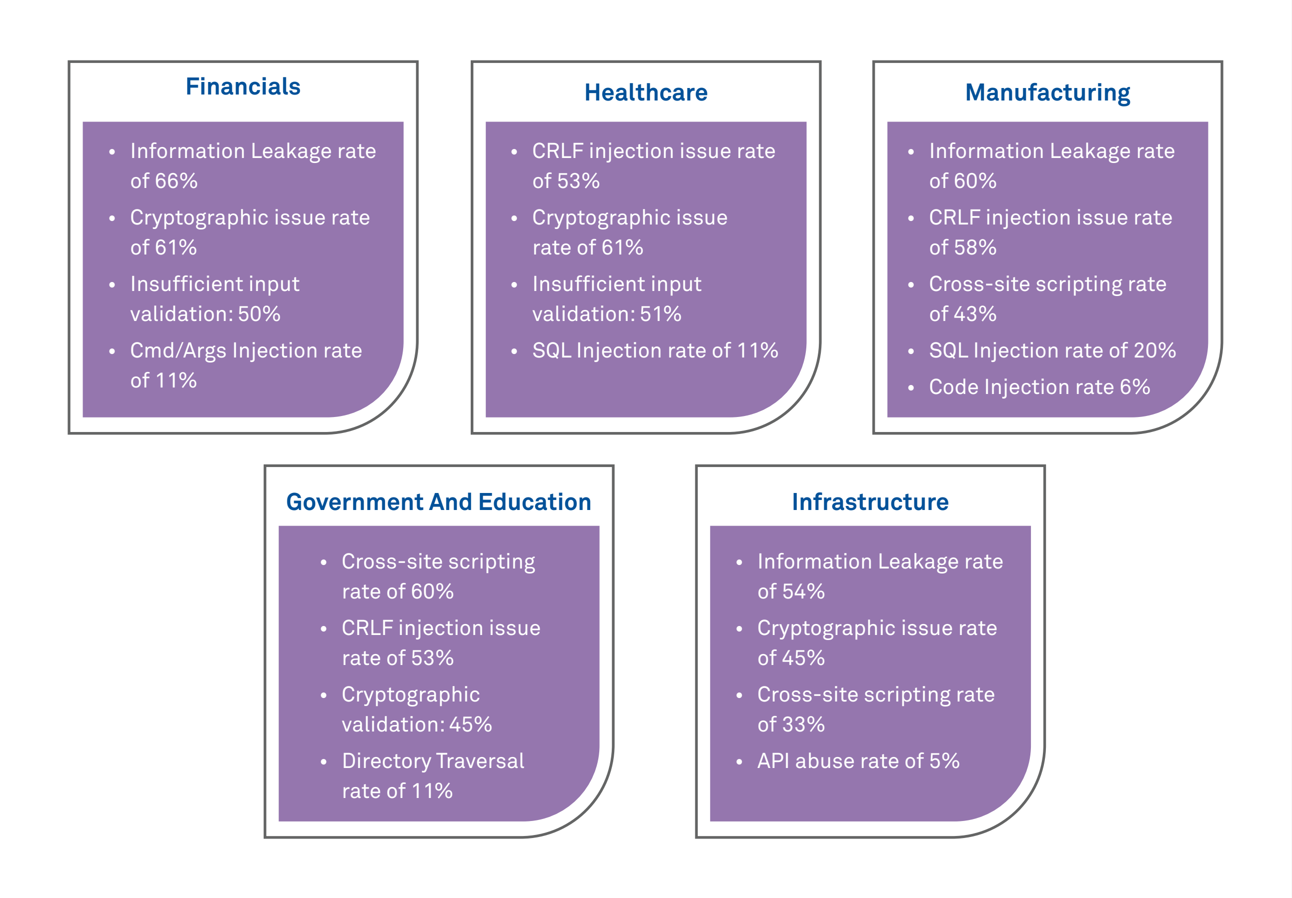
Embedding security into new ways of working

With increasing technology digitization, innovation and agility have become essential ingredients for competitive advantage; regardless of industry. Technology has become the pulse of every single interaction; rapidly reshaping not just daily life but society collectively allowing business in every industry to reimagine what's possible. Security and trust are the bedrock of digital technology, with digital transformation often security gets muffled out. Technology these days constitutes predominantly of software, as even things which are considered as hardware have a malleable layer of software on top that runs the show; making software and software developers driving the pace of innovation and agility. The growing demand around increased business agility and democratization of innovation has potential uptrend for misuse, thereby increasing the software risk portfolio. Market trend showcased 2018 as the year of agility; experiencing organization shifting focus from traditional agile to Digital driven mindset adopting DevOps empowered agile software development methodology. Industry trends for application security reveals the relative impact of delivering software at high velocity, propelling the competitive demands while considering application security an after-release activity.



Financials

- Information Leakage rate of 66%
- Cryptographic issue rate of 61%
- Insufficient input validation: 50%
- Cmd/Args Injection rate of 11%

Healthcare

- CRLF injection issue rate of 53%
- Cryptographic issue rate of 61%
- Insufficient input validation: 51%
- SQL Injection rate of 11%

Manufacturing

- Information Leakage rate of 60%
- CRLF injection issue rate of 58%
- Cross-site scripting rate of 43%
- SQL Injection rate of 20%
- Code Injection rate 6%

Government And Education

- Cross-site scripting rate of 60%
- CRLF injection issue rate of 53%
- Cryptographic validation: 45%
- Directory Traversal rate of 11%

Infrastructure

- Information Leakage rate of 54%
- Cryptographic issue rate of 45%
- Cross-site scripting rate of 33%
- API abuse rate of 5%

Figure 1: Application Security Vulnerability trend by Industry since 2019-20[i]

This brings us to Enterprise IT paradox, how to go faster and innovate and yet stay secure delivering competitive software at high velocity maneuvering the imperative security challenges to deliver secure software. Organizations adopted DevOps, the principle of integrating software development and IT operations under a single automated umbrella, achieving frequent releases and stable application. Security in large is regarded as the main obstacle to rapid development; resulting in application security suffering in DevOps ecosystem.

Shifting Focus to DevSecOps – the bigger picture

A holistic and proactive approach embracing DevSecOps, envisioning long term gains for customer. Application with built-in security from inception phase will resist attacks and avoid potential devastation to daily operations. To ensure seamless alignment to agile methodology and integration with DevSecOps, a change in below approach is required around people, process and technology aspects:

- Security is viewed as a technology problem, rather than shifting security left, it's assumed to be everyone's responsibility.

- Security focuses on finding issues, rather striking right balance between finding and fixing.

- Security gate-checks are rule-based rather than risk-based.

- Security is viewed as an end-thought rather to be included in all decision phases of SDLC process.

- Security metrics are based on identification of vulnerabilities rather than overall enablement to deliver secure software.

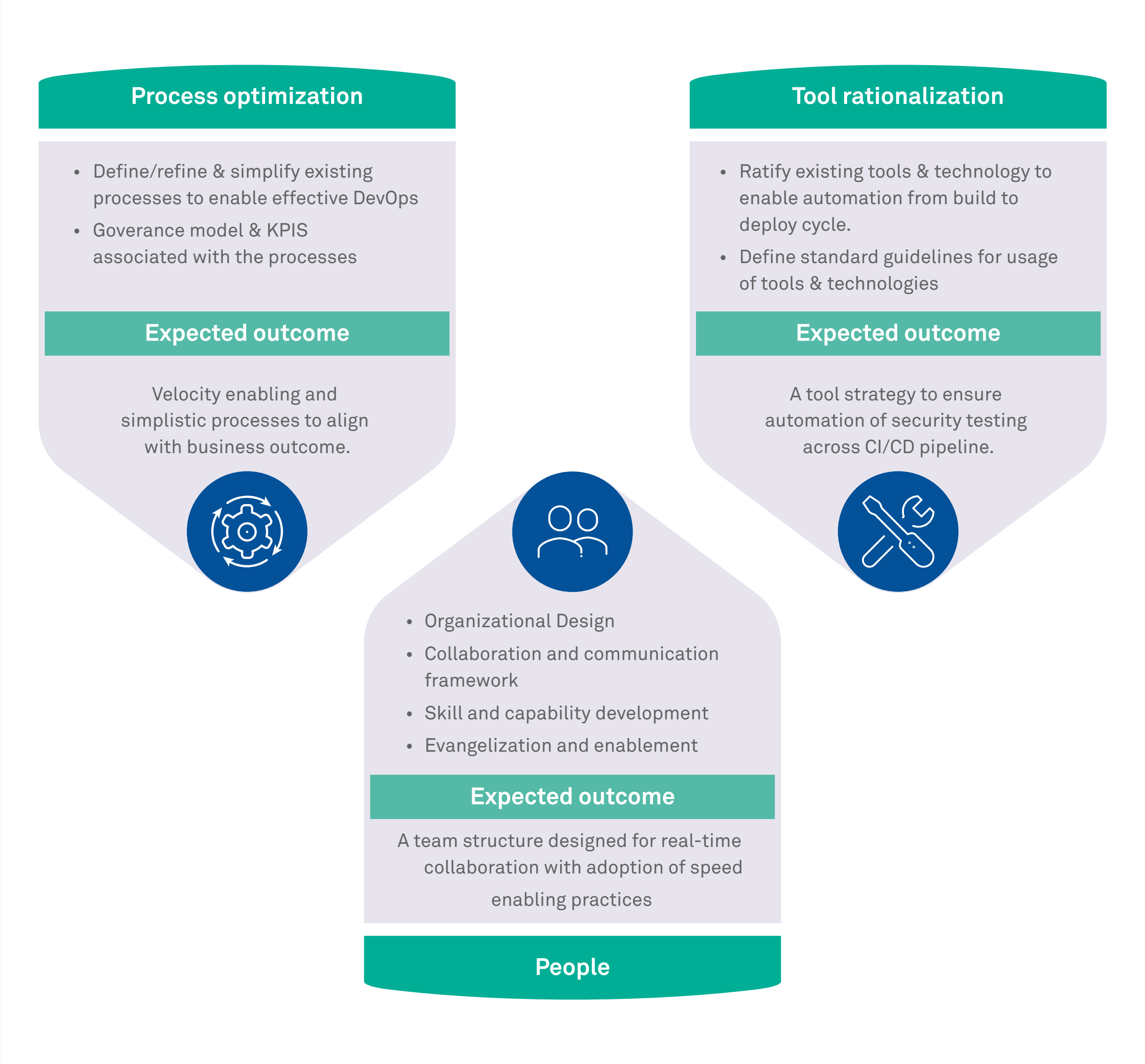
- Security professionals can only interpret security results rather than empowering developers via skill and capability trainings to understand security issues.

- Adoption of manual approach to identifying vulnerability rather than leveraging automation throughout the pipeline.

- Security team works in silos rather building collaborative working style.

- Security is not a destination rather a journey

The three step approach below aims to achieve security in DevSecOps addressing the people, process and technology change; developing a progressive security program.



Process optimization

- Define/refine & simplify existing processes to enable effective DevOps
- Goverance model & KPIS associated with the processes

Expected outcome

Velocity enabling and simplistic processes to align with business outcome.

Tool rationalization

- Ratify existing tools & technology to enable automation from build to deploy cycle.
- Define standard guidelines for usage of tools & technologies

Expected outcome

A tool strategy to ensure automation of security testing across CI/CD pipeline.

- Organizational Design
- Collaboration and communication framework
- Skill and capability development
- Evangelization and enablement

Expected outcome

A team structure designed for real-time collaboration with adoption of speed enabling practices

People

Figure 2: Approach on Shifting from DevOps to DevSecOps

DevSecOps Reference Architecture

DevSecOps architecture aims at improving the security DNA envisioning it as a journey, not a destination. The below reference architecture helps deliver an ecosystem that is tool agnostic, platform independent, allowing out-of-box integration offering defense-in-depth capabilities to the SDLC supply chain.

Wipro's DevSecOps ecosystem overcomes the fundamental challenges of stitching security into DevOps, harnessing security into each phase of software development lifecycle. The below diagram is an outcome from varying implementation across customer base to be leveraged as reference and not a takeaway recipe.

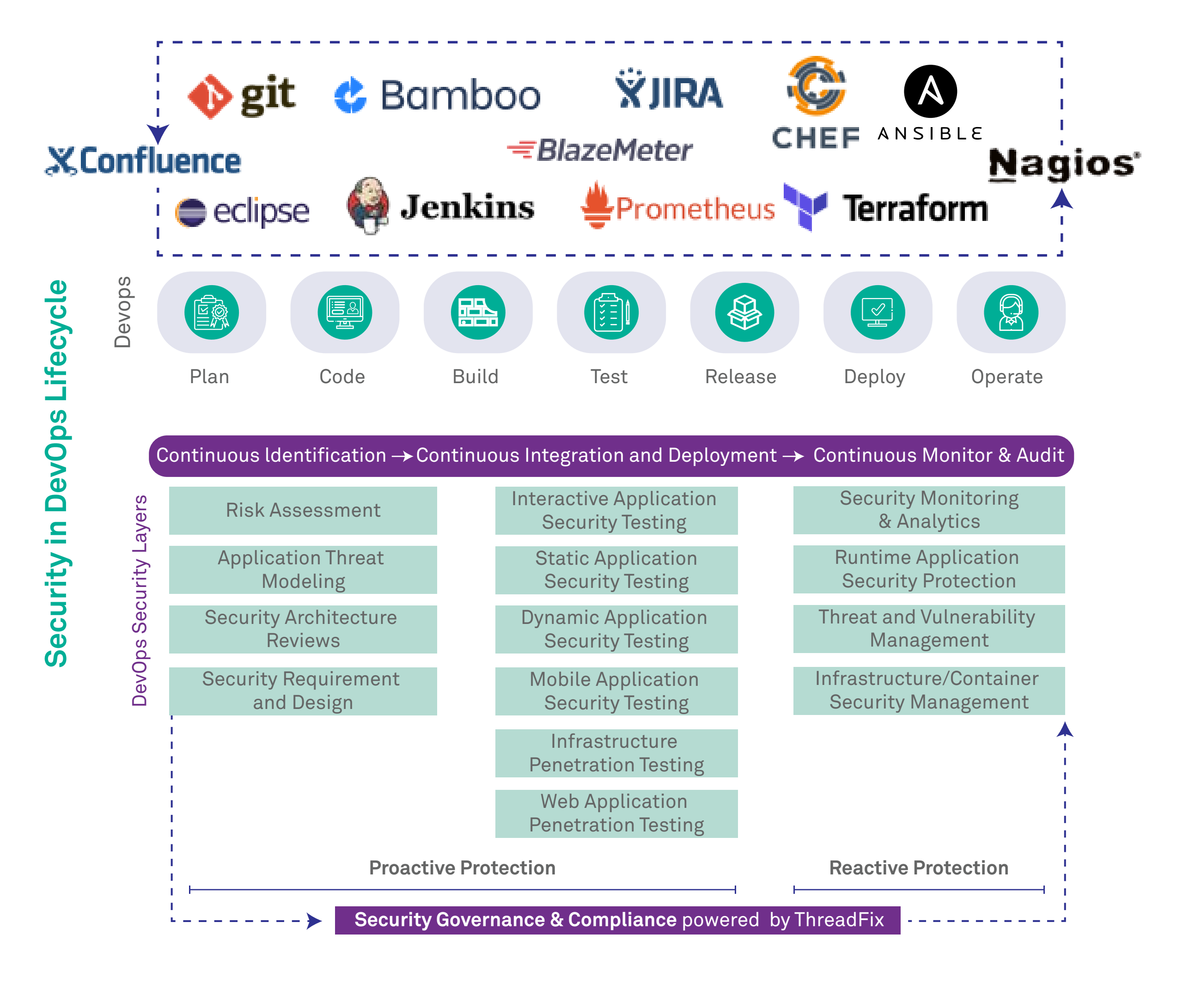

git
Bamboo
JIRA
CHEF
ANSIBLE
Confluence
BlazeMeter
Nagios
eclipse
Jenkins
Prometheus
Terraform
Security in DevOps Lifecycle
Devops
Plan
Code
Build
Test
Release
Deploy
Operate
Continuous Identification → Continuous Integration and Deployment → Continuous Monitor & Audit
DevOps Security Layers
Risk Assessment
Application Threat Modeling
Security Architecture Reviews
Security Requirement and Design
Interactive Application Security Testing
Static Application Security Testing
Dynamic Application Security Testing
Mobile Application Security Testing
Infrastructure Penetration Testing
Web Application Penetration Testing
Security Monitoring & Analytics
Runtime Application Security Protection
Threat and Vulnerability Management
Infrastructure/Container Security Management
Proactive Protection
Reactive Protection
Security Governance & Compliance powered by ThreadFix

Figure3: DevSecOps Reference Architecture

The below section enumerates the application security capability while leveraging the above DevSecOps architecture. One of the prominent reasons why any architecture is not meant to be consumed as a copy-paste template for DevSecOps adoption is due to the eco-system governing the organization in terms of people, technology and process.

The reference architecture addresses the people, process and technology aspects as part of implementation approach followed by integrating Continuous Identification, Continuous Integration & Deployment, Continuous Monitoring & Auditing and Continuous Security Governance & Compliance.

a) **Continuous Identification** empowers the planning phase of SDLC with security offering of conducting Threat Model for business requirements creating a risk profile followed by security control recommendations. Introducing security controls at the right place and time decides the effectiveness of the control with minimal impact on the CI/CD pipeline. A risk-based approach towards security requirements and design goes long way allowing business to to prioritize strategic goals in the inception phase of SDLC.

b) **Continuous Integration & Deployment** empowers the code, build, test, release and deploy phase of SDLC with security capability, conducting verification and validation on proactive security recommendations from Continuous Identification phase. Security Verification entails development team to continuously discover and fix issue on daily basis prior to deploy phase performing Static Application Security Testing (SAST), while Security Validation allows developer to discover and fix issues post deploy phase performing Dynamic Application Security Testing. A risk-based approach towards implementing of security requirement & design reaps cascading returns allowing delivery teams priorities tactical goals.

c) **Continuous Monitoring & Audit** empowers the operational phase of SDLC with security capability, performing vulnerability confirmation and exploit prevention leveraging agent-based monitoring for application in production and during implementation. Interactive Application Security Testing (IAST) entails continuous monitoring into maintenance code while baking continuous compliance and remediation. Runtime application Self Protection allows to discover and protect live attacks for applications deployed in production environment. A risk-based approach to monitor and audit applications allows operations team to prioritize daily operational objectives.

d) **Continuous Security Governance and Compliance** empowers all phases of SDLC with automated correlation of vulnerability result, smart vulnerability management and remediation; integrated with leading Governance, Risk and Compliance (GRC) tools for better application security risk management. Placing application security squarely in front of management decision makers for analysis and comparison to arrive at risk-based decisions.

Reference above aims at helping adopter to strategize and implement best practices to deliver continuous security across software development supply chain delivering value to customer.

Conclusion

Wipro's DevSecOps ecosystem aims at evolving maturity levels rather than an end state. DevSecOps has become a popular buzz word for organizations tackling the ever-evolving security challenge in the digital era. Adopting security into DevOps means incorporating security culture, practice and tooling into all phases of SDLC supply chain. DevSecOps success depends on how an organization can marry culture, automation, measurement and sharing into the golden triad of people, process and technology achieving the business objectives thus making security an influencing factor alongside agility and innovation.

About the authors

Arun Pillai

Security Architect, Cybersecurity & Risk
Services Wipro Ltd.

Arun Pillai Security Architect who champions DevSecOps for Security Assurance Service within Wipro's Cybersecurity and Risk Services (CRS) division. He has over 14 years of experience, with specilization in the security domain and is responsible for evangelising DevSecOps across Wipro. He has worked and managed projects related to Security Architecture, Secure SDLC, Threat Modelling, Secure Coding, Penetration Testing and Security Consulting. Arun is ISC2 Certified Information Systems Security Professional (CISSP) and ISACA's Certified in Risk and Information Systems Control (CRISC). Arun holds a Master's degree in Information Technology from Sikkim Manipal University of Science & Technology and TOGAF certified Enterprise Architect from The OpenGroup.

References

[i] https://info.whitehatsec.com/rs/675-YBI-674/images/WhiteHatStatsReport2018.pdf

[ii] https://www.wipro.com/en-IN/applications/integration-of-security-in-devops-a-bigger-picture/

[iii] https://www.nist.gov/cyberframework/framework

https://medium.com/@seanguthrie/devops-principles-the-cams-model-9687591ca37a

[iv] https://www.veracode.com/state-of-software-security-report#snap__subnav_43941

Notes

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035, India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 175,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**