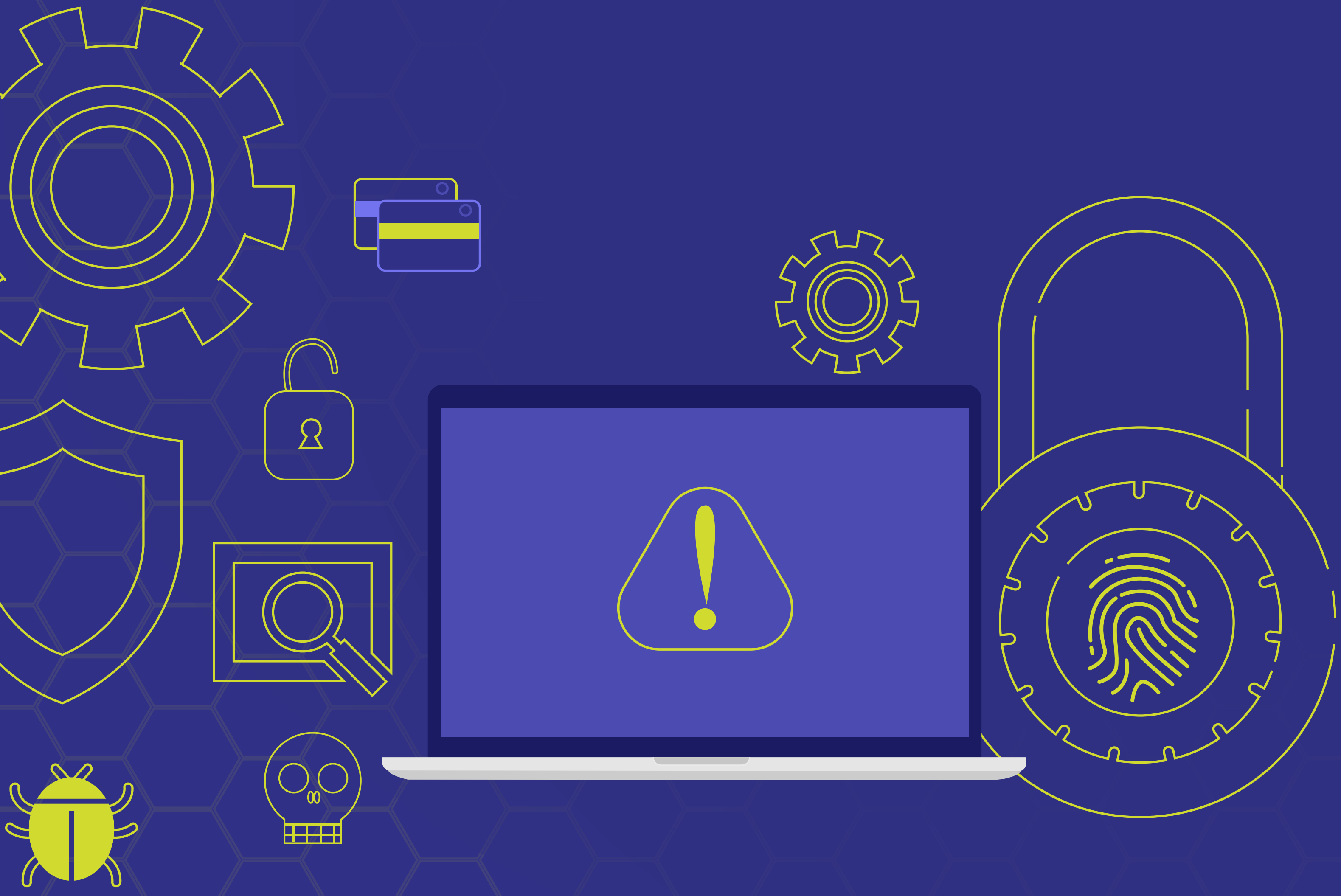
ManageEngine
PAM360

Breaching the security silo

- Ian Aitchison



www.manageengine.com/pam360

How a silo-busting combination of identity, security, automation, and service management can improve business productivity and improve your security game at the same time

The rapid growth in the IT security industry over recent years has brought exciting innovations, new concepts, and many new vendor technologies in response to the ever-changing threat landscape that IT leaders face every day. This growth has led to IT security being a well-established and highly funded industry with a strong career path for IT security pros commanding high salaries.

Yet, as with any IT function, when implemented into the enterprise, there can be a risk from implementing IT security in functional silos. A siloed approach to IT security can hinder business success. Silos often also result in delays, disconnections, and misalignment, and can be indicative of unhealthy internal politics.

So, the next level of IT security maturity requires broad functional integration and the conscious removal of silos.

Here are three ways to break down IT security silos.

1. Bake security into IT service management workflow

IT service management (ITSM) blends the business purpose and IT value with task management. Security information, knowledge, and actions can enhance the flow of IT along with the value and safety that a business receives from IT. Here are some examples:

- Include security approval directly in the workflow of service requests where there may be a risk in the service, application, or access requested.

- Make security guidance and advice a part of your IT knowledge base, and make sure it's available to the entire organization through self-service portals.

- Rather than publishing a separate security portal and an IT service portal, blend the two. Place security news, training, and other advice in your IT self-service portal.

- Start recording security-status values on employee user records in your ITSM data set. Ensure the IT support teams can see and understand the security status of all users. If a new employee has not yet completed their security training, they are a higher risk to the organization, and the IT team should responded accordingly.

- Don't manage security incidents in separate systems; instead, expand your ITSM platform to include workflows to manage all types of security incident in one place.

Despite all of the above being heavily reliant on your ITSM tool, it's critical that your security team takes the lead here. This is not an exercise in removing security, but in bringing security into everything that IT does. Positioning is critical.

2. Leverage automations for a faster, proactive security response

Once your ITSM toolset supports the management of workflows relating to security, whether it involves incidents, events, requests, or knowledge, the next step is to add automation. There should be a clear, well-defined strategy to automate a workflow as a response to a particular action, incident, or security process. This is best described with examples:

- If an unknown device is detected accessing your network, automatically and instantly remove network access to that device. Automatically create the relevant security incident ticket to find out who connected it and why.

- If employees' corporate email addresses or login details are reported in a pwned or breached external data set, automatically notify those employees and force password resets immediately.

- Always check if patches are okay to deploy. Ensure they have been tested. Use automation to roll patches out to their destinations in phases.

- Does an employee keep turning their firewall off? Don't just simply turn it back on automatically; find out why they need to keep turning it off by automatically directing them to simple survey to drive the steps they need to take. This keeps the environment secure without frustrating your employees.

- Does someone temporarily need their privileges raised to take specific actions? Don't make them wait; build an automatic self-service privilege elevation workflow that provides privileges for a limited time and revokes them after privileges are no longer needed.

Many siloed security tools provide these functions. You can focus on integration and automation to achieve these capabilities and stay away from the risks of managing siloed and disconnected security tools that provide these capabilities.

3. Enable greater productivity through better role and privilege management

Moving beyond detecting and reacting to security threats, there is one area of maintaining a secure business that can immediately benefit from an integrated approach—continual management and maintenance of access, privileges, and permissions. It's essential that security permissions and privilege access rights are maintained correctly throughout the process.

By combining onboarding and off-boarding through service management workflows and changing permissions and access rights through automation, you can ensure that all identities—with high risk, standard or privileged access—follow well understood, audited, and automated security life cycles at all times.

By automating HR system role changes, you can immediately and automatically change roles and access rights, complete with automatically generated ITSM workflows for further security approval and non-automated actions.

Putting it all together

Applying these three integrated approaches together can go a long way. Let's see how.

1. A new IT security admin starts their job. They automatically have all the basic rights, access, and privileges they need to do their job on day one.

2. On that first day, the IT self-service portal also shows the employee that there is new security training that they need to take and security documents that they need to read.

3. Once they complete that training and exhibit their caliber over the course of their tenure, they're granted higher levels of access and are notified of that change.

4. Since they have higher privileges, they're automatically notified when a high-risk security event comes into the organization, and they can report it through the self-service portal.

5. Because they reported the security incident, workflows and automations ensure that the required patch is delivered immediately, minimizing the risk to a great extent.

By consciously seeking to build security controls into a wider workflow and automation strategy, you can remove operational inefficiency risks that come with siloed security; increase productivity; and ensure a better, safer, security state at all times in your business.

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360