Why DevSecOps?

Reducing Risk

Findings of Cyber security report by Checkpoint\(^1\) for NTSC\(^2\)
- DevSecOps approach has been able to close the strategic gap in security posture for many organisations
- Focus on risk awareness, prevention & outlining action plan for integrating security early and often has proven business benefits
- Assessing and prioritizing vulnerabilities in applications, for example, can directly reduce the risk exposure (OWASP\(^3\))

Creating Trust

Provision of client visibility of controls and measures (e.g. the xMatters Trust\(^4\) site)
- Protecting corporate data assets and privacy
- Reducing impact of security breaches
- Ensure traceability and alignment of security and data privacy regulation

---

\(^1\) https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf
\(^2\) https://www.ntsc.org/
\(^3\) https://owasp.org/
\(^4\) https://www.xmatters.com/trust/
What DevSecOps is NOT...

➢ Applying more layers of security
  ○ DevSecOps must remain lean and not add additional toil

➢ Establishing a dedicated security team
  ○ DevSecOps is about the collaborative use of teams

➢ A big transformation project
  ○ Any transformation should be made based upon an iterative, risk based backlog

➢ Compromising ROI
  ○ Implementing Security should ADD value, not remove it.
# Proactive, shift-left

## Culture
- Default inclusion of security as part of a requirement
- Product Managers and Engineers should be constantly challenged
- End User empathy to services
- ALL elements targeted by Ethical hackers
- Manual Ethical Hacking approach to innovation

## Automation
- Inclusion of Security in CI/CD pipeline:
  - SAST (Statistical analysis)
  - DAST (Dynamic Analysis)
  - Security code coverage analysis
  - Digitally signed secure repositories for built binaries
  - Penetration Tests
  - Smoke Tests

## Lean
- Security inclusive definitions
- Security inclusive designs
- Security inclusive engineering
- Security inclusive testing
- Security inclusive deployments
## Reactive, shift-right

### Culture
- No fortress is impregnable
- Production Smoke testing from ‘Time Zero’ as part of monitoring/observability
- Chaos Engineering approach to Prod AND non-Prod
- Root cause analysis with data captured in real time

### Automation
- Continuous Security monitoring of Prod AND non-Prod
- Chaos Engineering, including automated security testing, of Production environments

### Lean
- Treating Major Incident Management (MIM) as a Value Stream - *Every second counts!*
- Response times to stopping an attack
- Response times for Return to Value
- Feedback to engineering for future prevention & Technical Debt
Common Measurement

➢ Security professionals to determine measures, such as from regulatory requirements, e.g. GDPR
➢ Measurements of both Prod AND non-Prod
➢ Definition of security as part of Business Value AND Success Criteria
➢ Security Scorecards, updated in real time

Sharing

➢ All parts of the organization must consider themselves responsible for security
➢ Autonomous ability to identify and implement security
➢ In the event of an attack;
   o a Security-led Damage Analysis team, supported by IT, must run in parallel to
   o an IT-led Remediation team, supported by Security
➢ Empowerment by leadership with shared accountability in a safe environment
   o Red Team vs Blue Team functions
   o Security Drills
Use Cases
Solarwinds (Early 2020)

Event

➢ Introduced malicious code into a system called “Orion”
➢ Used in a large number of companies to manage IT resources
➢ Included in system updates between March and June 2020 as recorded in SEC documents
➢ Initial attack vector through the companies Microsoft Office 365 email system
➢ Malicious code added through Solarwinds own Continuous Delivery Pipeline

Result

➢ Cascaded out to almost 18,000 Orion product customers
➢ Initial mitigating hotfix update was provided
➢ Second update was prepared to address the vulnerability fully at a later date
➢ Impacts to business via:
  ○ Fines
  ○ Trust
➢ Impacted “approximately $343m, or approximately 45% of total revenue”

Lesson Learned (report)

➢ Adherence to security strategies & ID of points of exposure
➢ Risk-analysis performed on third-party components and a full analysis of the build with the engineering team
➢ Inclusion of pen testing, smoke tests & targeted dynamic scanning (DAST) as a function of any other automated test approach
➢ Ensuring that designs, code, infrastructure, tests and pipelines are available to ethical hackers

---

British Airways (2018)

Event

➢ Vulnerability was discovered to be in a third-party Javascript used on BA’s website
➢ A hacking group inserted 22 lines of code that diverted crucial information around payment details to a separate site controlled by the hackers
➢ Vulnerability had been well known since 2012

Result

➢ Accessed the personal data of approximately 429,612 customers and staff according to the findings of an ICO report
➢ Included names, addresses, payment card numbers and CVV numbers of 244,000 BA customers
➢ Usernames and passwords of BA employee and administrator accounts
➢ Usernames and PINs of up to 612 BA Executive Club accounts

Lesson Learned (report¹)

➢ Lack of cultural acceptance of security as a value
➢ ID of a known exposure point & a weakness in the defences should have led to an immediate action
➢ The lack of use of Red Teams and automated monitoring of production systems was extremely severe
➢ The response times upon discovery of issue were deemed unacceptable and a leaner approach to MIM practices around security was required

People, Process & Technology: An example