Implementing Security into Software Development Lifecycle: an Experience Return

Laurent Butti – Orange France

November, 16th 2021

% whoami

- 20+ years of experience in security domain (R&D then operations)
- Head of security at Digital Experiences Factory
- Former speaker at international security conferences (BlackHat USA/EU, FIRST, SSTIC, CESAR...)
- Interested in vulnerability discovery (e.g. fuzzing) and mitigation techniques
- Interested in how to implement pragmatic security organizations/measures/techniques

About This Talk

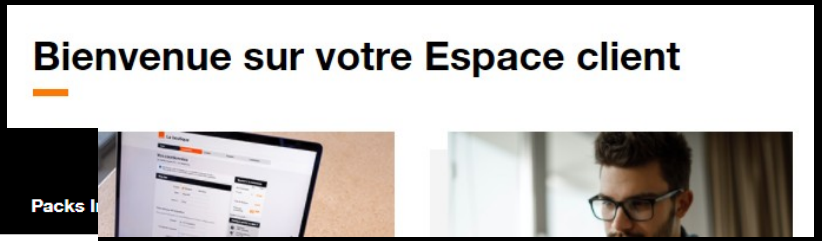
- What this talk is about:
  - an humble feedback of what could be achieved to reach a decent level of security in a web context
  - an overview from both organizational and technical perspectives
  - some hints of what does work and what does not work
  - a collaborative work, not from an individual
  - only an overview presentation: so feel free to get in touch for more in-depth information

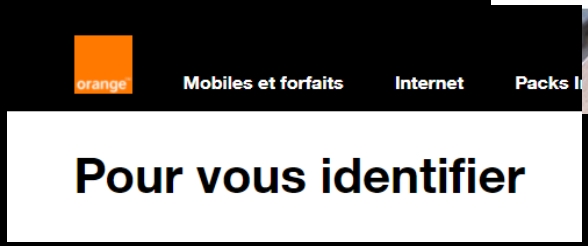
- What this talk is not about:
  - « one size fits all » tips and tricks list, every context is different, so it only represents my own opinion!

Agenda

- Business Context: Digital Enablers for “Grand Public”
- Risks: Threat Landscape Overview
- Challenge: Protect Our Assets in a Highly Exposed Environment
- REX on Foundations: Feedbacks About Management Support and Security Organization
- REX on Automation: Overview of Security Measures in a DevOps Life-Cycle
- Conclusion and Take-Aways

Business Context: Digital Enablers for “Grand Public”





ChatBots

Customer Tools
GP

Risks: Threat Landscape Overview

- Data breach
  - web application attacks (SQL injection, XSS, cookie theft...)
  - business-logic web application attacks (abuse of feature, i.e. changing contracts identifiers)
  - abuse of authenticated customer journeys (data leak with already compromised accounts)
  - vulnerable (or back-doored) web application components
  - vulnerable or poorly-protected exposed components (infrastructure, back offices...)
  - malvertising (malicious advertisement)

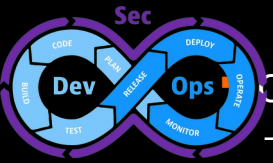
Fraud
- business-logic web application attacks (abuse of feature...)
- web skimming attacks (payment chain compromising)

- Availability
  - DDoS attacks on network links/infrastructure components
  - DDoS attacks on application (capacity overload)

Challenge: Protect Our Assets in a Highly Exposed Environment

- Threats: constantly evolving and increasing
  - attacks focusing at personal data breaches are more and more predominant
  - attackers are more and more focused on money-making (fraud, abuse...)
  - attacks are more and more taking advantage from cloud hosting

- Multi-hosting: applications (front, back) and its data are to be hosted everywhere
  - internal/public clouds requires same security processes/tools/architectures but replicated
  - developing skills is necessary to keep security level



- Organizational changes: agility is both a chance and a challenge
  - agility requires automation of security processes/tools and a strong security culture

Facing These Threats: “Security is a Business Issue”

- Everything starts from a strong support from top management

- Digitalization of customer’s journeys is a strong business challenge

REX: Security Organization (1/2)

- Our organization is composed of ~1000 people:
  - security team composed of security experts (~15 people)
  - one full-time security specialist in every “development unit” (~5 people)

- Security specialists who are close to product teams is a strong requirement
  - trust and confidence are easier to build when close to teams (both hierarchical and social ways)
  - complex situations are often better understood when “in-depth”
  - helps to mitigate the ivory tower issue that people may have about a centralized security team
  - helps to develop relationship between product teams and all security specialists
  - helps to develop skills of product teams thanks to advices and trainings by example

- But security specialists are far to be enough: goal is to promote security mindset at every level
  - need of product team leaders and business owners sensitive and empowered regarding security
  - need of security awareness and trainings

REX: Security Organization (2/2)

- Product teams are responsible for the security of their product
  - security skills have to be within product team: need to build security maturity little-by-little
  - need of security “relays”/”leaders”/”champions” in product teams

Key success factors

- security-aware business owners
- security team to provide pragmatic governance, vision, consultancy and security enablers
- security specialists close to product teams
- products teams must partner with security
- automation of security processes into DevOps life-cycle

Overview of Security Measures in a DevOps and Hosting Context

- DevOps Life-Cycle
  - Secrets Management (storage, PKIaaS)
  - Static Application Security Testing (SAST)
  - Patch Management and Dependency Checks
  - Dynamic Application Security Testing (DAST)
  - Other security checks (configuration compliance, TLS compliance, network exposition...)

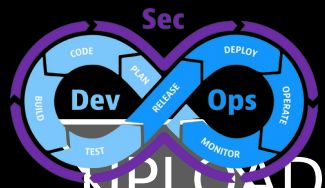
- Hosting: Security Monitoring (SOC) / Web Application Firewall / Security Enablers
  - detection of applicative attacks thanks to Web Application Firewall
  - detection of business-logic attacks thanks to SIEM
  - automatic mitigation based on IP blacklist
  - automatic mitigation of robot attacks thanks to “bot detection”/“captcha” (enabled on some assets)
  - automatic mitigation of network-based DDoS attacks targeting datacenters

- Pen-testing (periodically) and Bug Bounty (permanent)
  - manual pen-testing on most critical assets
  - bug bounty permanently opened on most of our assets

Security Within DevOps: What Did We Choose to Focus on

- “Shift-left” as far as possible: empower product teams on security
- Automate as far as possible: only way to scale
- Focus on implementation/non-compliance issues: quality-based approach that fits developers’ habits

Security Within DevOps: Current Status



GitLab

SECRETS MANAGEMENT CHECKS

GitLeaks
HashiCorp Vault

SAST

MicroFocus Fortify
Coverity Prevent
CheckMarx

DEPENDENCY CHECKS

DOCKER IMAGES PATCH MANAGEMENT CHECKS

"In-house tools" based on Open Source components

COMPLIANCE CHECKS

UPLOAD TO DOCKER REGISTRY

Security Within DevOps: Static Application Security Testing

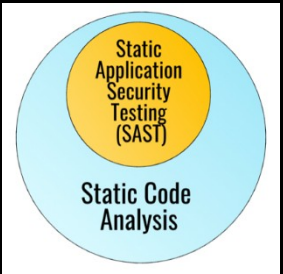
- Find security flaws thanks to automated web white-box source code static analysis

- Rely on commercial tools to cover most of our cases
  - Microfocus Fortify SCA since 2011: mainly for PHP and Java
  - Synopsis Coverity Prevent since 2012: mainly for C/C++
  - CheckMarx since 2017

- SAST tools should be the first shoot for any DevOps
  - find security issues and help developers to understand security issues
  - force developers and security specialists to dig into the code and thus (eventually) discover other issues
  - can be configured to block CI pipelines if critical issues are discovered

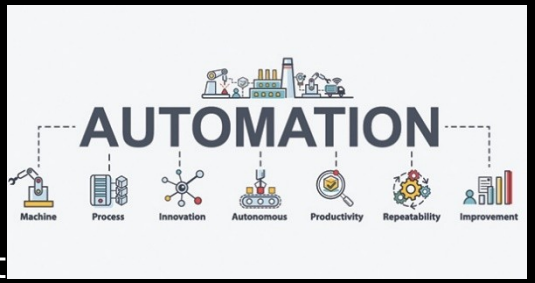
- SAST are not a silver-bullet, but is a mandatory link in the chain

REX: SAST



- False positives are a huge burden: product teams can loose their “trust”
- Languages ecosystem is fast-evolving: that’s a challenge for SAST efficiency
- Triaging issues and exceptions cannot be automated (→ parallel manual process)
- Issues tracking can hardly be automated (→ parallel manual process)

REX: Automation



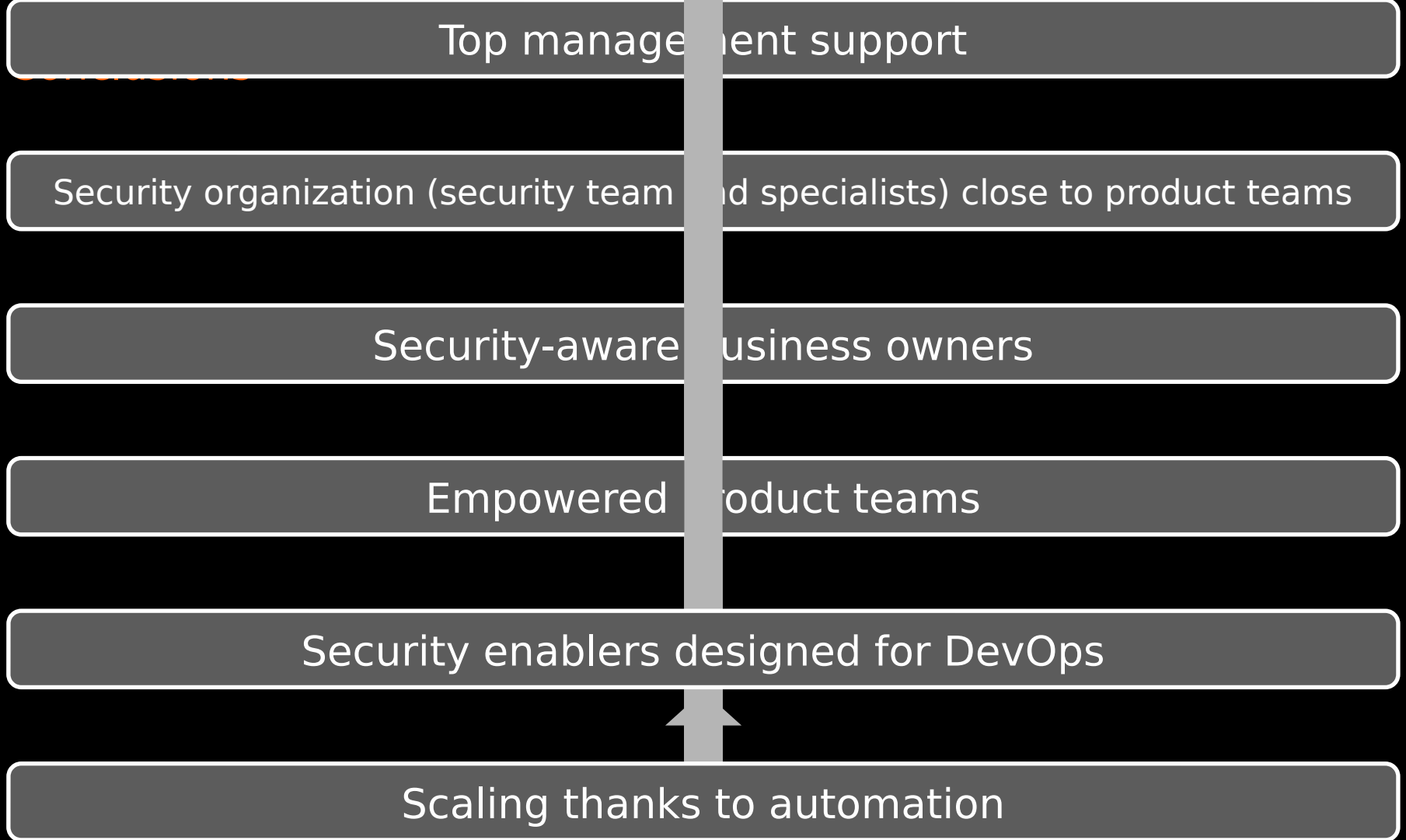
- Automation helps to focus teams on other “interesting” things
- Automation helps to provide KPI, projects provisioning, access right
- Automation helps to scale, and scaling with SAST is quite natural
- Automation helps to deliver faster: mandatory with DevOps/Agility
- Automation helps to have a minimum compliance: limits regressions
- Business-logic issues are not discoverable by automation in development phases

REX: Posture

- Security gates in developers' hands: empower them!
- Ease adoption: security teams have to co-build security enablers that fits developers' habits and needs
- Security enablers: have to be "professional" (SLA, guidelines, support...) and must prove their value
- Security teams must be "software teams": more prone to be "trusted" by product teams

Every Security Team is a Software Team Now

Dino Dai Zovi | Mobile Security Lead, Square
Location: Mandalay Bay Events Center
Date: Wednesday, August 7 | 9:00am–10:00am
Format: 50-Minute Briefings
Track: Keynote


Top manage ent support
Security organization (security team d specialists) close to product teams
Security-aware usiness owners
Empowered oduct teams
Security enablers designed for DevOps
Scaling thanks to automation