What's Next in ITSM – Drive, Automation, Then Integrate.
The Federal Leaders Playbook - Season 1, Episode 6

Featuring:
Eric Lazerson - Vice-president at Acuity
Jessica Alfaro - Senior Manager at Acuity
Tom Hamill - Tactical lead for the BSM practice within Acuity
Kerri Posteraro - Managing Director at Acuity
Jeff Collison – BMC Software

Tom Hamill: Welcome. Today's topic's going to be what's next drive automation integrated. I'm Tom Hamill. I've been working in the federal space with ITSM for about 20 years now and I am with Acuity.

Eric Lazerson: Excellent! I'm Eric Lazerson. I have in the ITSM space for about 15 years. I worked at a number of large software vendors in this space as well. I love the topic you know, great, so let's yeah, let's get into it.

Jessica Alfaro: I'm Jessica Alfaro, Senior Manager at Acuity, been working in the ITSM space for 15 years, very passionate about automation and integration. A lot of my previous work is around CMDB and discovery, so interested in seeing how organizations could move forward with automation.

Kerri Posteraro: I'm Kerri Posteraro. I've been in the federal consulting space for about 13 years, largely focused on the implementation of enterprise applications as well as process definition and maturity, happy to be here, looking forward to the conversation.

Tom Hamill: Nice. We also have a special guest today from BMC, Jeff Collison.

Jeff Collison: Hey folks. Jeff here, been working with BMC software for about 18 years. Primarily, when I first started my career, it was working with various civilian agencies inside the Beltway; last seven or eight years been focusing on the DoD agencies out there, so I have a lot of experience before and automation really excites me because that's where I can really drive a lot of efficiency gains across the enterprise.

Tom Hamill: Ok. Thank you. So, let's just dive right in. So, what is automation? What does it look like in the IT Service Management world?

Jeff Collison: I see it really about maximizing efficiencies by integration of technology out there. So, by integration, that technology what I see is you're starting to break down silos. I used to work for a security company, my second job I'm a little older now, but on my second job, used to work for a well-known security company out there so I really have a passion for IA and information assurance. And, really what I see from an automation and integration perspective is tying the IA world into the operations world, so, I can break down that silo and have multiple tools really combine as one again through technology, integration and automation to provide better situational awareness across the enterprise for each one of the- the agencies, whatever agency in whatever mission that you're you know conducting today.

Eric Lazerson: Yeah, I think that that's a great point – starting to pull in those other tools. A number of these agencies, they'll make their initial purchase, by now, all of them have purchased, all the major government agencies out there have already purchased some sort of tool for service management. There is a tool that is varying in levels of usage, the functionality within it, there-there's some automation within the tool itself but then they start to see gaps in data and I think that's what you're referring to Jeff is there's gaps in, you know, vulnerability information or in their assets or their CI's out in production and how do you get that information in and then you know how do you do that so it's not a manual process.

Kerri Posteraro: Right. I think we've-we've experienced a lot of recognition that certain tools can and maybe should tie into ITSM, but there's a fear in doing so to actually make the technical integration. I think when you get the technical people in the room the message is always the same, is that these things do work together and it's easy to make them talk to each other it's figuring out why you don't want to. I think we've been in numerous situations where we're pursuing a direct integration to get a data point that we didn't have in the past but the answer that we get is instead of an integration how about we just give you a report that you can consume so we don't want to make that direct connection and why do you think, why do you think that's the case?

Jeff Collison: I think there are a lot of different issues that are not technology-related around that. Primarily somewhere based upon control, do I want you to see my data or not; but you're really going to get to a situational, provide a situation awareness map or picture.

It's got to be a lot more than hey I'll just give you a report because at the end of the day if I if you keep going down the road of hey I'll just provide a report the way that the world is changing and the way that technology is changing the reports manually created won't really be able to keep up with the maturing whether it be a threat from IA or cyber or-or not is it technology in the world is changing so quickly and the missions are changing so quickly to satisfy things that the old manual methods of providing a report is really going to be challenging, as we-we move forward to satisfy you know mission requirements.

And even as you know an example, when you think about it ACAS or NASUS come out and tell you these are how many servers are not passed or going to meet this requirement but there really isn't too many zero-day attacks out there, present today. A lot of the challenges that I see that agencies are facing is just patching where there's already a patch out there.

Eric Lazerson: Right, basic known vulnerabilities and coming up with ways to mediate them.

Tom Hamill: And the time it takes to get that patch, right. A lot of problems is that you'll recognize that it has to be patched but the time to get that patch into place, tested and put it in there is a long time so a lot of automation resolves that issue right; because you'll have time to patch much quicker if you automate it and push them out automatically.

Kerri Posteraro: But does it seem to you that the-the conversation around integration is more focused on a new tool that gives me a capability that I can bring into my environment

versus things we already have and have had for years and can we make them work together. I personally feel like the focus is always on this new thing that can bring certain pieces of information together but there's not a whole lot of conversation about hey I know this group in my department owns this and manages it I could use it, let's go talk to them about an integration.

Jessica Alfaro: Yeah, I mean, I've, I'm a big fan of concept of operations, you know, being able to look at all of the different tools that are out there and laying out how they interact with each other. What am I trying to get from one? How does that feed the other? And what is my final output of what I'm trying to gain like from that bigger picture? What would, what's the end thing that's going to be consumed? And so, I've-I've always tried to push, let's lay out a concept of operations to start, here are those key tools and how they tie in and you know to come up with some type of at least a starting point that gives you something that you can bring to the table and say, 'this is how I think we can utilize the data from your tool and the output of what that would look like.'

Eric Lazerson: So, le-let's get a little more specific. So, we talked about tools and integrate and automate and, let's give some examples. So I'll go, you know, to one example that I know of and then then I know there's some-some buzzwords we want to touch on as well, but you know that monitoring tools and-and just system outages and being able to quickly identify applications down and integrating your system monitoring tools that have alerts to your service management or Incident Management tracking tools is one integration that used to be really popular and then it was aw I get, I get you know spammed with too many false positives and-and I've seen a kind of trend away from just integrating those two tools. Any, Tom, any thoughts on other tools that you see integrated?

Tom Hamill: Yeah, I mean recently we just helped out with the Close and Compliance

Eric Lazerson: Ah the buzzword close and compliance

Tom Hamill: Yeah, close and compliance. Sure, well, when it works, it's pretty cool. So, we saw that in one contract where it was so nice to see putting together the ITSM's we were, there's a change piece to it; they put in a change for a new server and that integrates with the BladeLogic that says okay I see you want a new server I put the change in I get approval on that says okay lay logical hand and deploy that configured server and that server is configured in such a way that's consistently going out. When that server goes out it closes that change but then discovery comes and finds it – right, and then puts it into the-the CMDB so there's a nice.

Eric Lazerson: So, you said BladeLogic which is a BMC tool.

Tom Hamill: Yeah.

Eric Lazerson: So, Jeff, I know you've got a lot of experience around that tool and some of the close and compliance, any stories you want to share of where you've seen it go well and where you've seen it, you know, go sideways - things to look out for?

Jeff Collison: I can share some scary stories. It's not only what was discussed kind of from a use case but also, I kind of see it is again going back to the, whether it's a vulnerability or you know many of us engineers are very used to going through and enabling a quick configuration maybe on a router or something like that that I don't necessarily share with the rest of the organization.

So it's-it's not only that the original use case that we just discussed but also you know if I do and out-of-band configuration change, I certainly want that to be recorded because you know many times I see there's usually a communications gap, so if let's say I did make that change because the reality is it takes me you know two minutes to make a change to a router on the routing list or whatever versus maybe a little bit longer to actually go through and record the change; but the reality of that is if, maybe if I something, I can, you know cause unavailability of service to someone else and start you know all those incidents start coming and flooding the help desk. So, it's really going through and helping me Jeff as the engineer.

So, we make those changes but also record them so that I'm sharing that information across the board to eliminate other issues in the organization that may occur if I perform a two-minute change badly or I don't do necessarily something. So it's about sharing the information, so I also see that use case, which is really, you know, certainly on the capability, it's from a deployment perspective or fulfillment perspective across the board and applying whatever stig's or dispatches that you need but also on the flip side it's helping everyone understand and breaking up the Silo of what Jeff the network engineer might do in the backend not just talk in reality but sharing that information across the board with the rest of my peers in the IT organization. And it provides a better situation of awareness and really starts to get you to kind of more of a mature organization.

Tom Hamill: I thought it was interesting looking at the recent Gartner report, that a lot of it evaluations they did on the product was focused on automation right new maturity and stuff so a lot of people that made Magic Quadrant, is I think they call it, those tools had an automation seamless piece to it. So, automation is important out there.

Jeff Collison: And as the technology has changed over the years and certainly becoming much more agile, but also, you know, REST and REST API's kind of more of a standard, from an integration perspective as all the various tools that the agency has out there they kind of look at some use cases across the board. They can use that type of capability - technology capability to integrate and become a little bit more mature as than before.

Eric Lazerson: So, if you were a federal IT manager and you were in charge of your ITSM system today, what is the first thing that you would integrate or what is the first piece of automation you would seek out?

Tom Hamill: Is it one or the other or both? I mean you think is the first step to say let me look at what I can integrate or is the first step how can I automate?

Eric Lazerson: I think integration with the purpose of some sort of process improvement.

Tom Hamill: Ok.

Jeff Collison: I would say – customers have asked me this before – I would say, you know, development of a discovery type capability with a CMDB, if I don't know what I-I don't have out there this, it's very difficult to instrument it to monitor it and is very difficult to protect it so I need to really start at a crawl-walk-run perspective to at least understand what I have out there and more importantly it's not just understanding what I have out there it's how those things are related to each other in the environment, as well as you know the status of it where is it. So that's really where, the first place I start and then it's-it's a lot easier to start automating once I know what I have, the you know automating you know patches and smashes or IA type of patches across that and then certainly sharing that information across the board with the rest of the, my peers, may or may not work in different organizations.

Eric Lazerson: I would agree with that. I think if you were embarking on a CMDB journey…

Tom Hamill: A journey, wow.

Eric Lazerson: To do it without a discovery tool is a mistake.

Tom Hamill: Yeah, I agree.

Jessica Alfaro: So, to wrap it up it sounds like concept of operations, what do I have, what is new, how things fit together, the automation helps to eliminate errors, so it streamlines service delivery, it maximizes investment of the current tools that you have in your environment and it enables situational awareness.

Tom Hamill: Awesome, thank you Jessica and Jeff thank you again for coming in and discussing what's next – the automation or integrate it sounds like it's a combination of the two really, they drive us forward so, thank you again.

Jeff Collison: Thank you.