**The JumpStart Challenge: Proposal Submission Form**



|  |  |
| --- | --- |
| Proposal Name: | GitSecure Smart Updates |

|  |  |
| --- | --- |
| Business Unit: | IBM Research |

|  |  |
| --- | --- |
| Proposal Owner: | Shripad Nadgowda |

|  |  |
| --- | --- |
| Technical Mentor: | Shripad Nadgowda |

Please describe the business problem your customers (e.g. external clients, internal team, etc.) are experiencing OR the improvement/opportunity that could be brought to them.

|  |
| --- |
| What makes a good business problem proposal?   1. Defines a problem that suggests a stakeholder or end user whose experience we can map 2. Has enough flexibility to be refined during the workshop. It doesn’t have to be perfect – the user and pain points may shift as we collaborate. 3. Does NOT provide a solution.   Avoid solutions and technology. We are looking at the user’s problem. Rarely does a person think “Oh, if only I had automation!”. They think “Gosh, filling out a vehicle registration form and having to mail it in takes so long”. If you find yourself writing down technology, dig deeper and ask yourself what PROBLEM that technology addresses.  Write a problem statement using this structure or prompt:  **i) How might we…** (what problem needs solving or improvement?) **for…** (which person is most affected by this?)  or  **ii) Design a better way for**… (which person is most effected?) **to…** (what does this person need to be able to do?)  See PPT JumpStart Tech Challenge Problem Statement Guidance for examples |

What is the key issue (customer pain) or benefit that motivates the need for this project?

|  |
| --- |
| Adoption of DevSecOps across industries has accelerated the whole Software Delivery Lifecycle (SDLC) for micro-service applications. It also helped ensure security posture for application in the early stages of software development. The challenge we are facing now, is the lack of automation in the secure software update framework. Users do not have insights into all the dependencies of their application and the notifications to the updates when they are available. This could potentially lead to security exposure or availability crisis from use of outdated dependencies.  Therefore, there is a need to provide an automated framework to allow “Smart Updates” for micro-service applications. |

How might the results of the project be used after the Challenge?

|  |
| --- |
| At research, we have built a DevSecOps platform, codename “GitSecure” that performs deep provenance of source artifacts for security and compliance assessment. The work is in progress to make this capability available on IBM Cloud under DevOps Toolchain service. GitSecure also being adopted as a foundational platform for Hybrid Cloud in Katamari project. The Smart Update framework will be one of the core extensions to our DevSecOps framework on IBM Cloud and Hybrid Cloud. |

What are the key technical and business goals?

|  |
| --- |
| Technical Goals:   1. Innovate and Build an update notification service and framework for various dependencies of micro-service application (e.g. images from registries, packages from various distros like Ubuntu, Alpine..) 2. Integrate this framework into GitSecure workflow 3. Hosting this service on IBM Cloud   Business Goals:   1. Demonstration of “Smart Update” feature to IBM Cloud BU and Hybrid Cloud BU |

What specialized skills might be beneficial for the project?

|  |
| --- |
| Required:   1. Programming languages – go, python 2. Familiarity with various Cloud Services 3. Basic Understanding of Containers, Micro-services   Good to have:   1. Knowledge of Kubernetes 2. Knowledge of CI/CD tools and processes 3. Knowledge of Tekton |

Any other information you’d like to add (e.g. validation points for the project; customer info available; etc.)?

|  |
| --- |
| This capability will be part of core DevSecOps platform that would allow IBM Cloud to differentiate against our competitors. |

**EXAMPLE OF A BUSINESS PROBLEM CURRENTLY BEING WORKED:**

Security continues to be an enormous challenge for all organizations. The typical struggles include limited budgets, shortage of security skills and an overwhelming number of security issues lurking in their business applications and services. Even when clients use security tools like AppScan, Guardium and NESSUS effectively, they can only manage to remediate a small subset of the issues found.

How might we provide effective and real-time prioritization of vulnerabilities and security issues for the security analyst to help minimize bottom-line risk to a business?

