

RSA[®]Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: PS-R07

Secure Your Code from Open Source Vulnerabilities



Megha Dixit

Technical Program Manager

Salesforce

@meghadixit11

#RSAC

Agenda

- What is Open Source
- Developers love for Open Source
- Software development lifecycle with Security development life cycle
- Stay Proactive Stay Protected: Dev-Sec-Ops
- Suggestions, thoughts and ideas
- Q&A

“Apply” Slide

- Session will enable us to achieve "security first" mindset while using any open source properties.
 - Adapt , inspect and remediate without affecting developer productivity.
- Best practices to prepare and prevent against the possible threats with the open source usage.
- Practical use cases and examples for better understanding, implementation.

RSA®Conference2020

What is Open Source

What is Open Source

- Type of Computer software.
- A Licensed source code.
 - Rights to modify, distribute and usage are dictated with the License category.



Open Source Adoption

- Developers are the "smart" community.
- Developers like to deliver at the rapid rate considering stringent timelines.
- Developers believe in churning out the features faster.



How do Developers do the smart work!

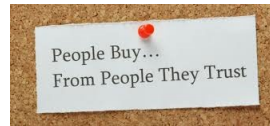
- Lucrative Open source aka working functionality available!
- Usage and adoption of Open Source has seen an “exponential” growth.
 - usage of open source lies between 70-90% off overall source code!!!

Security : Open Source Usage

- Hacker community loves open source too as most often
 - Open source packages in use are typically Outdated.
 - Not actively maintained and monitored.

Impacts :

- Losing "Brand name".
- Lost "Customer Trust".
- Legal litigations.
- Stock Crash.



RSAConference2020

Software Development LifeCycle or Secure Development Lifecycle

Stay Proactive Stay Protected




How:

Some basic theoretical solutions:

- Developers engage security and legal experts.
- Get the open source code reviewed.
- Once approved ship it.

Can we scale this! NO

Why Not: "lack of validation mechanisms"

- Approved libs may not be re-validated.
- Prone to human errors. 
- Legal risk compliance requirements. 
- Lack off feedback loop to re-instate the updates to outdated libs 

Stay Proactive Stay Protected

Some practical solutions: Transition Dev-Ops as Dev-Sec-Ops.

- Introduce open source scanning solutions /tools.
- These tools with the appropriate security policies defined in tandem with Legal Counsel can perform the security and legal review during development phases.
- Integrate these components in the design and security reviews.
- Post deployment checks should be run by using the similar tool set on the Gold Image published for end customers (could be a jar, docker, tarball etc).

Stay Proactive Stay Protected

Responsibility to maintain the TRUST of our customers on us to PROTECT their data and keeping our development methodologies in sync with the continuous reviews and updates /patch the open source usage can take us a long way.

RSA[®]Conference2020

Q & A