ManageEngine
PAM360

# Bringing identity, security, automation, and ITSM together to deliver security and productivity transformation

Stephan Mann

www.manageengine.com/pam360

The world of corporate IT is known for its operational siloes, where one team—with its own purpose, objectives, responsibilities, and activities—works in isolation from a peer team rather than collaborating with other teams to collectively optimize theiroperations and business outcomes. A good example of this is the distance that's often found between corporate IT security and IT service management (ITSM) teams where, despite them both working in the best interests of their parent organization, they fail to work together effectively to optimize their individual knowledge, skills, and capabilities.

This article will explain how your organization can bridge the gap between security and ITSM teams and improve both operations and outcomes by implementing an automated, workflow-driven approach to reactive and proactive identity and access management (IAM). You'll also learn how good IAM and privileged account management (PAM) security posture requires a combination of security, automation, and service management capabilities.

## The traditional corporate positioning of security

While the aforementioned team-based siloes in IT and other parts of the business are well-known, corporate IT security teams and their work are often an extreme example. There's an odd dynamic at play, especially given the never-ending growth of cyber risks and the associated importance of IT security—every part of the organization should theoretically be clamoring to work with corporate security personnel to help ensure that the business is secure.

A commonly touted reason for the distance between the security team and ITSM operations is that security operations are seen as slow and a barrier to productivity, preventing ITSM personnel from speeding up both IT service delivery and support. As a result, the security team is deliberately kept at arm's length to prevent delays and the introduction of security-based hurdles that slow down the delivery, operation, and support of business applications and the employees who want to use them productively.

Additionally, the security team can be viewed as "living in an ivory tower" in business terms—positioning the importance of security protocols ahead of business needs and operations. While this is why they exist—to protect the organization—there's a fine line between securing the organization and applying so much protection that it stifles operations and holds the business back.

## The need for digital transformation in IT security management

Importantly, this silo-based method isn't only limited to human interactions. It's also relevant to security operations and the tools that are employed, where the operations are still overly reactive and manual and, while great IAM and PAM technology and tools may be in place, the technology is also leveraged in isolation. This results in a missed opportunity for end-to-end digital workflows where, as with many aspects of modern-day working, the biggest benefits come from the integration of tools, the capabilities they provide, and the data they hold. For example, security activities can become more proactive when they're integrated into ITSM workflows and automated.

This may be seen as the modernization of IT security practices but, more importantly, your organization benefits two-fold—it's more secure and the workflows and automation bring about greater productivity.

# Bringing IT security activities into ITSM workflows

IT service and support teams have long benefited from the power of ITSM tools, including the provision of digital workflows with capabilities such as automated routing, queue management, notifications and alerts, approvals, and service level targets, along with complementary digital capabilities such as self-service and knowledge management. This can be viewed as bringing IT security activities into ITSM workflows or, if you prefer, as bringing ITSM capabilities into security operations. The result is the same either way: With both technology sets integrated, this offers improved capabilities for both parties. For example:

- Security approval can be included within service request digital workflows. These can be service requests that have traditionally come to the IT help desk or requests that are directed at the security team. This capability is especially relevant where PAM comes into play. For example, when approving access to accounts, providing an audit trail of not only the what and the when, but also—importantly—who is granting that access and why is crucial.

- Knowledge management can be used to better share security-related information, whether it's a security policy, security guidance, or other security knowledge that's relevant to employees. Importantly, the security knowledge can be made available to different audiences in different formats. For example, security knowledge can be made available to IT service desk analysts within ITSM tool tickets, or business colleagues can access it via self-service capabilities provided by the ITSM tool.

- The ITSM tool's incident management process can be replicated to provide a security incident management process that's tailored to your organization's needs. The process can then be accessed by any party via a variety of channels—for example, by calling the IT service desk, emailing the IT security team, via a self-service portal, by using chat capabilities (both human and those that employ intelligent automation), or any other channel that's offered to employees. The security incidents can also be automatically created by security information and event management tools, whether they're simply being logged or requiring further action.

- The ITSM tool can be used to track the security status of employees, ranging from associated security-related IT incidents and overall related security incidents across the enterprise to the completion of mandatory security training courses. This information can be used to create employee security profiles for both ITSM and security team purposes.

- Teams should leverage the configuration management database (CMDB) for security and risk management purposes. Understanding security relationships and managing privileged accounts across a CMDB can bring a whole new dimension to understanding risk. For example, decisions on privileged access to one endpoint may be different when you know that the configuration item is being moved to be part of a high-risk, business-critical service.

## Leveraging automation more for faster security responses and increased productivity

As with traditional ITSM processes, a corporate ITSM tool can facilitate improved speeds, cost reductions, and better service experiences to security tasks through both the tool's native work management and automation capabilities and integrations with third-party tools. This optimizes the response capabilities for security-related issues, whether they're treated as IT incidents or security incidents.

For example, when security incidents occur and are created, either manually or via monitoring and event management tools, the response—including corrective action—can be automated in line with the agreed security policy. Alternatively, an automated workflow—with the benefits of automated routing, queue management, notifications and alerts, approvals, and service-level targets—can be used to ensure that the correct personnel are involved in handling a security incident through to resolution in a timely manner.

The benefits of automation also apply to scenarios where IT incidents have a security-related need. For example, when what the ITSM team has classed as a major incident requires significant security team involvement, appropriate digital workflows and other collaborative tools can be used to speed up responses and resolution. This includes getting the right personnel involved, coordinating work tasks and decision-making, coordinating communications to involved parties, optimizing response times, and escalating—either functionally or hierarchically—as needed.

Importantly, the use of automation to improve security team capabilities and joint security and ITSM operations and outcomes not only provides quicker responses to security threats and service requests but also improves employee productivity two-fold. First, for the security team or ITSM team members involved in the task, and second, for the employees receiving assistance from either or both teams. Both sets of productivity wins improve employee experience and the associated business outcomes

For example, automation makes onboarding and offboarding employees faster and safer, and employee role changes can also be enacted through role and privilege security automation integrated into the ITSM tool to benefit from its workflow automation capabilities. This extension of self-service capabilities could be the starting point in reducing the demand for human tasks, speeding up operations, reducing costs, improving the service experience, and optimizing business outcomes.

## In summary

Like many other business functions, corporate security teams cannot continue to work in siloes or rely on manually-intensive operations; if they want to ensure that they're able to fully automate their responsibilities and also to deliver these responsibilities "at the speed of business," security teams must meet both business and employee demands for better, faster, and cheaper operations and outcomes.

Your security team, in conjunction with your ITSM team, can better serve your organization and its employees by bringing identity management, security, automation, and ITSM best practices together to create end-to-end incident management and provisioning capabilities. Through the use of a corporate ITSM tool and digital workflow enablement in particular, the combined capabilities will deliver both security and productivity transformation, modernizing security operations such that the need for manual effort is minimized, IT and security operations are quicker, operational costs are reduced, service experiences are improved, and better business outcomes are realized, including the minimized impact of security-related issues and threats. So, look to integrate and automate your organization's security activities to benefit from enhanced security capabilities, improved productivity, and better business outcomes.

## About the author:

Stephen Mann

Stephen Mann is the Principal Analyst and Content Director at the ITSM-focused industry analyst firm ITSM tools. He is also an independent IT and IT service management marketing content creator, and a frequent blogger, writer, and presenter on the challenges and opportunities for IT service management professionals.

He has previously held positions in IT research and analysis (at IT industry analyst firms Ovum and Forrester and the UK Post Office), IT service management consultancy, enterprise IT service desk and IT service management, IT asset management, innovation and creativity facilitation, project management, finance consultancy, internal audit, and product marketing for a SaaS IT service management technology vendor.

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