Massive Automation to Reduce Human Risk

Even in large organizations, it is not unusual to find controls that still involve a great deal of manual effort. In fact, evidence for an attestation may be entirely generated by someone taking screenshots. This is certainly one area where innovation needs to play a bigger role. People are an organization's most valuable resource and, often, its greatest risk. Innovating how we collect evidence and perform audits can help with both aspects. It can free up personnel to be more productive and reduce a great deal of the human risk regarding controls and the like. In fact, we are in an era when we need to look at innovating through automation because we simply cannot keep up otherwise.

Virtualization and Cloud

When system administrators managed a handful of servers, auditing these servers manually was not an onerous effort. However, with the prolific use of virtualization and the increase in cloud adoption, the number of devices or hosts has increased exponentially. After all, resources can be provisioned and shut down automatically. We can even script triggers to scale out web farms during periods of heavy usage and other triggers to eliminate web servers when the load dies back down. In a cloud environment, where an organization pays for what it uses, having excess capacity always available is money wasted.

K. Brian Kelley, CISA, CSPO, MCSE, Security+
Is an author and columnist focusing primarily on Microsoft SQL Server and Windows security. He currently serves as a data architect and an independent infrastructure/security architect concentrating on Active Directory, SQL Server and Windows Server. He has served in a myriad of other positions including senior database administrator, data warehouse architect, web developer, incident response team lead and project manager. Kelley has spoken at 24 Hours of PASS, IT/Dev Connections, SQLConnections, the TechnoSecurity and Forensics Investigation Conference, the IT GRC Forum, SyntaxCon, and at various SQL Saturdays, Code Camps, and user groups.

> "WE ARE IN AN ERA WHEN WE NEED TO LOOK AT INNOVATING THROUGH AUTOMATION BECAUSE WE SIMPLY CANNOT KEEP UP OTHERWISE."

Given the scale, which can be an order of magnitude (or two or three orders) more than previous device counts, auditing manually is just not realistic. We could sample, but it would be better if we could evaluate every provisioned resource, would it not? It most certainly would, as a single misconfigured device could be the entry point for an adversary seeking to do harm.

Speaking of auditing every device, how about capturing evidence for devices stood up for a period of time and then retired when load died? How can we be sure that those devices had proper controls? After all, they no longer exist. We can look at the provisioning process, but that does not tell us how well that provisioning process worked during that particular time frame if we are resorting to manual auditing efforts. Devices and systems that came into being after the last audit and were decommissioned before the present one are particularly problematic.

We could have an individual or even a whole team trying to capture information on systems as they come along, but that is a huge resource drain for arguably no gain. If an organization were to go down that route, an auditor could argue that it does not meet a reasonable return on investment (ROI) and would represent waste so far as the organization is concerned.

The Risk With Manually Created Artifacts

Whenever we have a manual process, we are relying on a person to do two things:

1. Capture information on the correct system or device.
2. Perform the proper procedure without error.

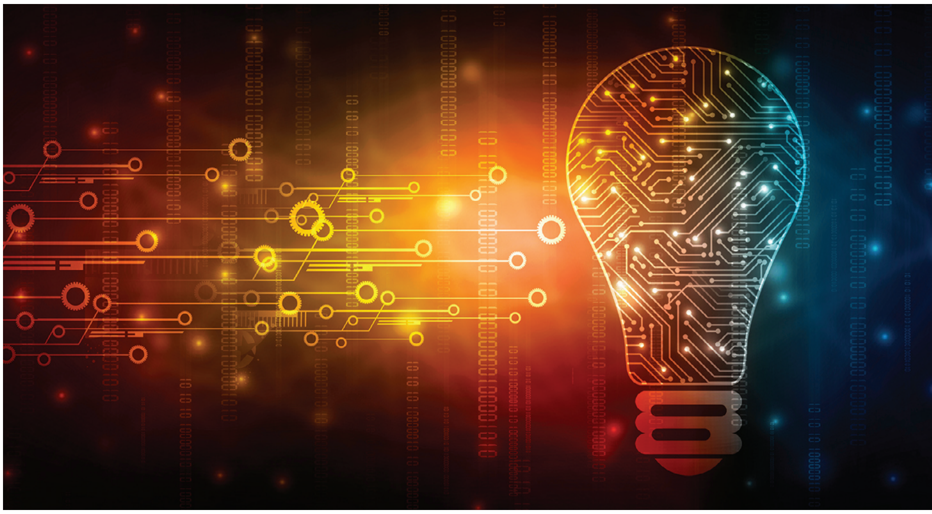
If either of these are done incorrectly, we do not have what we need. If there are a lot of artifacts to capture, it may be some time before the error is detected and the evidence is regathered (if that is possible). There is always additional risk due to human error. But what if it is not a case of human error?

Part of manual collection of evidence or validation of controls is that we assume that the person performing the work is trustworthy. With proper controls, we usually have other mechanisms to mitigate this risk. However, that is not always the case. When we can automate, we can reduce the risk due to the human element, not just with respect to error, but also due to malicious intent.

Let us consider what an untrustworthy person could do in manually collecting the evidence. Screenshots can be altered. One does not have to be proficient with the latest imaging tools to make nearly undetectable changes. Certainly, they would be undetectable to the human eye, especially an eye that is going through a large amount of evidence quickly for the purposes of an audit.

Altering a screenshot is not the only way. Old screenshots that have been saved can be reused. But the file date should protect us, right? Nothing stops a person from opening up an image in MS Paint (on Windows) and resaving the document with a different name, thereby creating a new timestamp. Or, if they are more technically clever, they might use other ways to alter the file date without actually touching the contents of the file.

If the evidence is not a screenshot but something such as a text file that is generated as a result of a script, that is even easier. One does not even need a modicum of artistic talent! And, if the script is handed over to be run by a person with the rights to make changes, they can make the changes to look clean for the audit and then put things back after the script runs. This situation is not that unusual because one often has to have elevated rights on systems to audit security—the same privilege level gives them the ability to administer the security.



Something else that comes up from time to time: The actions to gather the evidence for a control may, in and of themselves, generate work for another control. For instance, if logins to a particular set of servers must be explained and documented, logging on to those servers to collect who are the admins, what are the permissions for a particular set of files, etc., would require that documentation.

> “WE CANNOT COMPLETELY ELIMINATE RISK, BUT ANY REDUCTION IS GOOD.”

We have these types of controls because the ability to log in with a privileged account to the server represents a risk to the organization. It would be better for said individual not to have the ability to log in at all. After all, if the person has the ability to log in, if the account is compromised, someone else has the potential to log in. There are countermeasures to this such as multifactor authentication systems and privileged access management solutions, but it is still better if the individual cannot log in. Those systems exist to prevent an unauthorized login. However, if the

Enjoying this article?

- Read *Auditing Artificial Intelligence. www.isaca.org/auditing-AI*
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

person is authorized to log in and is also malicious (insider threat), they can do damage to the organization. No login equals no damage.

Automation to Reduce the Risk

Automation takes the human out of the collection tasks. Any risk due to the human element is reduced. Yes, there is still some risk due to human error. For instance, if someone misinterprets the evidence, that is human error. There is also some risk due to malicious intent. Someone can attempt to get rid of evidence, misrepresent the evidence or flat out lie on a report. We cannot completely eliminate risk, but any reduction is good. That includes the amount of time someone spends collecting evidence. When people have to perform manual processes that could be handled by automation, it means they are not available during that time to perform what the organization would consider more valuable work. After all, if I have to spend four hours collecting evidence, that is four hours I cannot spend innovating or solving problems.

Another thing to consider is the scale problem. With automation, scale is not so daunting. I may need to scale my collection process/systems, but as systems increase in number, I do not have to increase my headcount linearly. That is a huge cost savings. Also, if I can automate any artifact collection around any scale out or scale in of systems, that means I can ensure I am capturing the evidence when I need to do so.

Speaking of scale, though, there is a risk with too much automation. If we try to collect too much, there can be a real performance impact on the system. If the information is necessary, the organization has to accept the performance hit or spend to increase capacity, if that is possible. But if it is not absolutely necessary, what is collected should be kept to what is defined as needed. By the way, collecting too much will result in a lot of noise. There will be a large amount of data to sift through for what we want.

Finally, we can automate comparison, at least at a high level. This allows us to detect differences and changes between the audit periods. Those periods could only be a few hours apart. Certainly, when we have to evaluate a great deal of evidence, having a report of detected differences will help tremendously. We will spend less time looking for the differences, there will be less risk of missing a difference and we should also be able to spot trends better.

> “SPEEDING UP PROCESSES, REDUCING RISK AND FREEING PEOPLE TO DO OTHER WORK IS ALL ABOUT BUILDING AND IMPROVING THAT COMPETITIVE EDGE.”

Automation Is Still Innovation

Innovation can be about giving an organization a competitive edge. Speeding up processes, reducing risk and freeing people to do other work is all about building and improving that competitive edge. It also focuses on the greatest risk factor: the human element. Whether we are talking malicious activity or honest mistakes, there is risk. Automation reduces that risk.