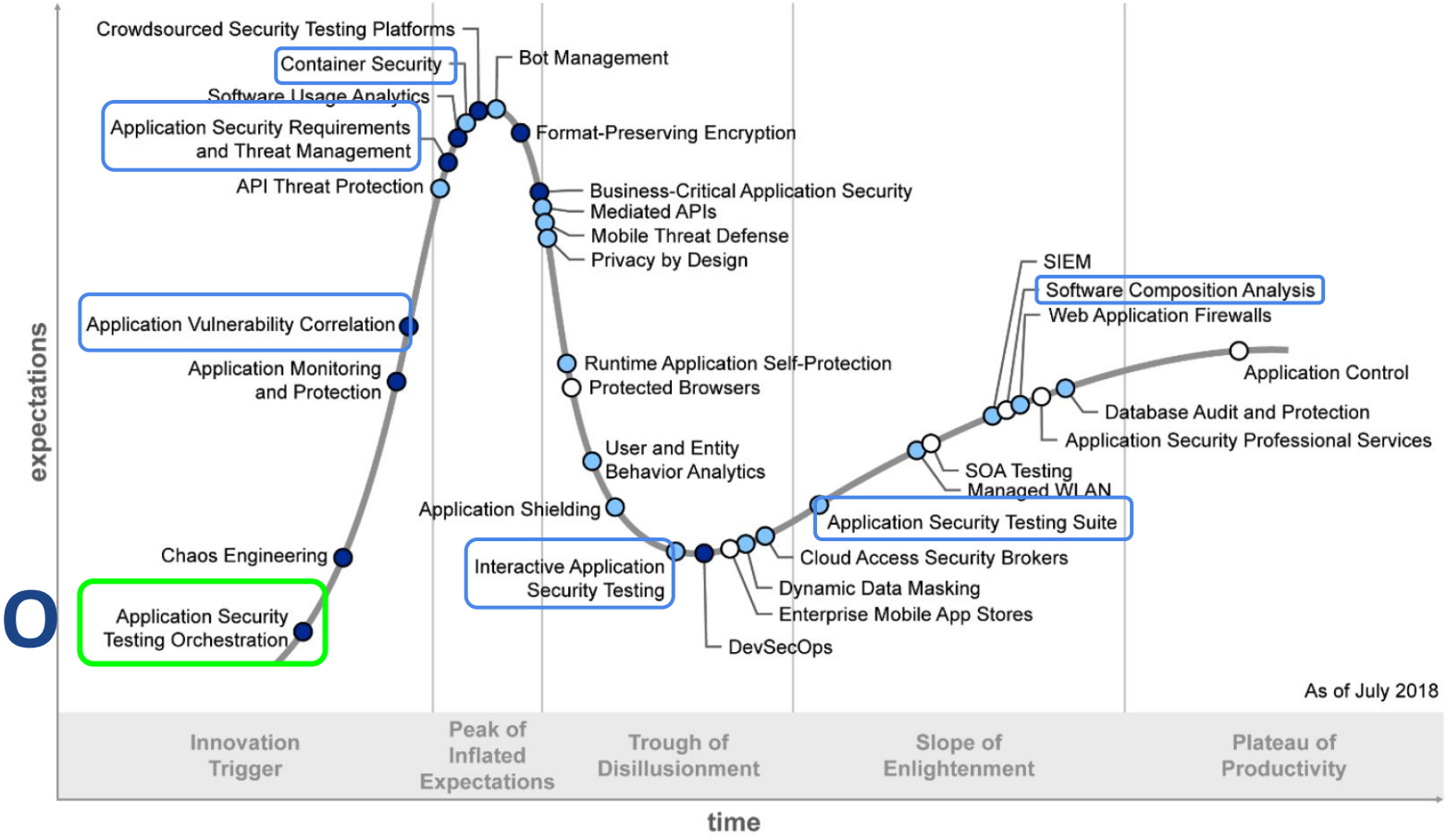
- (Static/Dynamic) Application Security Testing
- SW Composition Analysis
- Container Security
- Vulnerability Correlation
- Security Requirements & Threat Management
- Abuse Story Checks?

Hype Cycle for Application Security, 2018



© 2018 Gartner, Inc.

Hype Cycle for Application Security, 2018



ASTO

© 2018 Gartner, Inc.

Gaps

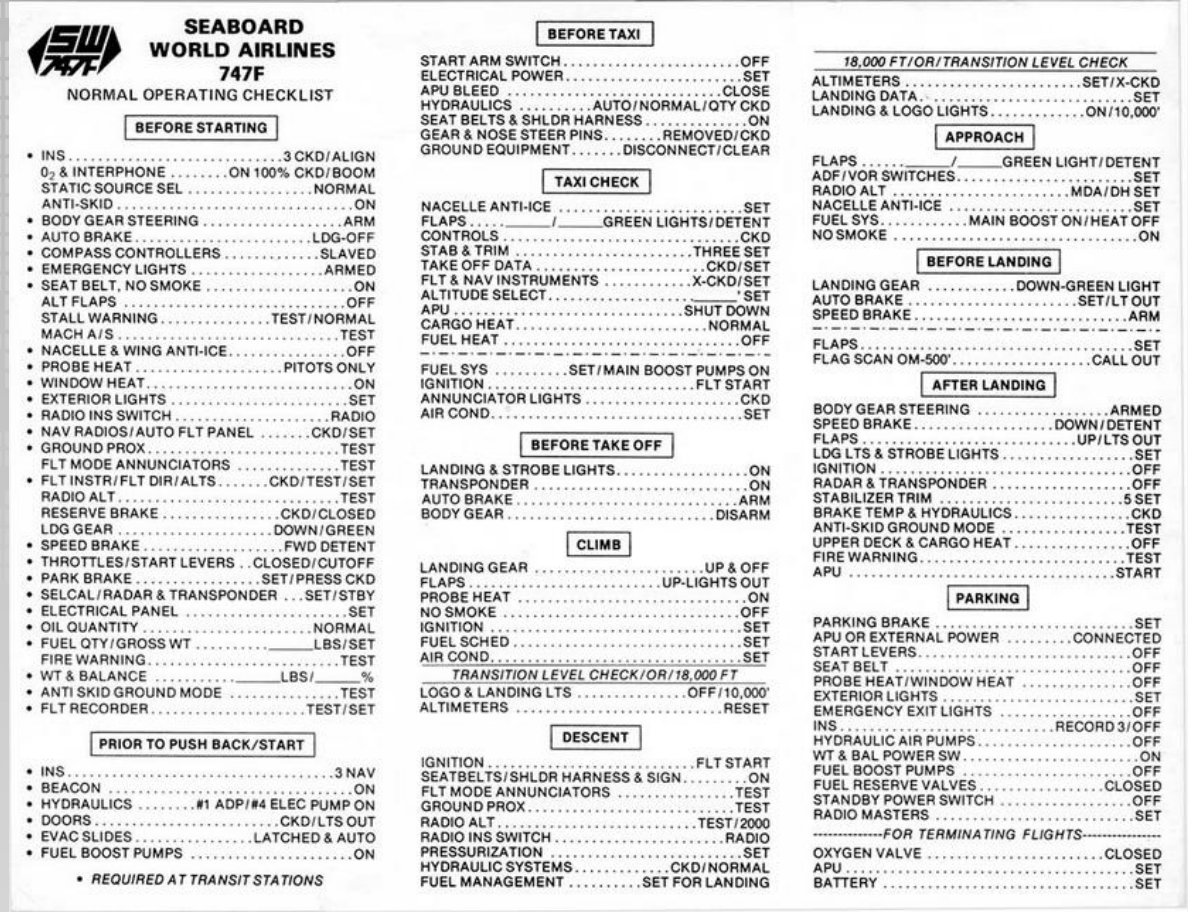
Gaps

Checking the Application (+Container) is not enough

Gaps

Checking the Application (+Container) is not enough

DevOps and SDx allow us to automate the building of the complete infrastructure



SEABOARD WORLD AIRLINES
747F
NORMAL OPERATING CHECKLIST

BEFORE STARTING

- INS ..... 3 CKD/ALIGN
  0_2 & INTERPHONE ..... ON 100% CKD/BOOM
  STATIC SOURCE SEL ..... NORMAL
  ANTI-SKID ..... ON
- BODY GEAR STEERING ..... ARM
- AUTO BRAKE ..... LDG-OFF
- COMPASS CONTROLLERS ..... SLAVED
- EMERGENCY LIGHTS ..... ARMED
- SEAT BELT, NO SMOKE ..... ON
  ALT FLAPS ..... OFF
  STALL WARNING ..... TEST/NORMAL
  MACH A/S ..... TEST
- NACELLE & WING ANTI-ICE ..... OFF
- PROBE HEAT ..... PITOTS ONLY
- WINDOW HEAT ..... ON
- EXTERIOR LIGHTS ..... SET
- RADIO INS SWITCH ..... RADIO
- NAV RADIOS/AUTO FLT PANEL ..... CKD/SET
- GROUND PROX ..... TEST
  FLT MODE ANNUNCIATORS ..... TEST
- FLT INSTR/FLT DIR/ALTS ..... CKD/TEST/SET
  RADIO ALT ..... TEST
  RESERVE BRAKE ..... CKD/CLOSED
  LDG GEAR ..... DOWN/GREEN
- SPEED BRAKE ..... FWD DETENT
- THROTTLES/START LEVERS .. CLOSED/CUTOFF
- PARK BRAKE ..... SET/PRESS CKD
- SELCAL/RADAR & TRANSPONDER ... SET/STBY
- ELECTRICAL PANEL ..... SET
- OIL QUANTITY ..... NORMAL
- FUEL QTY/GROSS WT ..... _____LBS/SET
  FIRE WARNING ..... TEST
- WT & BALANCE ..... _____LBS/_____%
- ANTI SKID GROUND MODE ..... TEST
- FLT RECORDER ..... TEST/SET

PRIOR TO PUSH BACK/START

- INS ..... 3 NAV
- BEACON ..... ON
- HYDRAULICS ..... #1 ADP/#4 ELEC PUMP ON
- DOORS ..... CKD/LTS OUT
- EVAC SLIDES ..... LATCHED & AUTO
- FUEL BOOST PUMPS ..... ON

• *REQUIRED AT TRANSIT STATIONS*

BEFORE TAXI

START ARM SWITCH ..... OFF
ELECTRICAL POWER ..... SET
APU BLEED ..... CLOSE
HYDRAULICS ..... AUTO/NORMAL/QTY CKD
SEAT BELTS & SHLDR HARNESS ..... ON
GEAR & NOSE STEER PINS ..... REMOVED/CKD
GROUND EQUIPMENT ..... DISCONNECT/CLEAR

TAXI CHECK

NACELLE ANTI-ICE ..... SET
FLAPS ..... _____/_____GREEN LIGHTS/DETENT
CONTROLS ..... CKD
STAB & TRIM ..... THREE SET
TAKE OFF DATA ..... CKD/SET
FLT & NAV INSTRUMENTS ..... X-CKD/SET
ALTITUDE SELECT ..... _____' SET
APU ..... SHUT DOWN
CARGO HEAT ..... NORMAL
FUEL HEAT ..... OFF

FUEL SYS ..... SET/MAIN BOOST PUMPS ON
IGNITION ..... FLT START
ANNUNCIATOR LIGHTS ..... CKD
AIR COND ..... SET

BEFORE TAKE OFF

LANDING & STROBE LIGHTS ..... ON
TRANSPONDER ..... ON
AUTO BRAKE ..... ARM
BODY GEAR ..... DISARM

CLIMB

LANDING GEAR ..... UP & OFF
FLAPS ..... UP-LIGHTS OUT
PROBE HEAT ..... ON
NO SMOKE ..... OFF
IGNITION ..... SET
FUEL SCHED ..... SET
AIR COND ..... SET

TRANSITION LEVEL CHECK/OR/18,000 FT

LOGO & LANDING LTS ..... OFF/10,000'
ALTIMETERS ..... RESET

DESCENT

IGNITION ..... FLT START
SEATBELTS/SHLDR HARNESS & SIGN ..... ON
FLT MODE ANNUNCIATORS ..... TEST
GROUND PROX ..... TEST
RADIO ALT TEST/2000
RADIO INS SWITCH ..... RADIO
PRESSURIZATION ..... SET
HYDRAULIC SYSTEMS ..... CKD/NORMAL
FUEL MANAGEMENT ..... SET FOR LANDING

18,000 FT/OR/TRANSITION LEVEL CHECK

ALTIMETERS ..... SET/X-CKD
LANDING DATA ..... SET
LANDING & LOGO LIGHTS ..... ON/10,000'

APPROACH

FLAPS ..... _____/_____GREEN LIGHT/DETENT
ADF/VOR SWITCHES ..... SET
RADIO ALT ..... MDA/DH SET
NACELLE ANTI-ICE ..... SET
FUEL SYS ..... MAIN BOOST ON/HEAT OFF
NO SMOKE ..... ON

BEFORE LANDING

LANDING GEAR ..... DOWN-GREEN LIGHT
AUTO BRAKE ..... SET/LT OUT
SPEED BRAKE ..... ARM

FLAPS ..... SET
FLAG SCAN OM-500' ..... CALL OUT

AFTER LANDING

BODY GEAR STEERING ..... ARMED
SPEED BRAKE ..... DOWN/DETENT
FLAPS ..... UP/LTS OUT
LDG LTS & STROBE LIGHTS ..... SET
IGNITION ..... OFF
RADAR & TRANSPONDER ..... OFF
STABILIZER TRIM ..... 5 SET
BRAKE TEMP & HYDRAULICS ..... CKD
ANTI-SKID GROUND MODE ..... TEST
UPPER DECK & CARGO HEAT ..... OFF
FIRE WARNING ..... TEST
APU ..... START

PARKING

PARKING BRAKE ..... SET
APU OR EXTERNAL POWER ..... CONNECTED
START LEVERS ..... OFF
SEAT BELT ..... OFF
PROBE HEAT/WINDOW HEAT ..... OFF
EXTERIOR LIGHTS ..... SET
EMERGENCY EXIT LIGHTS ..... OFF
INS ..... RECORD 3/OFF
HYDRAULIC AIR PUMPS ..... OFF
WT & BAL POWER SW ..... ON
FUEL BOOST PUMPS ..... OFF
FUEL RESERVE VALVES ..... CLOSED
STANDBY POWER SWITCH ..... OFF
RADIO MASTERS ..... SET

FOR TERMINATING FLIGHTS

OXYGEN VALVE ..... CLOSED
APU ..... SET
BATTERY ..... SET

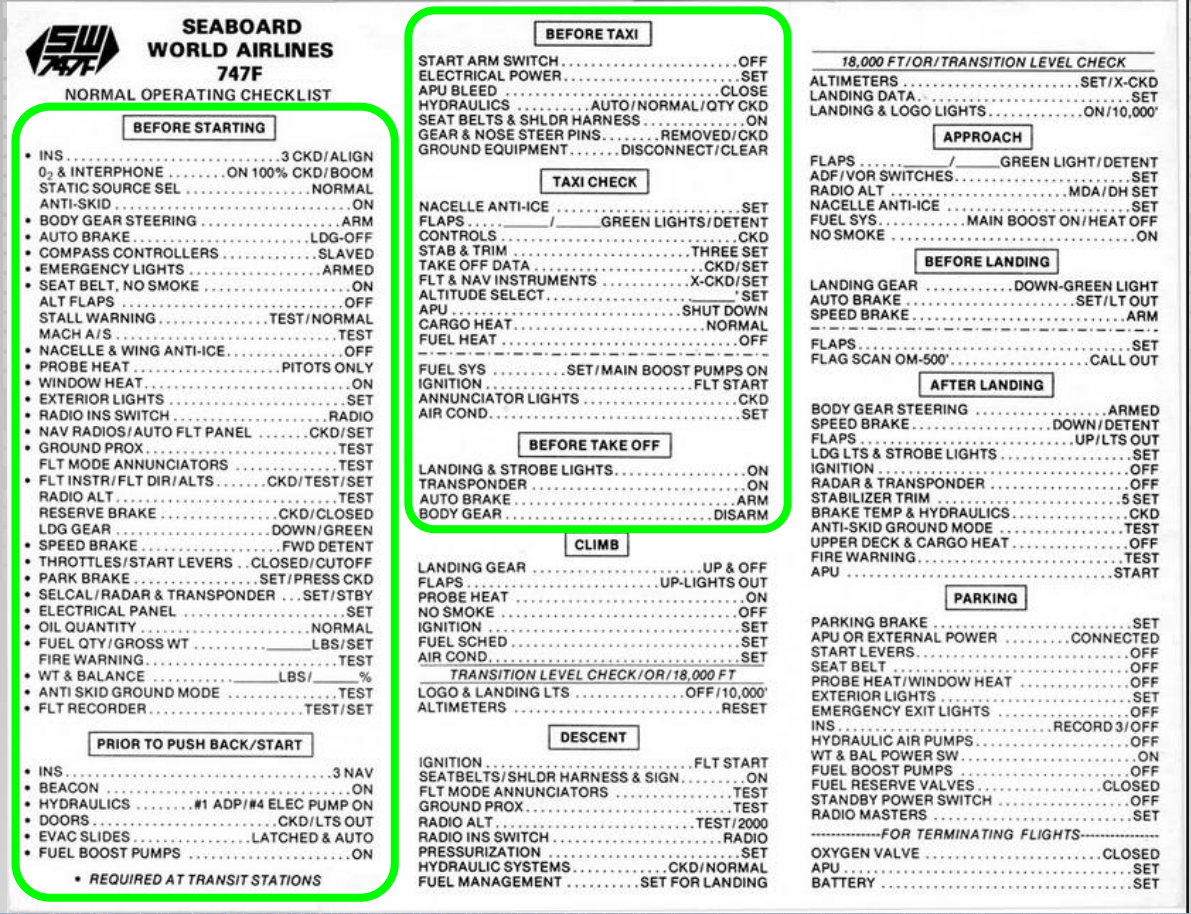
Image: http://www.askthepilot.com/checklists/

Flight checklists

OWASP
Open Web Application Security Project

https://es.m.wikipedia.org/wiki/Archivo:Airbus_A380_cockpit.jpg


https://pxhere.com/en/photo/988500



SEABOARD WORLD AIRLINES
747F
NORMAL OPERATING CHECKLIST

BEFORE STARTING

- INS ..... 3 CKD/ALIGN
  0_2 & INTERPHONE ..... ON 100% CKD/BOOM
  STATIC SOURCE SEL ..... NORMAL
  ANTI-SKID ..... ON
- BODY GEAR STEERING ..... ARM
- AUTO BRAKE ..... LDG-OFF
- COMPASS CONTROLLERS ..... SLAVED
- EMERGENCY LIGHTS ..... ARMED
- SEAT BELT, NO SMOKE ..... ON
  ALT FLAPS ..... OFF
  STALL WARNING ..... TEST/NORMAL
  MACH A/S ..... TEST
- NACELLE & WING ANTI-ICE ..... OFF
- PROBE HEAT ..... PITOTS ONLY
- WINDOW HEAT ..... ON
- EXTERIOR LIGHTS ..... SET
- RADIO INS SWITCH ..... RADIO
- NAV RADIOS/AUTO FLT PANEL ..... CKD/SET
- GROUND PROX ..... TEST
  FLT MODE ANNUNCIATORS ..... TEST
- FLT INSTR/FLT DIR/ALTS ..... CKD/TEST/SET
  RADIO ALT ..... TEST
  RESERVE BRAKE ..... CKD/CLOSED
  LDG GEAR ..... DOWN/GREEN
- SPEED BRAKE ..... FWD DETENT
- THROTTLES/START LEVERS ..... CLOSED/CUTOFF
- PARK BRAKE ..... SET/PRESS CKD
- SELCAL/RADAR & TRANSPONDER ..... SET/STBY
- ELECTRICAL PANEL ..... SET
- OIL QUANTITY ..... NORMAL
- FUEL QTY/GROSS WT ..... _____LBS/SET
  FIRE WARNING ..... TEST
- WT & BALANCE ..... _____LBS/_____%
- ANTI SKID GROUND MODE ..... TEST
- FLT RECORDER ..... TEST/SET

PRIOR TO PUSH BACK/START

- INS ..... 3 NAV
- BEACON ..... ON
- HYDRAULICS ..... #1 ADP/#4 ELEC PUMP ON
- DOORS ..... CKD/LTS OUT
- EVAC SLIDES ..... LATCHED & AUTO
- FUEL BOOST PUMPS ..... ON

• *REQUIRED AT TRANSIT STATIONS*

BEFORE TAXI

START ARM SWITCH ..... OFF
ELECTRICAL POWER ..... SET
APU BLEED ..... CLOSE
HYDRAULICS ..... AUTO/NORMAL/QTY CKD
SEAT BELTS & SHLDR HARNESS ..... ON
GEAR & NOSE STEER PINS ..... REMOVED/CKD
GROUND EQUIPMENT ..... DISCONNECT/CLEAR

TAXI CHECK

NACELLE ANTI-ICE ..... SET
FLAPS _____/_____ GREEN LIGHTS/DETENT
CONTROLS ..... CKD
STAB & TRIM ..... THREE SET
TAKE OFF DATA ..... CKD/SET
FLT & NAV INSTRUMENTS ..... X-CKD/SET
ALTITUDE SELECT ..... _____' SET
APU ..... SHUT DOWN
CARGO HEAT ..... NORMAL
FUEL HEAT ..... OFF

FUEL SYS ..... SET/MAIN BOOST PUMPS ON
IGNITION ..... FLT START
ANNUNCIATOR LIGHTS ..... CKD
AIR COND ..... SET

BEFORE TAKE OFF

LANDING & STROBE LIGHTS ..... ON
TRANSPONDER ..... ON
AUTO BRAKE ..... ARM
BODY GEAR ..... DISARM

CLIMB

LANDING GEAR ..... UP & OFF
FLAPS ..... UP-LIGHTS OUT
PROBE HEAT ..... ON
NO SMOKE ..... OFF
IGNITION ..... SET
FUEL SCHED ..... SET
AIR COND ..... SET

TRANSITION LEVEL CHECK/OR/18,000 FT

LOGO & LANDING LTS ..... OFF/10,000'
ALTIMETERS ..... RESET

DESCENT

IGNITION ..... FLT START
SEATBELTS/SHLDR HARNESS & SIGN ..... ON
FLT MODE ANNUNCIATORS ..... TEST
GROUND PROX ..... TEST
RADIO ALT TEST/2000
RADIO INS SWITCH ..... RADIO
PRESSURIZATION ..... SET
HYDRAULIC SYSTEMS ..... CKD/NORMAL
FUEL MANAGEMENT ..... SET FOR LANDING

18,000 FT/OR/TRANSITION LEVEL CHECK

ALTIMETERS ..... SET/X-CKD
LANDING DATA ..... SET
LANDING & LOGO LIGHTS ..... ON/10,000'

APPROACH

FLAPS _____/_____ GREEN LIGHT/DETENT
ADF/VOR SWITCHES ..... SET
RADIO ALT ..... MDA/DH SET
NACELLE ANTI-ICE ..... SET
FUEL SYS ..... MAIN BOOST ON/HEAT OFF
NO SMOKE ..... ON

BEFORE LANDING

LANDING GEAR ..... DOWN-GREEN LIGHT
AUTO BRAKE ..... SET/LT OUT
SPEED BRAKE ..... ARM

FLAPS ..... SET
FLAG SCAN OM-500' ..... CALL OUT

AFTER LANDING

BODY GEAR STEERING ..... ARMED
SPEED BRAKE ..... DOWN/DETENT
FLAPS ..... UP/LTS OUT
LDG LTS & STROBE LIGHTS ..... SET
IGNITION ..... OFF
RADAR & TRANSPONDER ..... OFF
STABILIZER TRIM ..... 5 SET
BRAKE TEMP & HYDRAULICS ..... CKD
ANTI-SKID GROUND MODE ..... TEST
UPPER DECK & CARGO HEAT ..... OFF
FIRE WARNING ..... TEST
APU ..... START

PARKING

PARKING BRAKE ..... SET
APU OR EXTERNAL POWER ..... CONNECTED
START LEVERS ..... OFF
SEAT BELT ..... OFF
PROBE HEAT/WINDOW HEAT ..... OFF
EXTERIOR LIGHTS ..... SET
EMERGENCY EXIT LIGHTS ..... OFF
INS ..... RECORD 3/OFF
HYDRAULIC AIR PUMPS ..... OFF
WT & BAL POWER SW ..... ON
FUEL BOOST PUMPS ..... OFF
FUEL RESERVE VALVES ..... CLOSED
STANDBY POWER SWITCH ..... OFF
RADIO MASTERS ..... SET

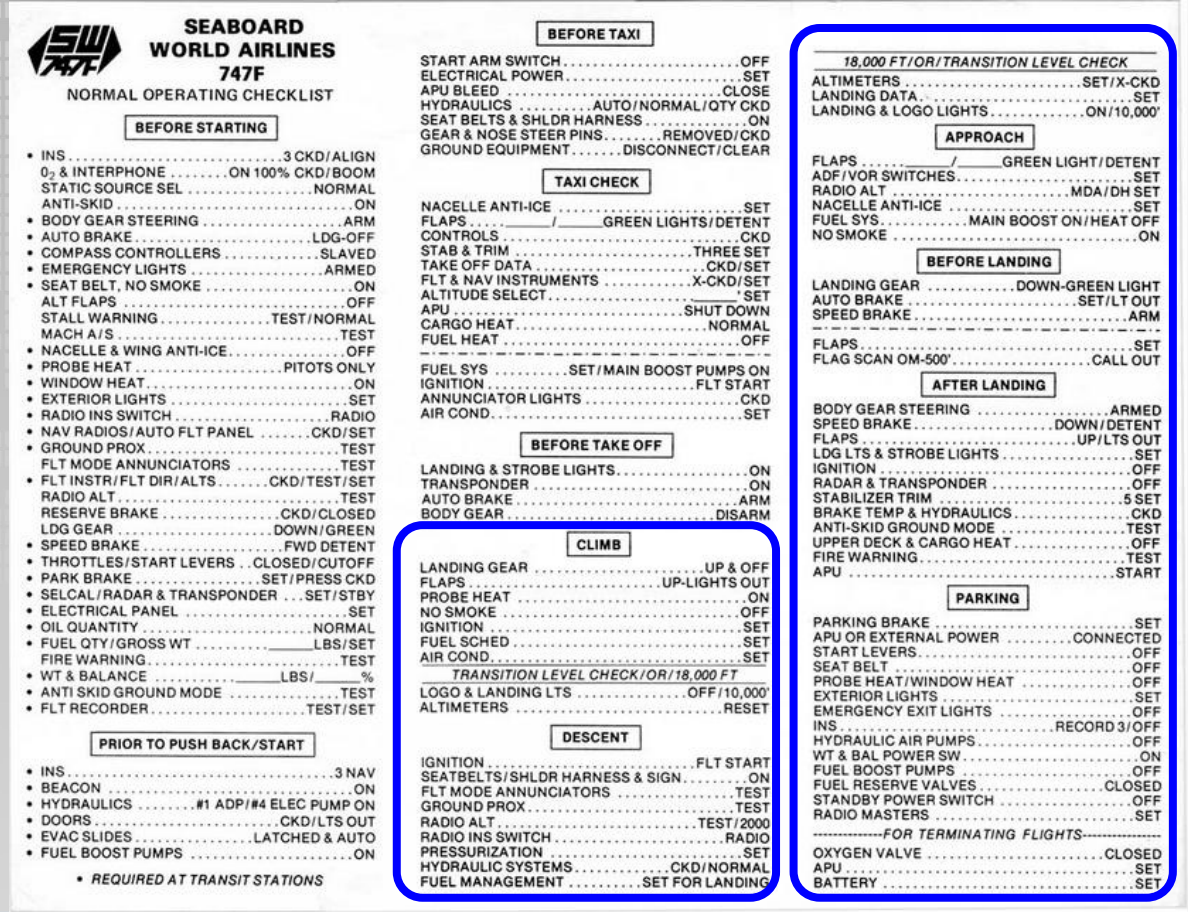
FOR TERMINATING FLIGHTS

OXYGEN VALVE ..... CLOSED
APU ..... SET
BATTERY ..... SET

Image: http://www.askthepilot.com/checklists/

Pre-Flight ("Built-time") checklists

OWASP
Open Web Application Security Project



SEABOARD WORLD AIRLINES
747F
NORMAL OPERATING CHECKLIST

BEFORE STARTING

- INS ..... 3 CKD/ALIGN
  0_2 & INTERPHONE ..... ON 100% CKD/BOOM
  STATIC SOURCE SEL ..... NORMAL
  ANTI-SKID ..... ON
- BODY GEAR STEERING ..... ARM
- AUTO BRAKE ..... LDG-OFF
- COMPASS CONTROLLERS ..... SLAVED
- EMERGENCY LIGHTS ..... ARMED
- SEAT BELT, NO SMOKE ..... ON
  ALT FLAPS ..... OFF
  STALL WARNING ..... TEST/NORMAL
  MACH A/S ..... TEST
- NACELLE & WING ANTI-ICE ..... OFF
- PROBE HEAT ..... PITOTS ONLY
- WINDOW HEAT ..... ON
- EXTERIOR LIGHTS ..... SET
- RADIO INS SWITCH ..... RADIO
- NAV RADIOS/AUTO FLT PANEL ..... CKD/SET
- GROUND PROX ..... TEST
  FLT MODE ANNUNCIATORS ..... TEST
- FLT INSTR/FLT DIR/ALTS ..... CKD/TEST/SET
  RADIO ALT ..... TEST
  RESERVE BRAKE ..... CKD/CLOSED
  LDG GEAR ..... DOWN/GREEN
- SPEED BRAKE ..... FWD DETENT
- THROTTLES/START LEVERS ..... CLOSED/CUTOFF
- PARK BRAKE ..... SET/PRESS CKD
- SELCAL/RADAR & TRANSPONDER ..... SET/STBY
- ELECTRICAL PANEL ..... SET
- OIL QUANTITY ..... NORMAL
- FUEL QTY/GROSS WT ..... _____ LBS/SET
  FIRE WARNING ..... TEST
- WT & BALANCE ..... _____ LBS/_____ %
- ANTI SKID GROUND MODE ..... TEST
- FLT RECORDER ..... TEST/SET

PRIOR TO PUSH BACK/START

- INS ..... 3 NAV
- BEACON ..... ON
- HYDRAULICS ..... #1 ADP/#4 ELEC PUMP ON
- DOORS ..... CKD/LTS OUT
- EVAC SLIDES ..... LATCHED & AUTO
- FUEL BOOST PUMPS ..... ON

• *REQUIRED AT TRANSIT STATIONS*

BEFORE TAXI

START ARM SWITCH ..... OFF
ELECTRICAL POWER ..... SET
APU BLEED ..... CLOSE
HYDRAULICS ..... AUTO/NORMAL/QTY CKD
SEAT BELTS & SHLDR HARNESS ..... ON
GEAR & NOSE STEER PINS ..... REMOVED/CKD
GROUND EQUIPMENT ..... DISCONNECT/CLEAR

TAXI CHECK

NACELLE ANTI-ICE ..... SET
FLAPS ..... _____/_____ GREEN LIGHTS/DETENT
CONTROLS ..... CKD
STAB & TRIM ..... THREE SET
TAKE OFF DATA ..... CKD/SET
FLT & NAV INSTRUMENTS ..... X-CKD/SET
ALTITUDE SELECT ..... _____' SET
APU ..... SHUT DOWN
CARGO HEAT ..... NORMAL
FUEL HEAT ..... OFF

FUEL SYS ..... SET/MAIN BOOST PUMPS ON
IGNITION ..... FLT START
ANNUNCIATOR LIGHTS ..... CKD
AIR COND ..... SET

BEFORE TAKE OFF

LANDING & STROBE LIGHTS ..... ON
TRANSPONDER ..... ON
AUTO BRAKE ..... ARM
BODY GEAR ..... DISARM

CLIMB

LANDING GEAR ..... UP & OFF
FLAPS ..... UP-LIGHTS OUT
PROBE HEAT ..... ON
NO SMOKE ..... OFF
IGNITION ..... SET
FUEL SCHED ..... SET
AIR COND ..... SET

TRANSITION LEVEL CHECK/OR/18,000 FT

LOGO & LANDING LTS ..... OFF/10,000'
ALTIMETERS ..... RESET

DESCENT

IGNITION ..... FLT START
SEATBELTS/SHLDR HARNESS & SIGN ..... ON
FLT MODE ANNUNCIATORS ..... TEST
GROUND PROX ..... TEST
RADIO ALT TEST/2000
RADIO INS SWITCH ..... RADIO
PRESSURIZATION ..... SET
HYDRAULIC SYSTEMS ..... CKD/NORMAL
FUEL MANAGEMENT ..... SET FOR LANDING

18,000 FT/OR/TRANSITION LEVEL CHECK

ALTIMETERS ..... SET/X-CKD
LANDING DATA ..... SET
LANDING & LOGO LIGHTS ..... ON/10,000'

APPROACH

FLAPS ..... _____/_____ GREEN LIGHT/DETENT
ADF/VOR SWITCHES ..... SET
RADIO ALT ..... MDA/DH SET
NACELLE ANTI-ICE ..... SET
FUEL SYS ..... MAIN BOOST ON/HEAT OFF
NO SMOKE ..... ON

BEFORE LANDING

LANDING GEAR ..... DOWN-GREEN LIGHT
AUTO BRAKE ..... SET/LT OUT
SPEED BRAKE ..... ARM

FLAPS ..... SET
FLAG SCAN OM-500' ..... CALL OUT

AFTER LANDING

BODY GEAR STEERING ..... ARMED
SPEED BRAKE ..... DOWN/DETENT
FLAPS ..... UP/LTS OUT
LDG LTS & STROBE LIGHTS ..... SET
IGNITION ..... OFF
RADAR & TRANSPONDER ..... OFF
STABILIZER TRIM ..... 5 SET
BRAKE TEMP & HYDRAULICS ..... CKD
ANTI-SKID GROUND MODE ..... TEST
UPPER DECK & CARGO HEAT ..... OFF
FIRE WARNING ..... TEST
APU ..... START

PARKING

PARKING BRAKE ..... SET
APU OR EXTERNAL POWER ..... CONNECTED
START LEVERS ..... OFF
SEAT BELT ..... OFF
PROBE HEAT/WINDOW HEAT ..... OFF
EXTERIOR LIGHTS ..... SET
EMERGENCY EXIT LIGHTS ..... OFF
INS ..... RECORD 3/OFF
HYDRAULIC AIR PUMPS ..... OFF
WT & BAL POWER SW ..... ON
FUEL BOOST PUMPS ..... OFF
FUEL RESERVE VALVES ..... CLOSED
STANDBY POWER SWITCH ..... OFF
RADIO MASTERS ..... SET

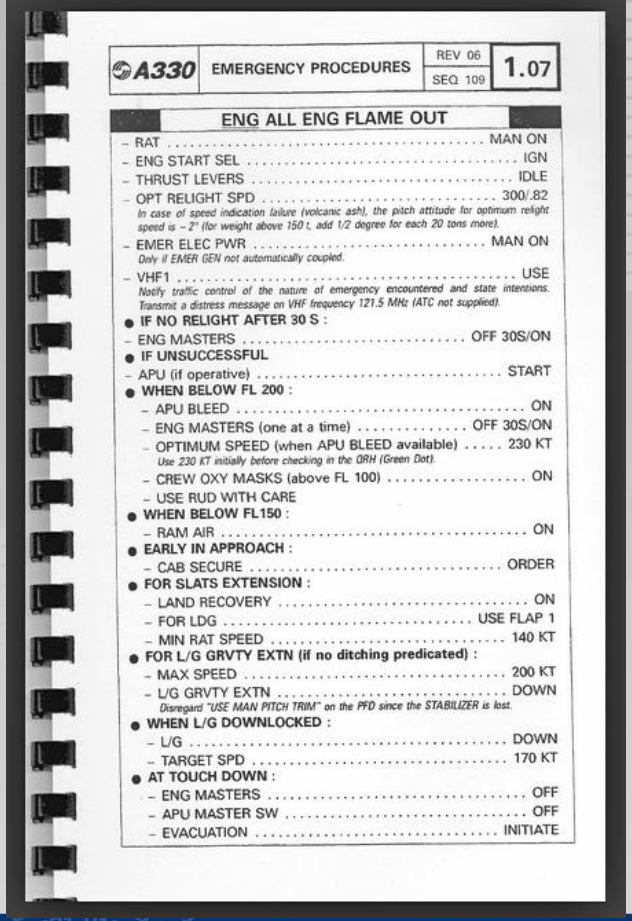
FOR TERMINATING FLIGHTS

OXYGEN VALVE ..... CLOSED
APU ..... SET
BATTERY ..... SET

Image: http://www.askthepilot.com/checklists/

During Flight ("Run-time") checklists

OWASP
Open Web Application Security Project



A330 | EMERGENCY PROCEDURES | REV 06 | SEQ 109 | 1.07

ENG ALL ENG FLAME OUT

- RAT ..... MAN ON
- ENG START SEL ..... IGN
- THRUST LEVERS ..... IDLE
- OPT RELIGHT SPD 300/.82

  In case of speed indication failure (volcanic ash), the pitch attitude for optimum relight speed is – 2° (for weight above 150 t, add 1/2 degree for each 20 tons more).
- EMER ELEC PWR ..... MAN ON

  Only if EMER GEN not automatically coupled.
- VHF1 ..... USE

  Notify traffic control of the nature of emergency encountered and state intentions. Transmit a distress message on VHF frequency 121.5 MHz (ATC not supplied).

- **IF NO RELIGHT AFTER 30 S :**
  - ENG MASTERS ..... OFF 30S/ON
- **IF UNSUCCESSFUL**
  - APU (if operative) ..... START
- **WHEN BELOW FL 200 :**
  - APU BLEED ..... ON
  - ENG MASTERS (one at a time) ..... OFF 30S/ON
  - OPTIMUM SPEED (when APU BLEED available) ..... 230 KT

    Use 230 KT initially before checking in the QRH (Green Dot).
  - CREW OXY MASKS (above FL 100) ..... ON
  - USE RUD WITH CARE
- **WHEN BELOW FL150 :**
  - RAM AIR ..... ON
- **EARLY IN APPROACH :**
  - CAB SECURE ..... ORDER
- **FOR SLATS EXTENSION :**
  - LAND RECOVERY ..... ON
  - FOR LDG ..... USE FLAP 1
  - MIN RAT SPEED ..... 140 KT
- **FOR L/G GRVTY EXTN (if no ditching predicated) :**
  - MAX SPEED ..... 200 KT
  - L/G GRVTY EXTN ..... DOWN

    Disregard "USE MAN PITCH TRIM" on the PFD since the STABILIZER is lost.
- **WHEN L/G DOWNLOCKED :**
  - L/G ..... DOWN
  - TARGET SPD ..... 170 KT
- **AT TOUCH DOWN :**
  - ENG MASTERS ..... OFF
  - APU MASTER SW ..... OFF
  - EVACUATION ..... INITIATE

Image: http://www.askthepilot.com/checklists/

QRH (“SOAR”) checklists

OWASP Open Web Application Security Project

Feature testing

- Simple test can be safely extrapolated

Feature testing

```
Feature: Record a ledger entry
  As an Accountant
  I want to account according COA selected by accountant
  In order to account all movements and comply with legislation and accounting rules

  Scenario: Record a ledger entry
    Given a bank named "Gringotts"
    And "Gringotts" bank has the default Accounting Periods, Chart of Accounts and Statements

    When the system registers an financial event with date "2016-05-25"
      | description                    | accountCode | Debit    | Credit   |
      | Cash and Balance with central Banks | 11000       | 1000 EUR |          |
      | Share Capital                  | 31000       |          | 1000 EUR |

    Then the following accounting entries in the Journal are added
      | description                | entryDate  | requestDate | accountingPeriod | periodCodes                |
      | society (bank) constitution | 2016-05-25 | 2016-05-25  | FY2016           | 2016M05, 2016Q2, FY2016 |

    And all accounting movements are recorded
      | description                    | accountCode | Debit    | Credit   |
      | Cash and Balance with central Banks | 11000       | 1000 EUR |          |
      | Share Capital                  | 31000       |          | 1000 EUR |
```

Feature testing

- Simple tests can be safely extrapolated
- Business dependent: Difficult to reuse

Feature testing

```
Feature: Record a ledger entry
  As an Accountant
  I want to account according COA selected by accountant
  In order to account all movements and comply with legislation and accounting rules

  Scenario: Record a ledger entry
    Given a bank named "Gringotts"
    And "Gringotts" bank has the default Accounting Periods, Chart of Accounts and Statements

    When the system registers an financial event with date "2016-05-25"
      | description                    | accountCode | Debit    | Credit   |
      | Cash and Balance with central Banks | 11000       | 1000 EUR |          |
      | Share Capital                  | 31000       |          | 1000 EUR |

    Then the following accounting entries in the Journal are added
      | description                | entryDate  | requestDate | accountingPeriod | periodCodes                |
      | society (bank) constitution | 2016-05-25 | 2016-05-25  | FY2016           | 2016M05, 2016Q2, FY2016 |

    And all accounting movements are recorded
      | description                    | accountCode | Debit    | Credit   |
      | Cash and Balance with central Banks | 11000       | 1000 EUR |          |
      | Share Capital                  | 31000       |          | 1000 EUR |
```

Security Controls testing complexity

All or nothing + Orchestration

A lesson about intentional risk

https://pixabay.com/photos/window-window-grille-lattice-window-243074/

Security Controls testing complexity

All or nothing + Orchestration

In security we need to test for **"all of"** or **"none of"** conditions

Mark Russinovich
@markrussinovich

Major Sysmon release coming soon with "anyof" and "allof" filters, as well as nested rules. Here's a config that reports all powershell.exe's launched from cmd.exe and all cmd.exe's launched from Explorer:

Traducir Tweet

```
<RuleGroup name="group 1" groupRelation="or">
  <ProcessCreate onmatch="include">

    <Rule groupRelation="and">
      <Image condition="end with">powershell.exe</Image>
      <ParentImage condition="end with">cmd.exe</ParentImage>
    </Rule>

    <Rule groupRelation="and">
      <Image condition="end with">cmd.exe</Image>
      <ParentImage condition="end with">explorer.exe</ParentImage>
    </Rule>

  </ProcessCreate>
</RuleGroup>
```

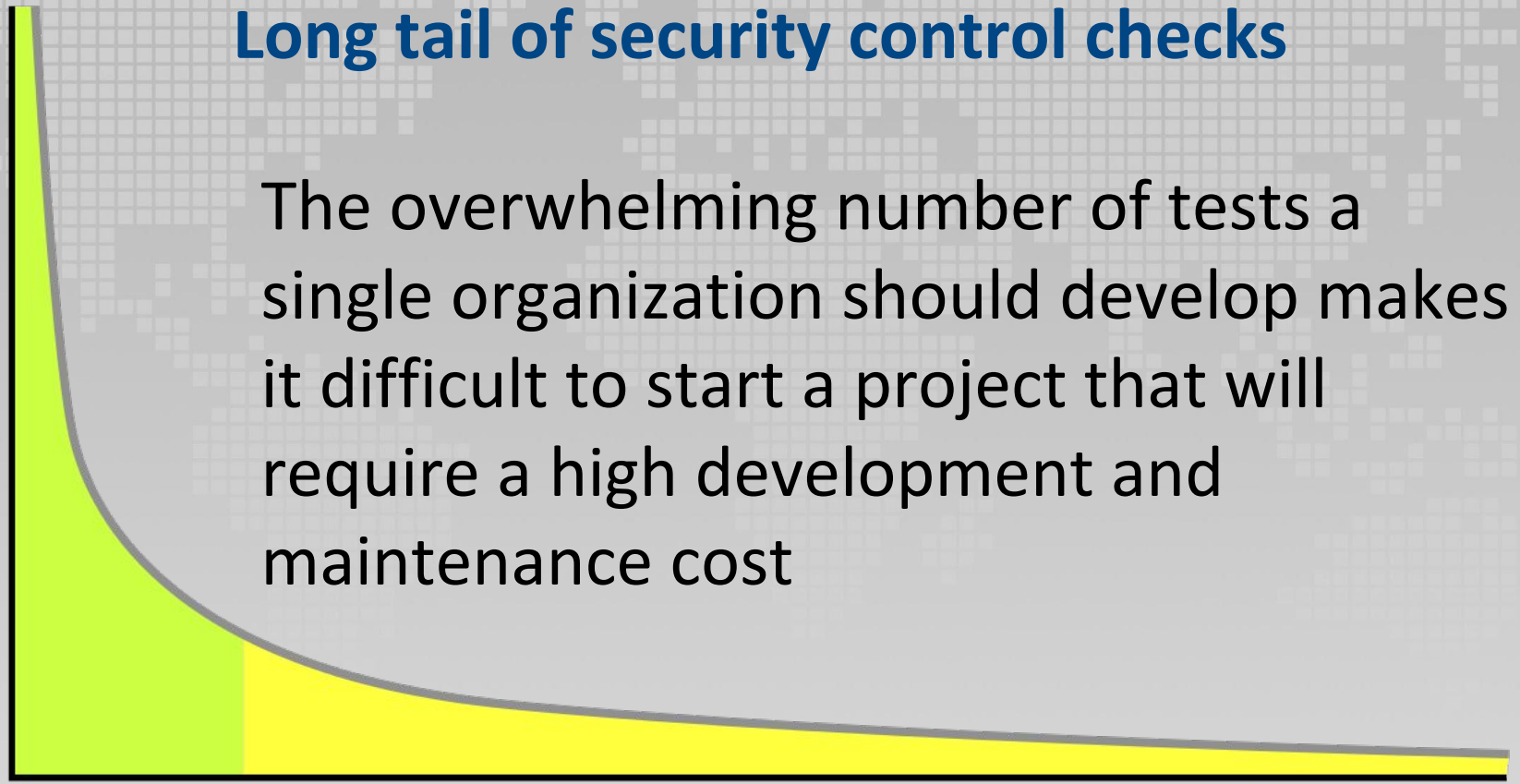
7:43 p. m. · 27 ago. 2019 · TweetDeck

Security Controls testing complexity

All or nothing + Orchestration

In security we need to test for **"all of"** or **"none of"** conditions, making it necessary to **pipeline** and **orchestrate** outputs of tools as inputs of other tools, whether they are commercial ones or small CLI scripts.

Long tail of security control checks



The overwhelming number of tests a single organization should develop makes it difficult to start a project that will require a high development and maintenance cost

Picture by Hay Kranen

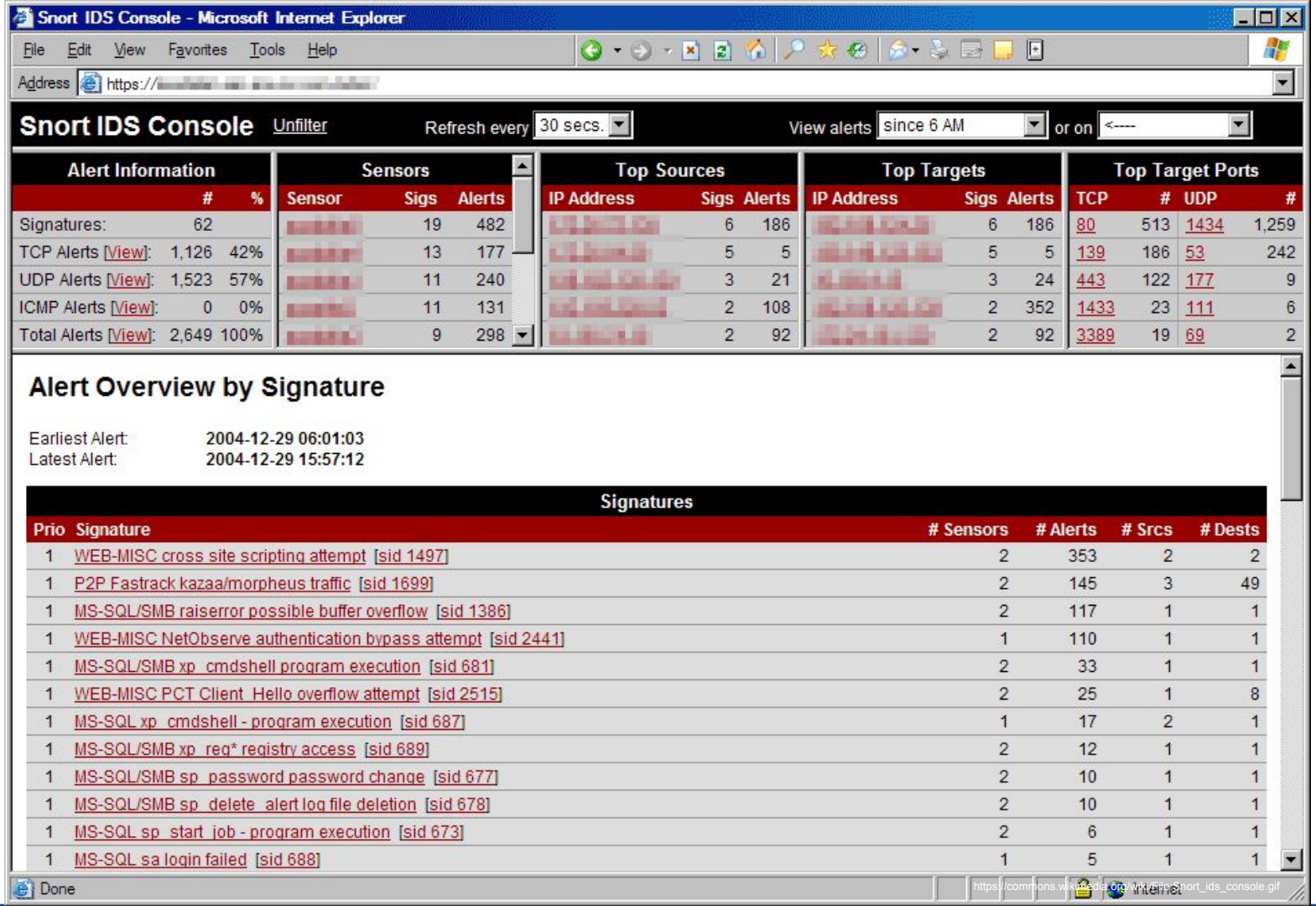
Standardizing Security Controls testing

- Unlike Functional Features, Security Controls are similar among different projects (Common Controls) and across organizations

Standardizing Security Controls testing

- Unlike Functional Features, Security Controls are similar among different projects (Common Controls) and across organizations
- We even have industry standards

Success stories


Snort IDS Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://
Snort IDS Console Unfilter Refresh every 30 secs. View alerts since 6 AM or on <----
Alert Information
%
Signatures: 62
TCP Alerts [View]: 1,126 42%
UDP Alerts [View]: 1,523 57%
ICMP Alerts [View]: 0 0%
Total Alerts [View]: 2,649 100%
Sensors
Sensor Sigs Alerts
19 482
13 177
11 240
11 131
9 298
Top Sources
IP Address Sigs Alerts
6 186
5 5
3 21
2 108
2 92
Top Targets
IP Address Sigs Alerts
6 186
5 5
3 24
2 352
2 92
Top Target Ports
TCP # UDP #
80 513 1434 1,259
139 186 53 242
443 122 177 9
1433 23 111 6
3389 19 69 2
Alert Overview by Signature
Earliest Alert: 2004-12-29 06:01:03
Latest Alert: 2004-12-29 15:57:12
Signatures
Prio Signature # Sensors # Alerts # Srcs # Dests
1 WEB-MISC cross site scripting attempt [sid 1497] 2 353 2 2
1 P2P Fastrack kazaa/morpheus traffic [sid 1699] 2 145 3 49
1 MS-SQL/SMB raiserror possible buffer overflow [sid 1386] 2 117 1 1
1 WEB-MISC NetObserve authentication bypass attempt [sid 2441] 1 110 1 1
1 MS-SQL/SMB xp_cmdshell program execution [sid 681] 2 33 1 1
1 WEB-MISC PCT Client_Hello overflow attempt [sid 2515] 2 25 1 8
1 MS-SQL xp_cmdshell - program execution [sid 687] 1 17 2 1
1 MS-SQL/SMB xp_reg* registry access [sid 689] 2 12 1 1
1 MS-SQL/SMB sp_password password change [sid 677] 2 10 1 1
1 MS-SQL/SMB sp_delete_alert log file deletion [sid 678] 2 10 1 1
1 MS-SQL sp_start_job - program execution [sid 673] 2 6 1 1
1 MS-SQL sa login failed [sid 688] 1 5 1 1
Done
Internet
https://commons.wikimedia.org/wiki/File:Snort_ids_console.gif

```
/*
   Yara Rule Set
   Author: Florian Roth
   Date: 2017-06-04
   Identifier: FireEye EternalBlue - Non-Wannacry Attacks
   Reference: https://goo.gl/OOB3mH
*/

/* Rule Set ----------------------------------------------------------------- */

rule Backdoor_Redosdru_Jun17 {
   meta:
      description = "Detects malware Redosdru - file systemHome.exe"
      license = "https://creativecommons.org/licenses/by-nc/4.0/"
      author = "Florian Roth"
      reference = "https://goo.gl/OOB3mH"
      date = "2017-06-04"
      hash1 = "4f49e17b457ef202ab0be905691ef2b2d2b0a086a7caddd1e70dd45e5ed3b309"
   strings:
      $x1 = "%s\\%d.gho" fullword ascii
      $x2 = "%s\\nt%s.dll" fullword ascii
      $x3 = "baijinUPdate" fullword ascii

      $s1 = "RegQueryValueEx(Svchost\\netsvcs)" fullword ascii
      $s2 = "serviceone" fullword ascii
      $s3 = " #p  #p  #p  #p  #p  #p  #p  #p  #p  #p  #p  #p  #p  #p  #p  #p  #p  #p  #p  #p  #p  #p  #p  #p  #f  #" fullword ascii
      $s4 = "servicetwo" fullword ascii
      $s5 = "UpdateCrc" fullword ascii
      $s6 = " #[  #x  #x  #x  #x  #x  #x  #x  #x  #x  #x  #x  #x  #x  #x  #x  #x  #x  #x  #x  #x  #x  #" fullword ascii
      $s7 = "nwsaPAgEnT" fullword ascii
      $s8 = "%-24s %-15s 0x%x(%d) " fullword ascii
   condition:
      ( uint16(0) == 0x5a4d and filesize < 700KB and 1 of ($x*) or 4 of them )
}

rule Backdoor_Nitol_Jun17 {
```

Awesome YARA

A curated list of awesome YARA rules, tools, and resources. Inspired by awesome-python and awesome-php.

> YARA is an ancronym for: YARA: Another Recursive Ancronym, or Yet Another Ridiculous Acronym. Pick your choice.
>
> -- *Victor M. Alvarez (@plusvic)*

YARA, the "pattern matching swiss knife for malware researchers (and everyone else)" is developed by @plusvic and @VirusTotal. View it on GitHub.

Rules

- AlienVault Labs Rules
  - Collection of tools, signatures, and rules from the researchers at AlienVault Labs. Search the repo for .yar and .yara extensions to find about two dozen rules ranging from APT detection to generic sandbox / VM detection. Last updated in January of 2016.
- Apple OSX
  - Apple has ~40 YARA signatures for detecting malware on OSX. The file, XProtect.yara, is available locally at /System/Library/CoreServices/XProtect.bundle/Contents/Resources/.
- bamfdetect rules
  - Custom rules from Brian Wallace used for bamfdetect, along with some rules from other sources.
- BinaryAlert YARA Rules
  - A couple dozen rules written and released by AirBnB as part of their BinaryAlert tool (see next section). Detection for hack tools, malware, and ransomware across Linux, Window, and OS X. This is a new and active project.
- Burp YARA Rules
  - Collection of YARA rules intended to be used with the Burp Proxy through the Yara-Scanner extension. These rules focus mostly on non-exe malware typically delivered over HTTP including HTML, Java, Flash, Office, PDF, etc. Last updated in June of 2016.
- BinSequencer
  - Find a common pattern of bytes within a set of samples and generate a YARA rule from the identified pattern.

```
2  /*
```

Tools

- AirBnB BinaryAlert
  - Open-source serverless AWS pipeline where any file uploaded to an S3 bucket is immediately scanned with a configurable set of YARA rules.
- androguard
  - YARA module that integrates APK analysis.
- bamfdetect
  - Identifies and extracts information from bots and other malware.
- base64_substring
  - Generate YARA rules to match terms against base64-encoded data.
- CAPE: Config And Payload Extraction 👀
  - Extension of Cuckoo specifically designed to extract payloads and configuration from malware. CAPE can detect a number of malware techniques or behaviours, as well as specific malware families, from its initial run on a sample. This detection then triggers a second run with a specific package, in order to extract the malware payload and possibly its configuration, for further analysis.
- CrowdStrike Feed Management System
  - Framework for automating collection and processing of samples from VirusTotal, and executing commands based on YARA rule matches.

```
37  rule Backdoor_Nitol_Jun17 {
```

OWASP ModSecurity Core Rule Set

THE 1ST LINE OF DEFENSE

The **OWASP ModSecurity Core Rule Set (CRS)** is a set of generic attack detection rules for use with **ModSecurity** or compatible web application firewalls. The CRS aims to protect web applications from a wide range of attacks, including the OWASP Top Ten, with a minimum of false alerts. The CRS provides protection against many common attack categories, including:

- SQL Injection (SQLi)
- Cross Site Scripting (XSS)
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- PHP Code Injection
- Java Code Injection
- HTTPoxy
- Shellshock
- Unix/Windows Shell Injection
- Session Fixation
- Scripting/Scanner/Bot Detection
- Metadata/Error Leakages


TareqAlKhatib Removed duplicate filters 7e4bb1d on 25 Jan

2 contributors 

Executable File | 79 lines (78 sloc) | 2.46 KB Raw Blame History

```
title: Equation Group Indicators
description: Detects suspicious shell commands used in various Equation Group scripts and tools
references:
    - https://medium.com/@shadowbrokerss/dont-forget-your-base-867d304a94b1
tags:
    - attack.execution
    - attack.g0020
    - attack.t1059
author: Florian Roth
logsource:
    product: linux
detection:
    keywords:
        # evolvingstrategy, elgingamble, estesfox
        - 'chown root*chmod 4777 '
        - 'cp /bin/sh .;chown'
        # tmpwatch
        - 'chmod 4777 /tmp/.scsi/dev/bin/gsh'
        - 'chown root:root /tmp/.scsi/dev/bin/'
        # estesfox
```

build passing

Sigma

Generic Signature Format for SIEM Systems

What is Sigma

Sigma is a generic and open signature format that allows you to describe relevant log events in a straight forward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers or analysts can describe their once developed detection methods and make them shareable with others.

Sigma is for log files what Snort is for network traffic and YARA is for files.

build passing

Sigma

Generic Signature Format for SIEM Systems

What is Sigma

Sigma is a generic and open signature format that allows you to describe relevant log events in a straight forward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers or analysts can describe their once developed detection methods and make them shareable with others.

Sigma is for log files what Snort is for network traffic and YARA is for files.

Proposing SUSTO

SUSTO would be for security control testing what

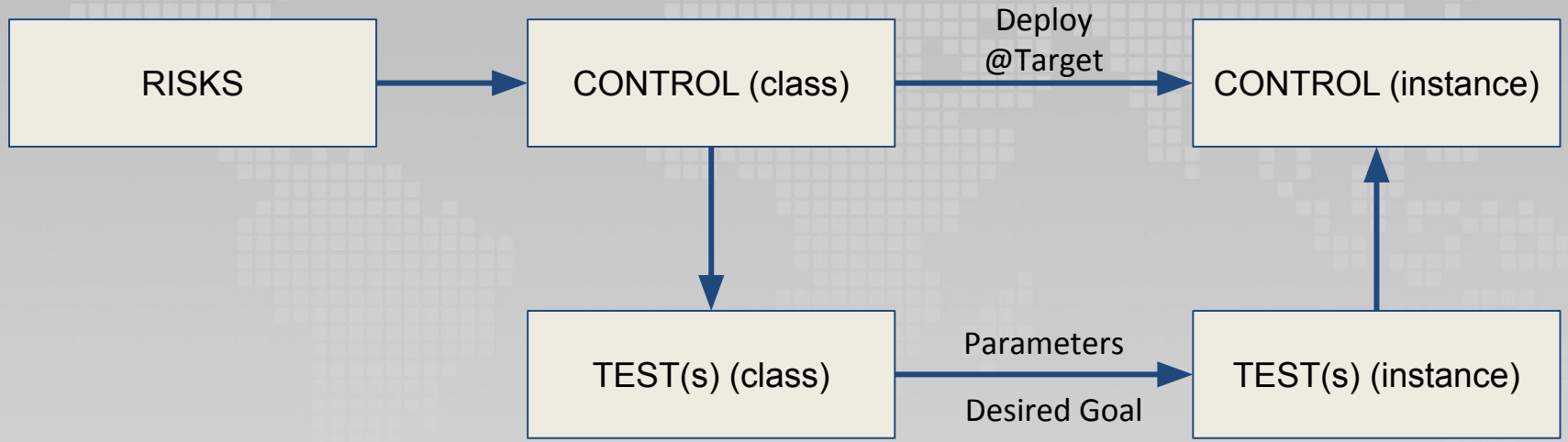
- Sigma is for log files
- Snort is for network traffic
- YARA is for files.

Proposing SUSTO

Extending the concept of ASTO

- **S**ystematic: Long tail coverage
- **U**niversal: Full stack testing, not only Application

Standardizing Security Control Testing



SUSTO implementation main features

- Tests should be generic in their objectives: WHAT?
- Tests should be configurable in their instantiation
  - Target Instance
  - Desired Goal (Boolean, Score, …)
- It should facilitate the integration of existing tools to
  - Obtain intermediate information
  - Launch the execution of more specific tests
- Manual intervention should be minimized
- Test execution should not introduce new threats

Rule Example - *Illustrative*

What is the risk?

SSL/TLS encrypts a channel between two endpoints (for example, between a web browser and web server) to provide privacy and reliability of data transmitted over the communications channel. Since the release of SSL v3.0, several vulnerabilities have been identified, most recently in late 2014 when researchers published details on a security vulnerability (CVE-2014-3566) that may allow attackers to extract data from secure connections. More commonly referred to as POODLE (Padding Oracle On Downgraded Legacy Encryption), this vulnerability is a man-in-the-middle attack where it's possible to decrypt an encrypted message secured by SSL v3.0.

The SSL protocol (all versions) cannot be fixed; there are no known methods to remediate vulnerabilities such as POODLE. SSL and early TLS no longer meet the security needs of entities implementing strong cryptography to protect payment data over public or untrusted communications channels. Additionally, modern web browsers have begun prohibiting SSL connections, preventing users of these browsers from accessing web servers that have not migrated to a more modern protocol.

How should I respond?

The best response is to disable SSL entirely and migrate to a more modern encryption protocol, which at the time of publication is a minimum of TLS v1.1, although entities are strongly encouraged to consider TLS v1.2. Note that not all implementations of TLS v1.1 are considered secure – refer to NIST SP 800-52 rev 1 for guidance on secure TLS configurations.

Rule Example - *Illustrative*

```
<rule id="EXAMPLE_RULE_2">
      <and>
            <run name="ssl-min-version"
                  id="checkssl"
                  url="{TARGET_HTTPS_URL}"
                  min-version="{TLS_MIN_VERSION}" />
            <run name="is-url-redirect"
                  id="follow-redirect"
                  url="{TARGET_HTTP_URL}"
                  on-closed="OK"
                  on-redirect="follow-redirect"
                  on-success="checkssl" />
      </and>
</rule>
```

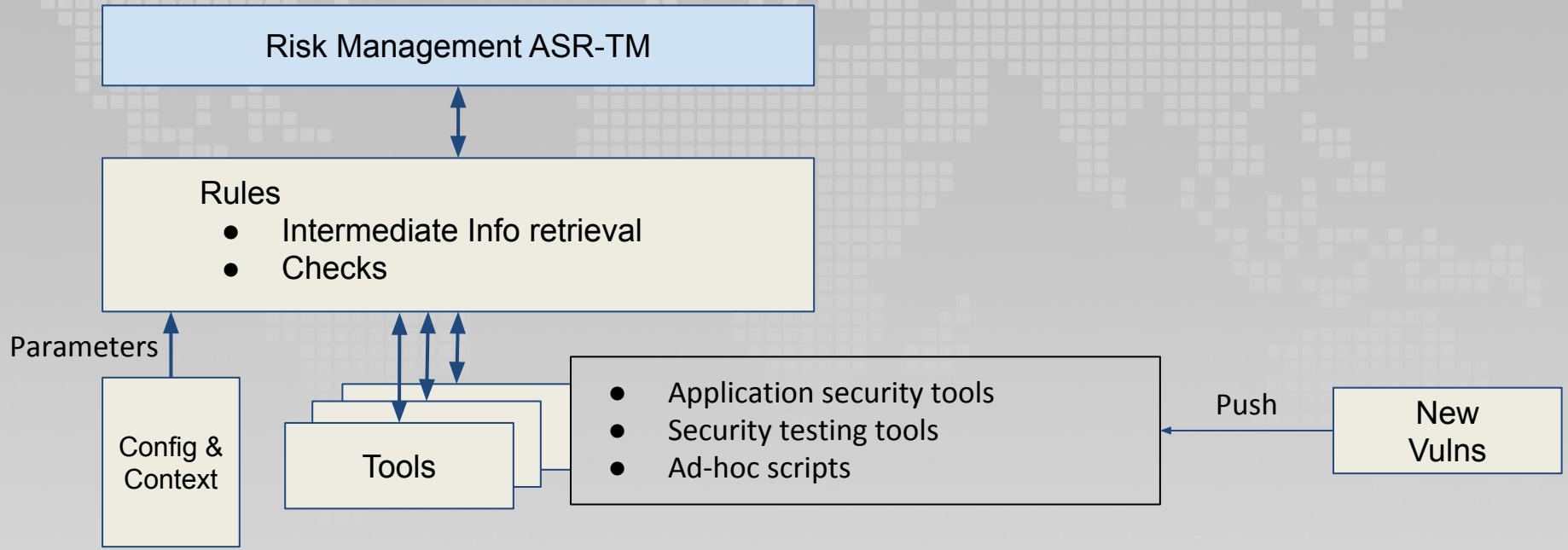
Rule Example - *Illustrative*

```
<rule id="EXAMPLE_RULE_2" result="OK">
        <and result="OK">
                <run name="ssl-min-version" id="checkssl" url="https://www.example.org" min-version="TLSv1.0" result="OK">
                        <start>Mon 23 Sep 2019 04:28:26 PM CEST</start>
                        <end>Mon 23 Sep 2019 04:28:31 PM CEST</end>
                        <got>TLSv1.0</got>
                        <expected>TLSv1.0</expected>
                        <output><![CDATA[
PORT    STATE SERVICE REASON
443/tcp open  https  syn-ack
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (secp256r1) - A
…
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (secp256r1) - A
…
|_  least strength: C
                ]]>
                </output>
                </run>
```

Rule Example - *Illustrative*

```
<rule id="EXAMPLE_RULE_2" result="OK">
        <and result="OK">
                <run name="ssl-min-version" id="checkssl" url="https://www.example.org" min-version="TLSv1.0" result="OK">
                        <start>Mon 23 Sep 2019 04:28:26 PM CEST</start>
                        <end>Mon 23 Sep 2019 04:28:31 PM CEST</end>
                        <got>TLSv1.0</got>
                        <expected>TLSv1.0</expected>
                        <output><![CDATA[
PORT    STATE SERVICE REASON
443/tcp open  https   syn-ack
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (secp256r1) - A
…
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (secp256r1) - A
…
|_  least strength: C
                ]]>
                </output>
                </run>
```

Overlord Architecture



Stakeholders

- CSPs/XaaS (AWS/GCP/Azure/Salesforce/RedHat/...)
- Security Vendors
  - Application Security Requirements & Threat Management
  - Governance, Risk&Compliance
  - SAST/DAST/IAST/SCA/AVC (*Build-time* **checking** tools)
  - SOAR (*Run-time* response **automation** tools)
- Start-ups opportunity
- And anyway: Your organization

Next steps: Feedback&Contribution

- Promote as an OWASP project
- Roadmap & Features
- “Overlord” as the OWASP SUSTO tool
- Plug-ins to existing tools
- Map standard control sets to Rules
- Contribute Community Rules
- Contribute CSP/Vendor Rules

SUSTO: Also Pun-intended

Susto (Spanish)=Fright

CC0 https://pxhere.com/es/photo/792049

- **Death or fright?**

CC0 https://pxhere.com/es/photo/792049

- Death or fright?
- *Fright*

CC0 https://pxhere.com/es/photo/792049

- Death or fright?
- *Fright.*
- Booooooooooh . . .

CC0 https://pxhere.com/es/photo/792049

- Death or fright?
- *Fright.*
- Booooooooooooh . . .
- *Oh my, how frightening!*

CC0 https://pxhere.com/es/photo/792049

- Death or fright?
- *Fright.*
- Booooooooooooh . . .
- *Oh my, how frightening!*
- Well, you could have chosen death!

CC0 https://pxhere.com/es/photo/792049


Don't fear the long tail
You better choose **SUSTO**
THANKS
@lsaiz
You
And you
https://bbvalabs.gitbook.io/oss/bbva_labs_security
CC0 https://pxhere.com/es/photo/792049