

2018 Secure360 Twin Cities

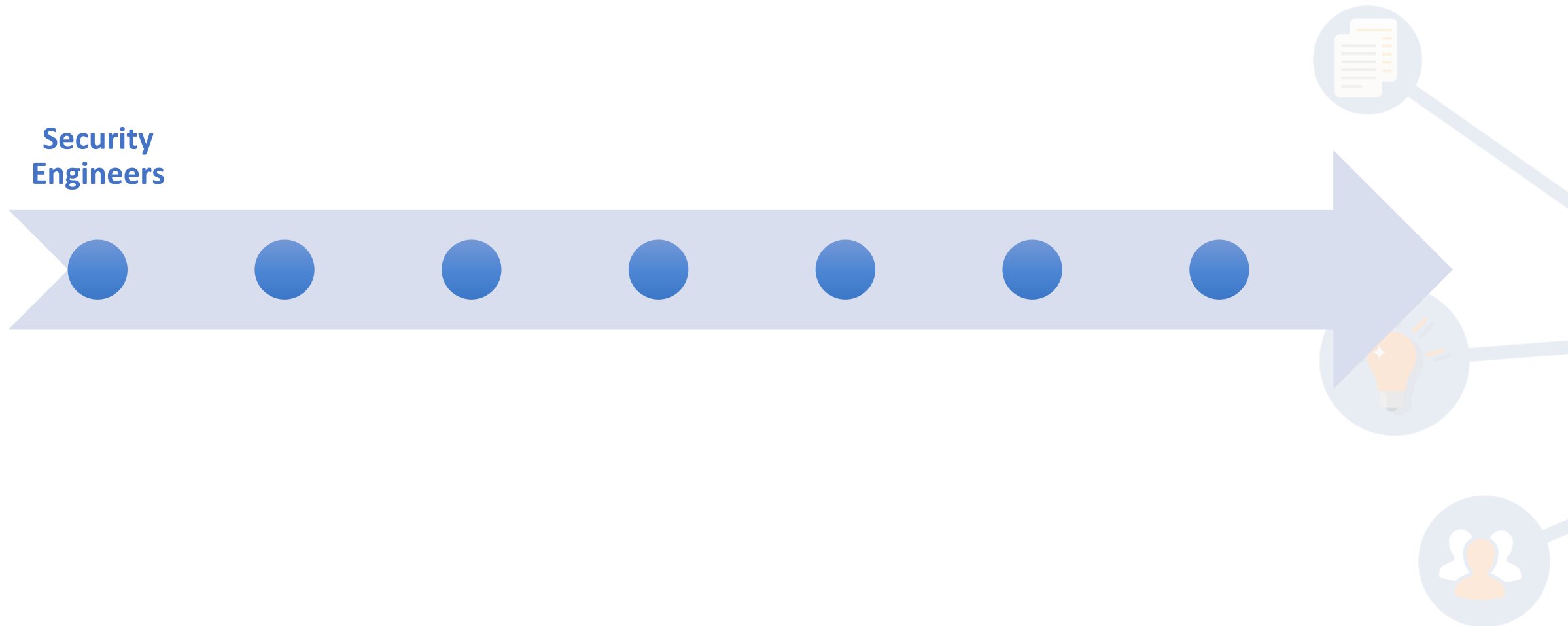
Integrating Security into Emerging DevOps

Tuesday May 15, 2018
4:00 PM - 5:00 PM

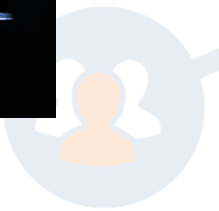
John Benninghoff
@jbenninghoff



Agile Journey

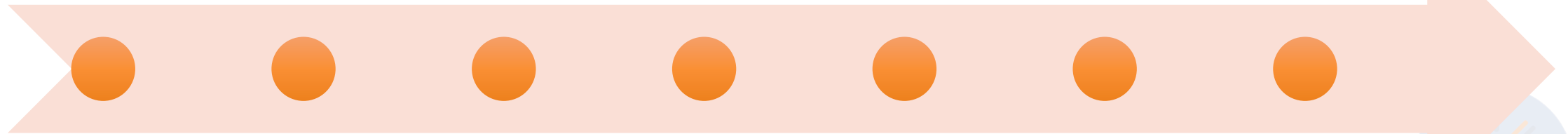


Go Hire Some Security Engineers!

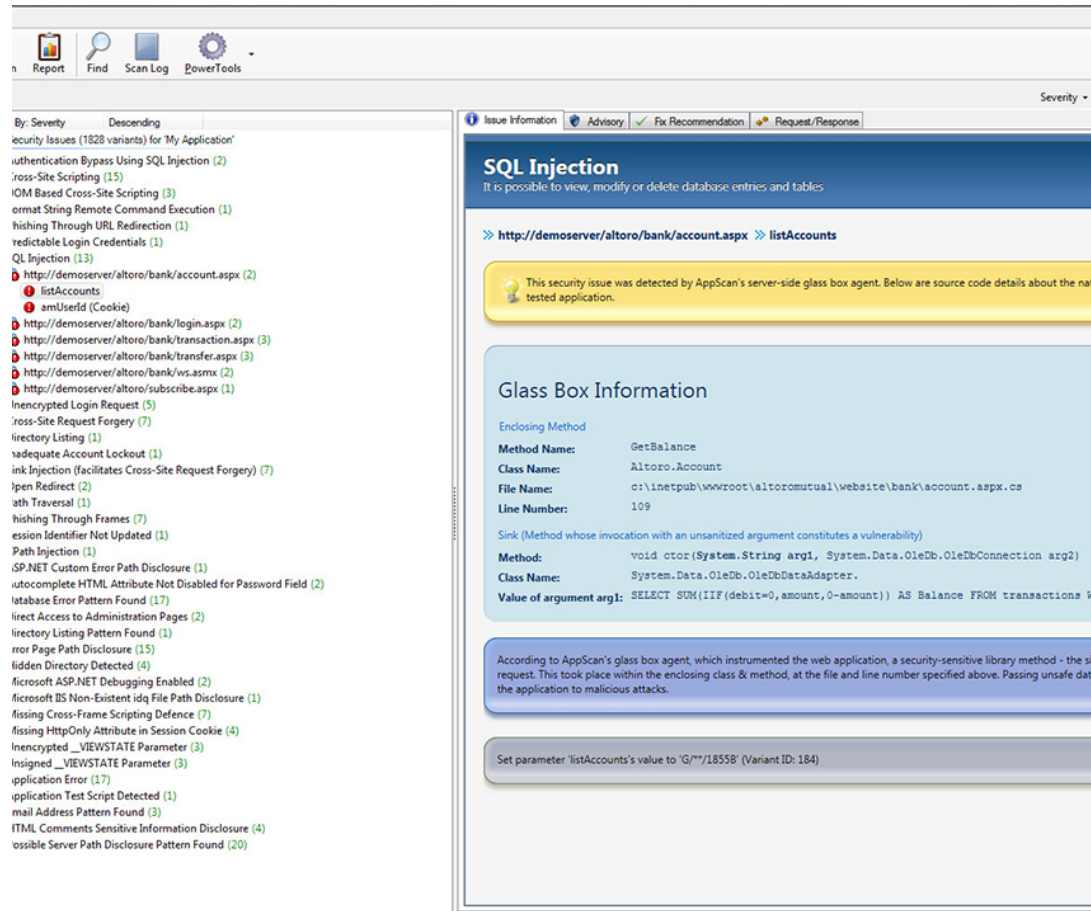


AppSec Journey

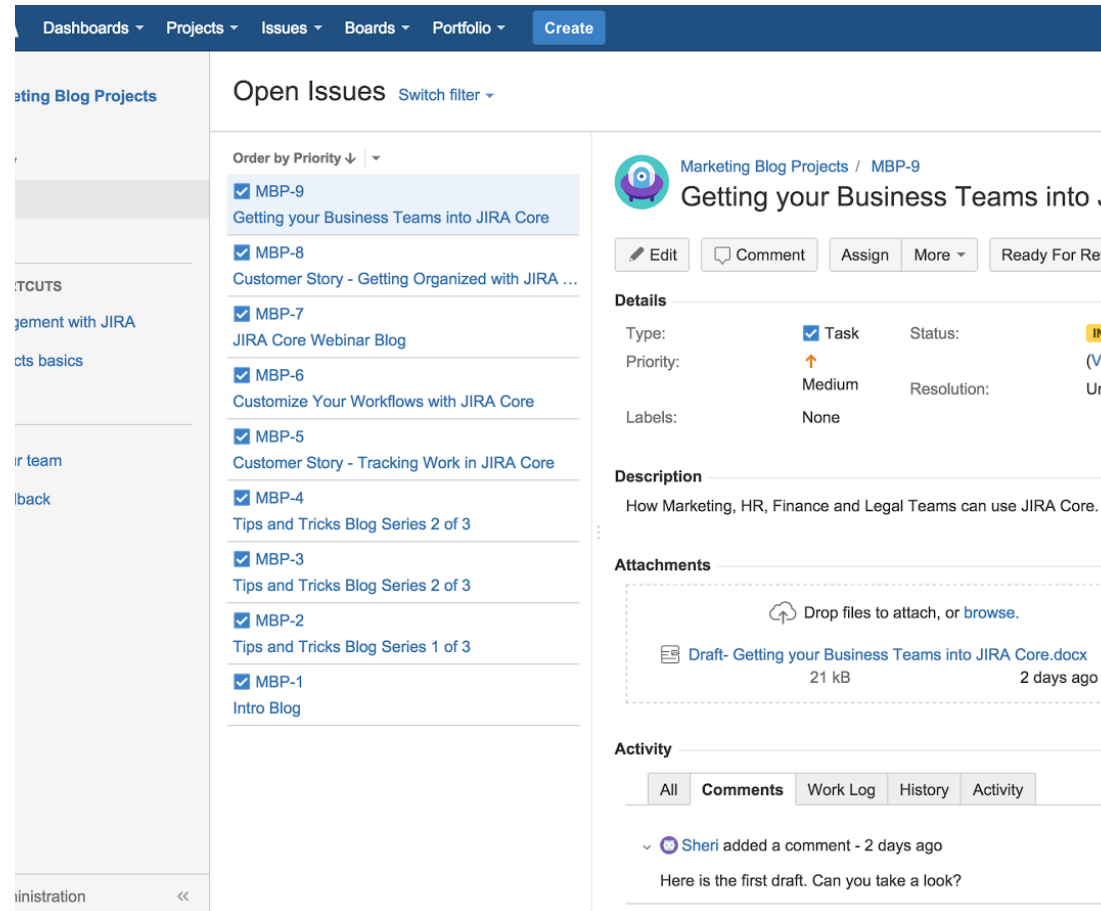
DAST
Deployed



Deploy Dynamic Scanning

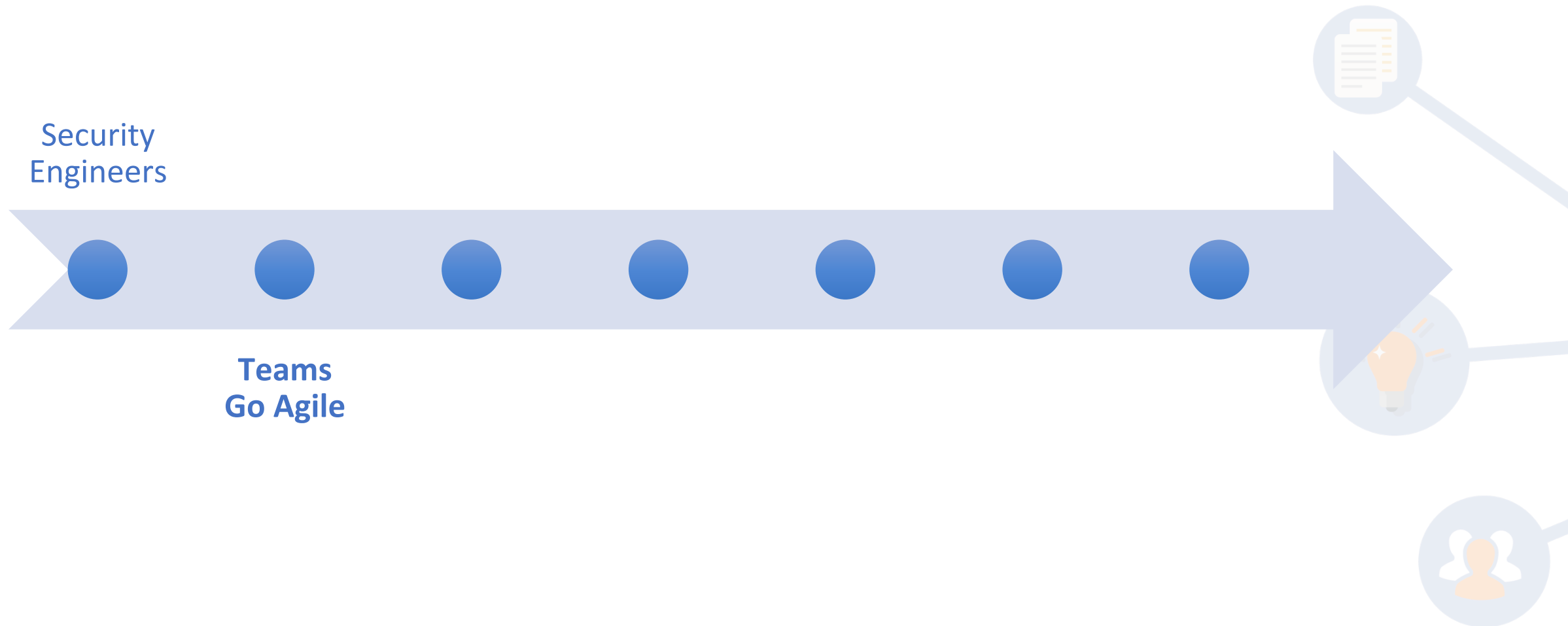


The screenshot shows the AppScan interface. On the left, a list of security issues is displayed, sorted by severity. The main panel shows the details for an SQL Injection issue. The issue title is "SQL Injection" and it is described as "It is possible to view, modify or delete database entries and tables". The URL is "http://demoserver/altoro/bank/account.aspx" and the endpoint is "listAccounts". The "Glass Box Information" section provides details about the enclosing method, including the method name "GetBalance", class name "Altoro.Account", file name "c:\inetpub\wwwroot\altoromutual\website\bank\account.aspx.cs", and line number "109". The value of the argument "arg1" is shown as "SELECT SUM(IIF(debit=0, amount, 0-amount)) AS Balance FROM transactions WHERE".

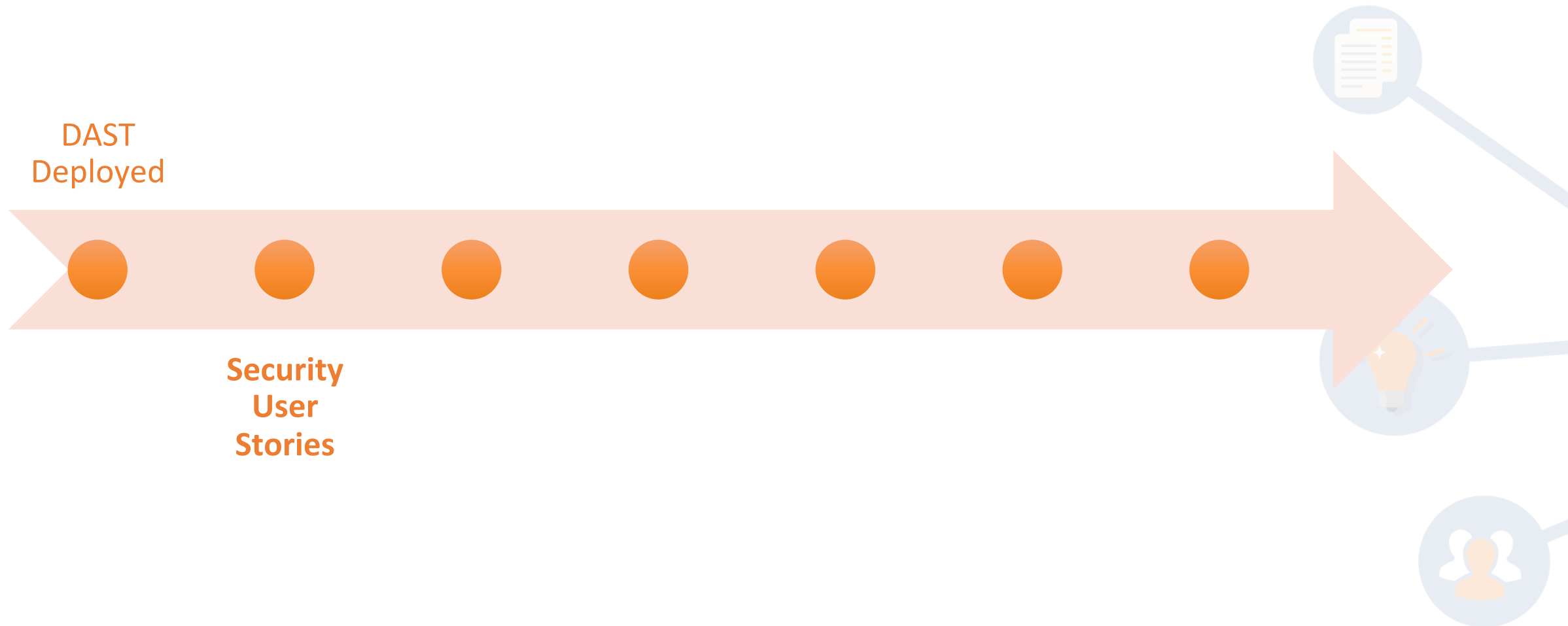


The screenshot shows the Jira issue tracking interface. The top navigation bar includes "Dashboards", "Projects", "Issues", "Boards", "Portfolio", and "Create". The main content area is titled "Open Issues" and shows a list of issues. The issues are ordered by priority and include titles like "Getting your Business Teams into JIRA Core", "Customer Story - Getting Organized with JIRA...", "JIRA Core Webinar Blog", "Customize Your Workflows with JIRA Core", "Customer Story - Tracking Work in JIRA Core", "Tips and Tricks Blog Series 2 of 3", and "Intro Blog". The details panel for the selected issue "Getting your Business Teams into JIRA Core" shows the following information: Type: Task, Status: In Progress, Priority: Medium, Resolution: Unresolved, Labels: None. The description is "How Marketing, HR, Finance and Legal Teams can use JIRA Core." The attachments section shows a draft document "Draft- Getting your Business Teams into JIRA Core.docx" with a size of 21 kB, uploaded 2 days ago. The activity section shows a comment from "Sheri" added 2 days ago: "Here is the first draft. Can you take a look?"

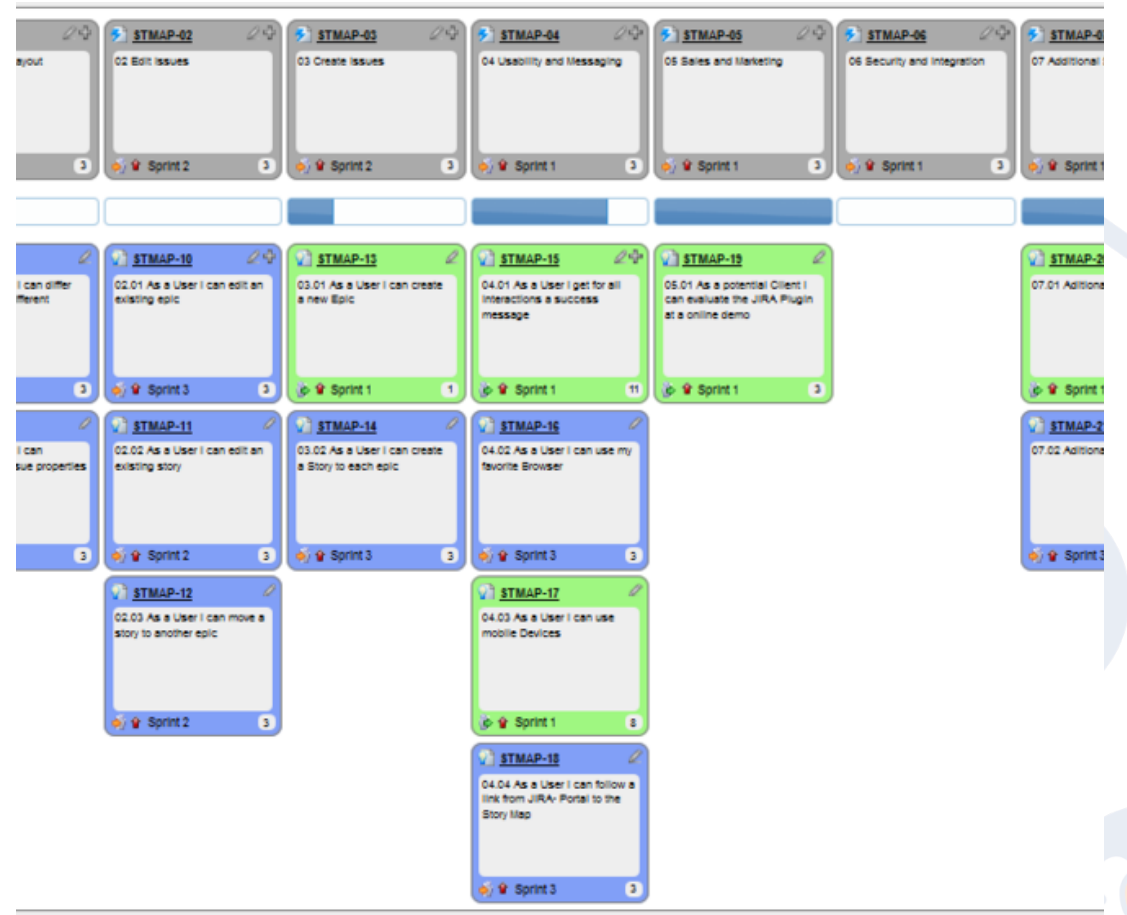
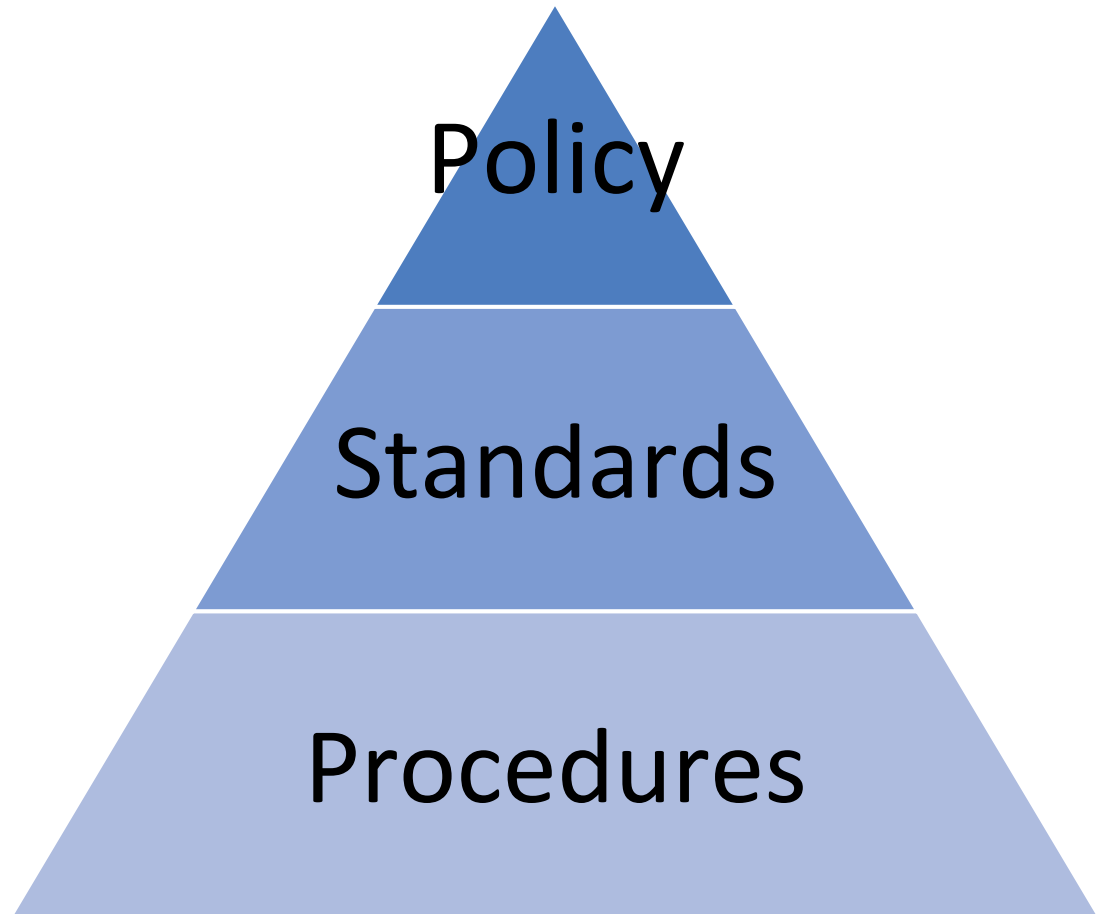
Agile Journey



AppSec Journey



Security Requirements Library

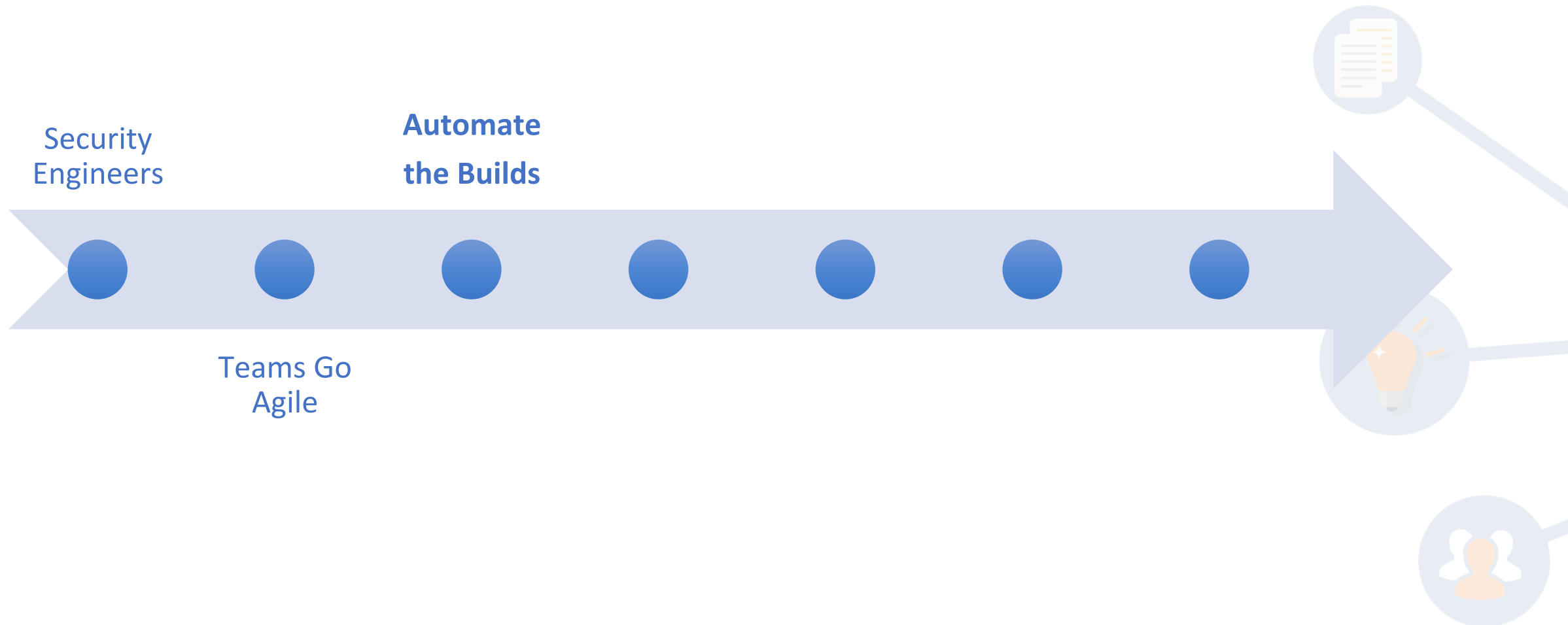


The screenshot shows a JIRA board with several cards representing security requirements. Each card has a title, a description, and a sprint assignment. The cards are color-coded: blue for general requirements and green for specific user stories.

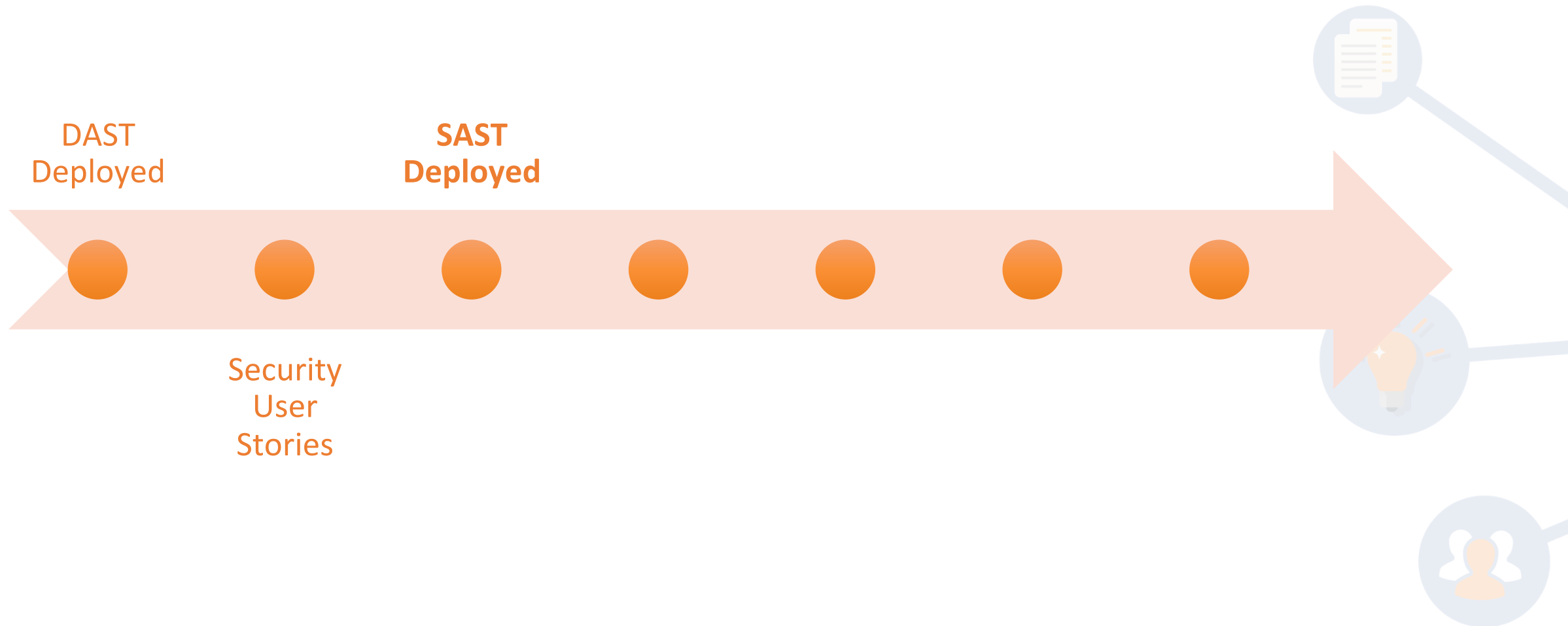
ID	Description	Sprint
STMAP-02	02 Edit Issues	Sprint 2
STMAP-03	03 Create Issues	Sprint 2
STMAP-04	04 Usability and Messaging	Sprint 1
STMAP-05	05 Sales and Marketing	Sprint 1
STMAP-06	06 Security and Integration	Sprint 1
STMAP-07	07 Additional	Sprint 1
STMAP-10	02.01 As a User I can edit an existing epic	Sprint 3
STMAP-13	03.01 As a User I can create a new Epic	Sprint 1
STMAP-15	04.01 As a User I get for all interactions a success message	Sprint 1
STMAP-19	05.01 As a potential Client I can evaluate the JIRA Plugin at a online demo	Sprint 1
STMAP-11	02.02 As a User I can edit an existing story	Sprint 2
STMAP-14	03.02 As a User I can create a Story to each epic	Sprint 3
STMAP-16	04.02 As a User I can use my favorite Browser	Sprint 3
STMAP-12	02.03 As a User I can move a story to another epic	Sprint 2
STMAP-17	04.03 As a User I can use mobile Devices	Sprint 1
STMAP-18	04.04 As a User I can follow a link from JIRA Portal to the Story Map	Sprint 3
STMAP-2	07.01 Addition	Sprint 1
STMAP-7	07.02 Addition	Sprint 1



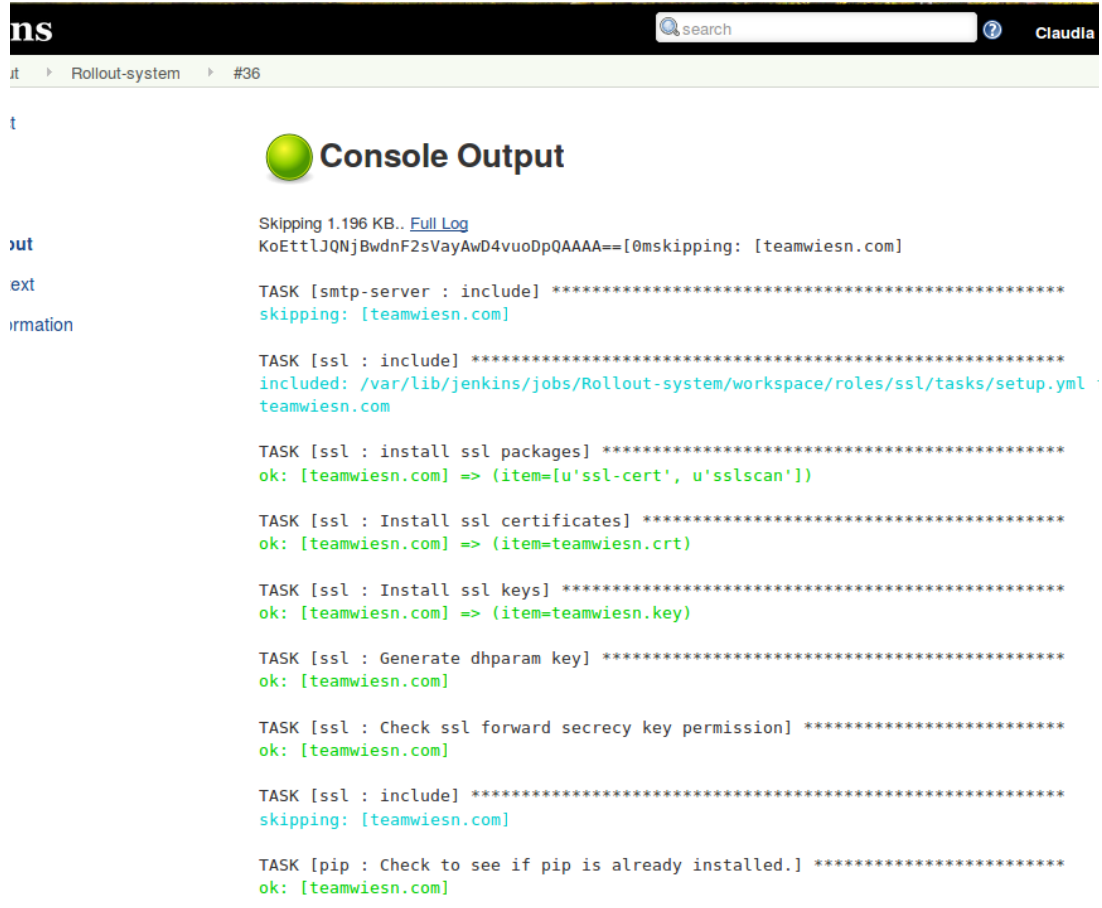
Agile Journey



AppSec Journey



Automate the Builds + Deploy SAST



ns ? Claudia

it > Rollout-system > #36

Console Output

Skipping 1.196 KB.. [Full Log](#)
KoEttlJQNjBwdnF2sVayAwD4vuoDpQAAAA==[0mskipping: [teamwiesn.com]

TASK [smtp-server : include] *****
skipping: [teamwiesn.com]

TASK [ssl : include] *****
included: /var/lib/jenkins/jobs/Rollout-system/workspace/roles/ssl/tasks/setup.yml
teamwiesn.com

TASK [ssl : install ssl packages] *****
ok: [teamwiesn.com] => (item=[u'ssl-cert', u'sslscan'])

TASK [ssl : Install ssl certificates] *****
ok: [teamwiesn.com] => (item=teamwiesn.crt)

TASK [ssl : Install ssl keys] *****
ok: [teamwiesn.com] => (item=teamwiesn.key)

TASK [ssl : Generate dhparam key] *****
ok: [teamwiesn.com]

TASK [ssl : Check ssl forward secrecy key permission] *****
ok: [teamwiesn.com]

TASK [ssl : include] *****
skipping: [teamwiesn.com]

TASK [pip : Check to see if pip is already installed.] *****
ok: [teamwiesn.com]



UNCOMPILED SOURCE CODE SCANNING

```
1 path = []
2 shortest;
3
4 while (nodes.length) {
5   end = nodes.shift();
6   predecessors = findPaths(map, start, end);
7
8   if (predecessors) {
9     shortest = extractShortest(predecessors, end);
10    if (nodes.length) {
11      path.push.apply(path, shortest.slice(0, -1));
12    } else {
13      return path.concat(shortest);
14    }
15  } else {
16    return null;
17  }
18  start = end;
19 }
20 }
```

ATTACK VECTOR SPECIFICATION

Attack Vector

- Source
- Method 1
- Method 2
- Sink

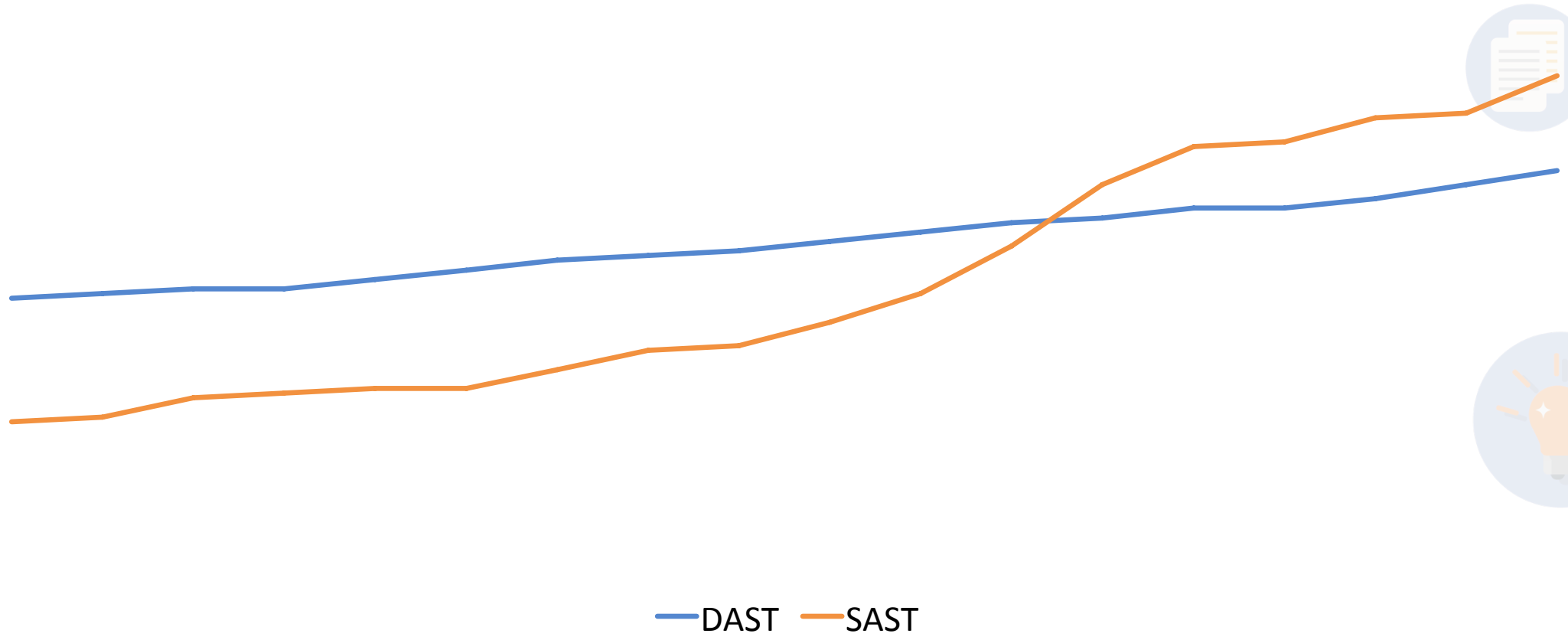
Results

ID	Status	Vulnerability Type	Priority	Source Object	?
1	New	Code Injection	High	"userID"	(?)
2	Pending	Command Injection	Medium	"menu"	(?)
3	Pending	Reflected XSS	Medium	"screen"	(?)
4	Pending	SQL Injection	High	"menu"	(?)
5	Pending	Connection String Injection	Low	"userID"	(?)

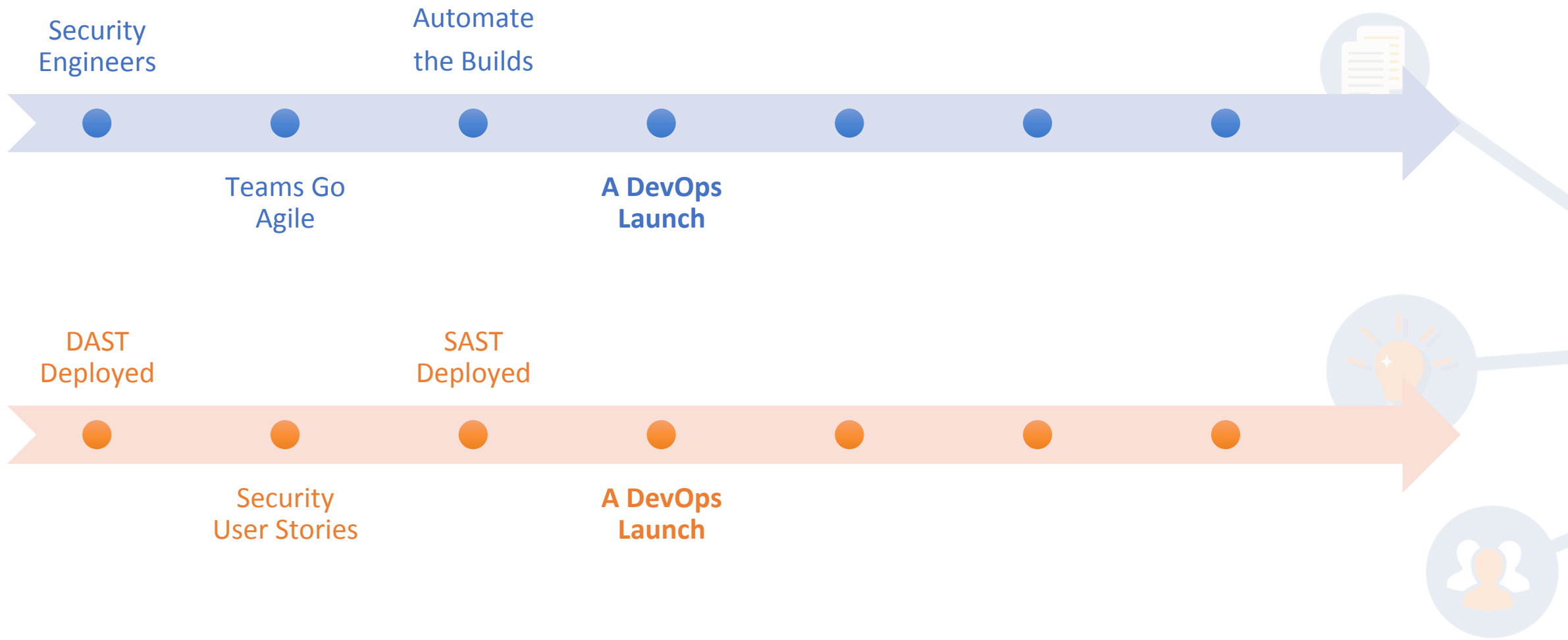
REMEDATION ADVICE



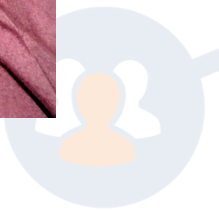
DAST & SAST Deployments



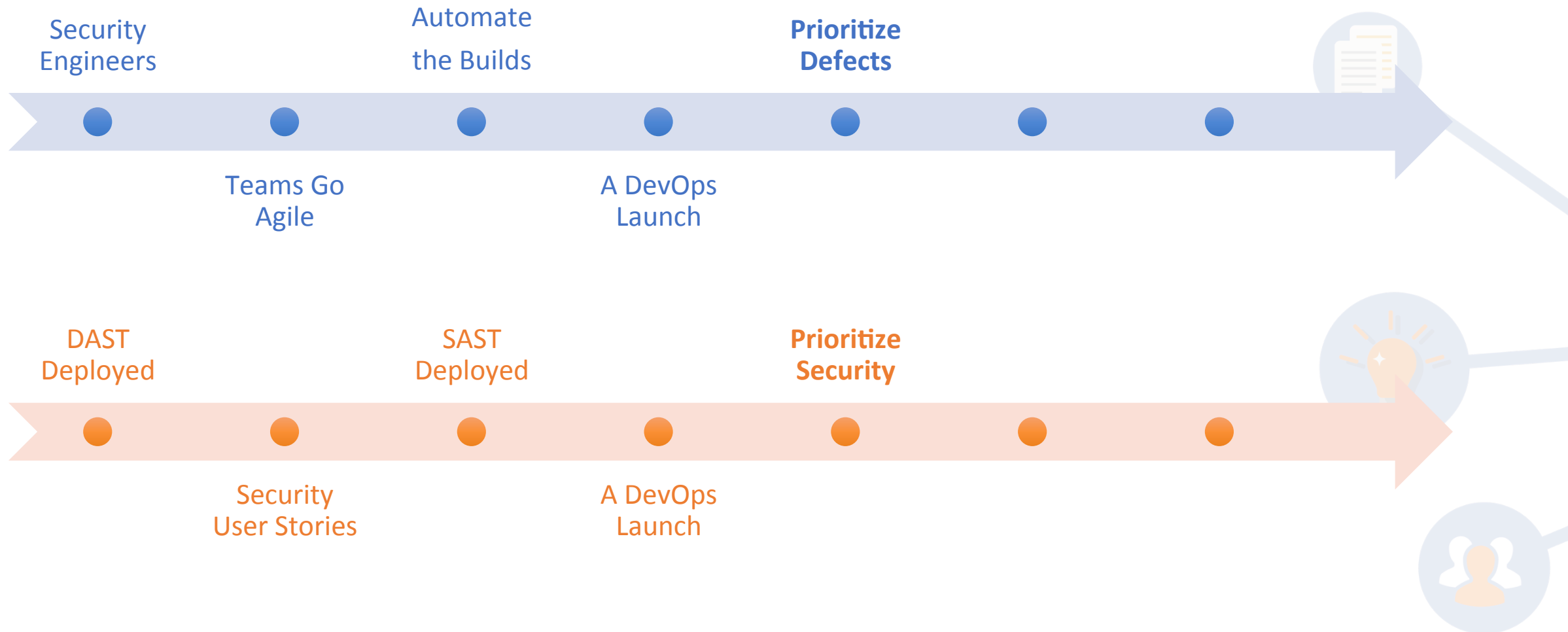
Agile + AppSec: A DevOps Launch



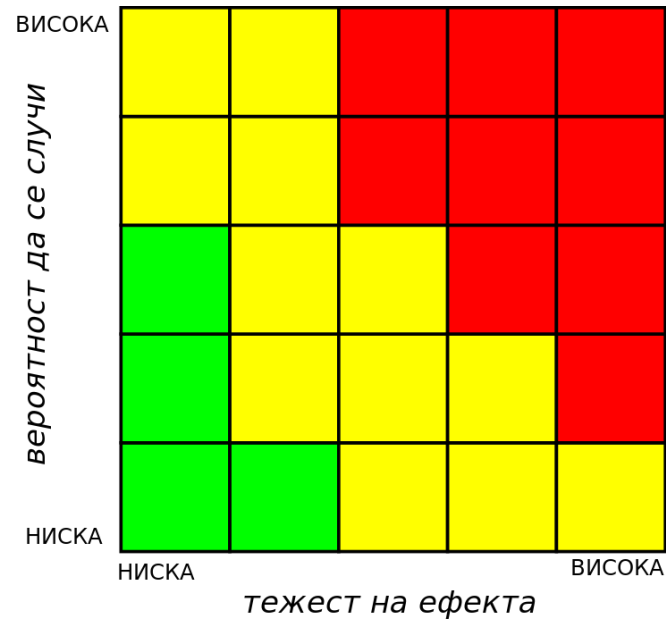
A DevOps Launch






Agile + AppSec Journey



Prioritization



ЛЕГЕНДА:

-  рискът може да бъде пренебрегнат
-  рискът трябва да бъде анализиран
-  рискът трябва да бъде управляван



Selected priorities

Remove all

-  DEFCON-1
-  DEFCON-2
-  DEFCON-3
-  DEFCON-4

Available priorities

Add all

-  Blocker
-  Highest
-  High
-  Medium
-  Low
-  DEFCON-5

What's next?



Bill Sempf
@sempf



Follow

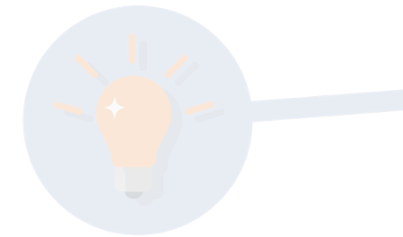
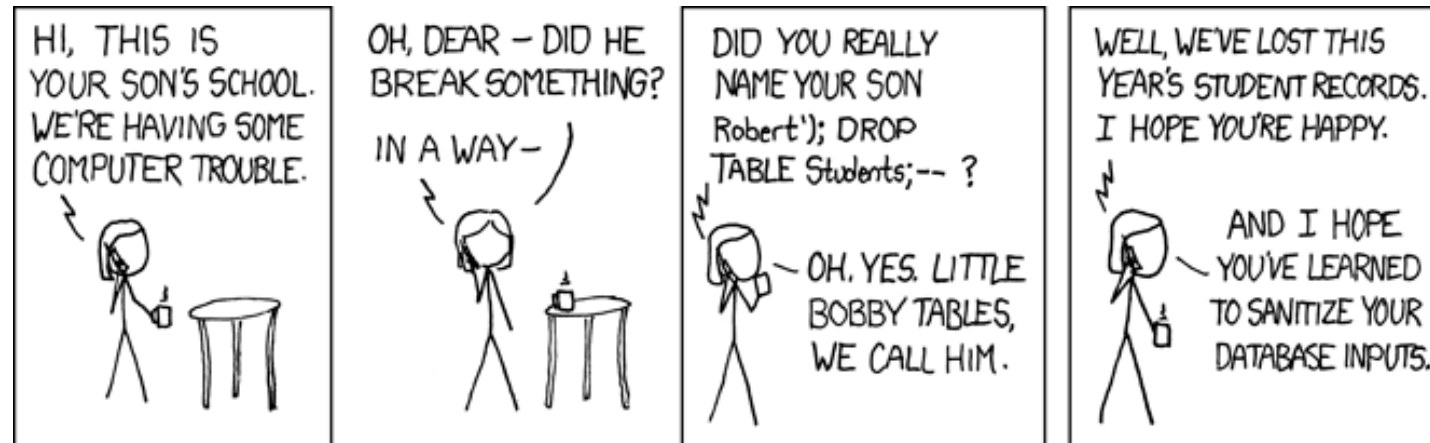
QA Engineer walks into a bar. Orders a beer. Orders 0 beers. Orders 999999999 beers. Orders a lizard. Orders -1 beers. Orders a sfdeljknsv.

RETWEETS
20,979

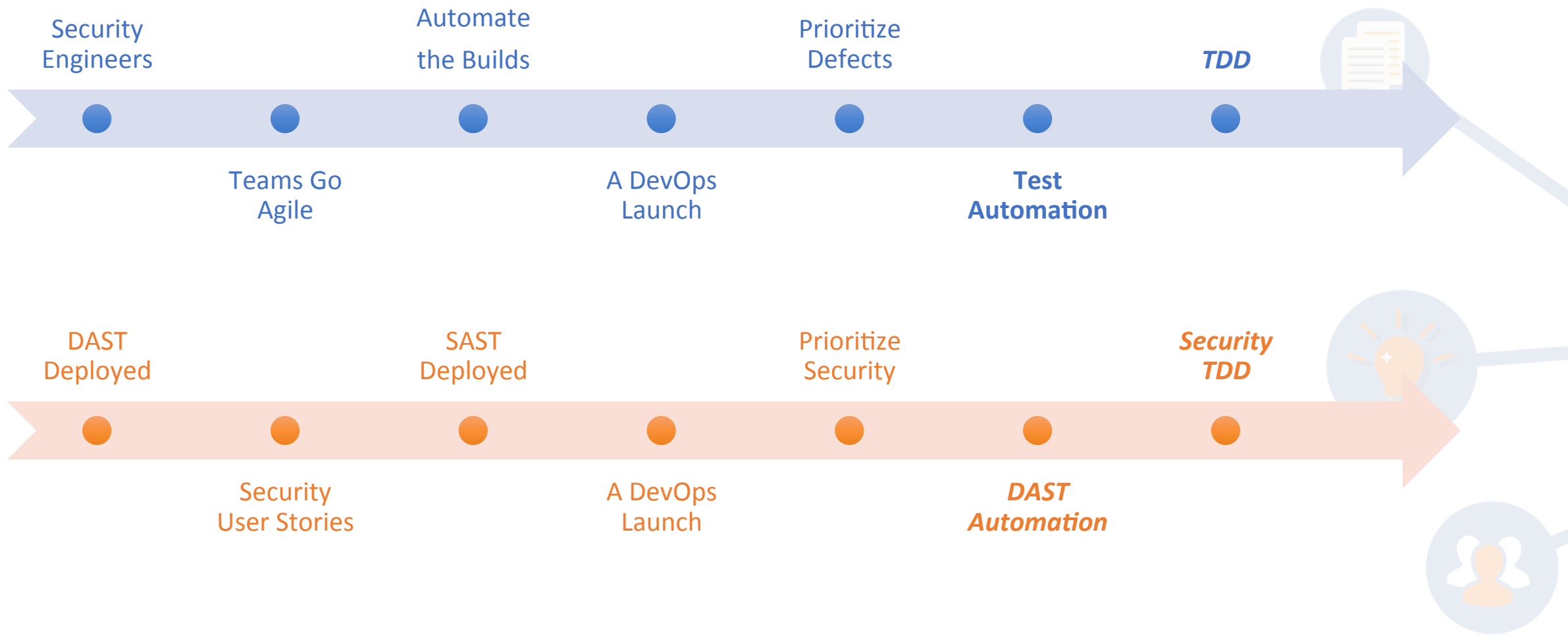
FAVORITES
12,415



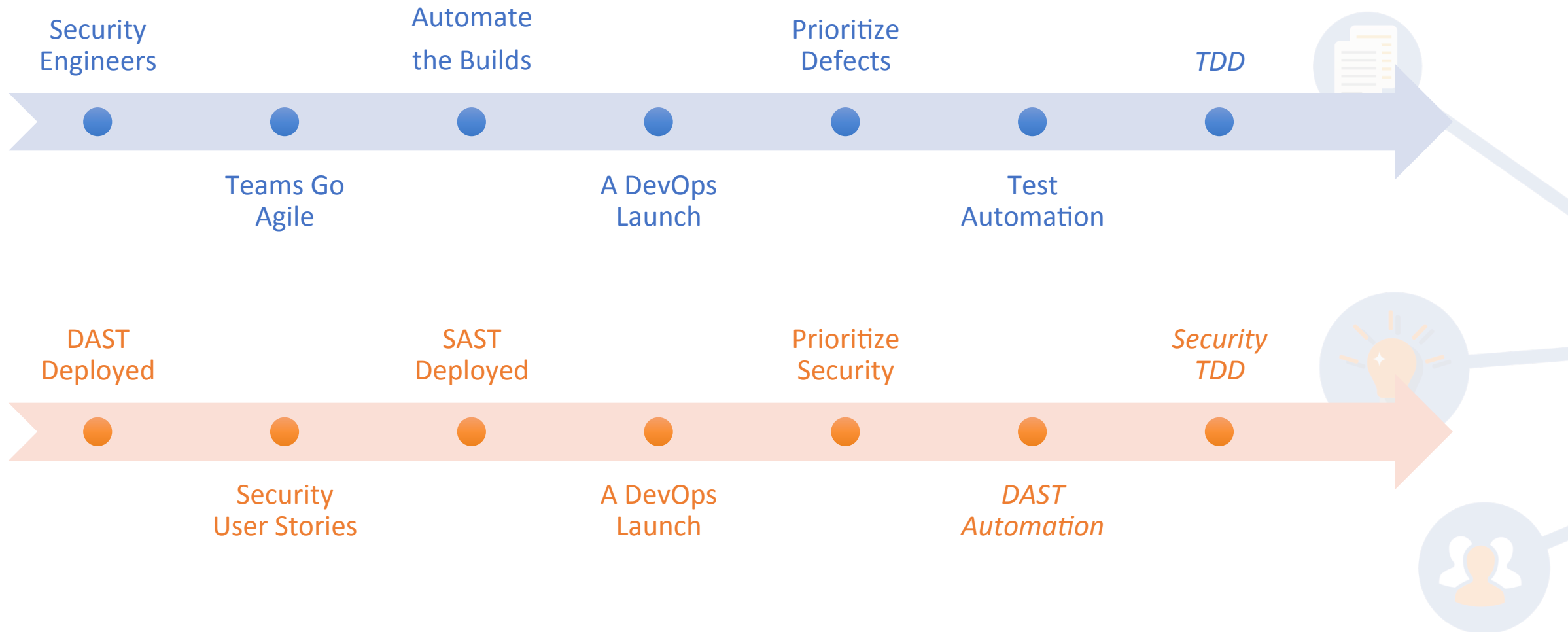
8:56 PM - 23 Sep 2014



Agile + AppSec Journey: What's next?



Our Journey



Thank You!

@jbenninghoff

jbenninghoff@mac.com

