Case Study
ebridge Increases Security Team Effectiveness

Learn how ebridge automates notification and approval processes while integrating a successful smart workflow for this company.

Security teams face a range of issues in managing day-to-day workflows, especially when department functions are operating within their own silos. A major issue is that these teams lack the visibility necessary to keep security alerts and approvals moving through a workflow quickly. When only some teams within an organization have visibility, localized within the client's enterprise security tool, security efforts are not as effective as they could be.

This was the case for a large organization that was struggling with security efficiency, patching, and lifecycle management. Entry in Excel for the population of the configuration management database (CMDB) such as ServiceNow, alert management, and follow-up all required manual, human entry. As such, workflows were getting stuck, and the organization lacked the visibility it needed to act.

These are the usual symptoms of Champion Solutions Group clients before they implement a tool like ebridge—teams working in their own silos, processes taking longer than they should, a lack of visibility at the top of the organization about security vulnerabilities and response time.

As Drew Baumhauer, Senior Full Stack Engineer at Champion Solutions Group says of security integration, "Alerts must be visible; they need to be in plain sight, and you want to remediate them as quickly and efficiently as possible."

One clear problem was that the organization needed to eliminate the "swivel-chair integration" that many teams face. This means that required security information for alert response isn't available in one place but within many different applications, and has to be pulled together from these systems, which takes a lot of time.

Other common problems for security teams, which this organization also faced, include lingering security offenses, unpatched endpoints, and inconsistency of data in the client's CMDB. These issues are often just the tip of the iceberg.

ebridge steps in

Then came ebridge. This real-time interface integrated this organization's tools, completely transformed operations, and eliminated errors. ebridge also introduced key metrics that are necessary for continuous team and organization improvement. Before ebridge, this level of growth would have been impossible because metrics weren't in place and alerts weren't managed efficiently.

Before ebridge, approval processes were lengthy and not integrated. For instance, if the security team received a routine alert, that alert would create an email chain. The security team members would then have to determine who to copy on the email and who could approve it. With ebridge, Baumhauer says, "We're automating notifications as well as the approval process," which is a major part of the security team's responsibility.

Now, security alerts are correlated with vulnerability patches. Security remediation measures are visible to the patching team, and data from the security information and event management (SIEM) and Management software automatically populates in the CMDB. Alerts and approvals move through the system and create workflows without emails between departments, which were slowing things down. Security and patching administrators initiate remediation all within the ServiceNow user interface, with visibility to management and the C-suite.

ebridge also gathers performance measures that are crucial for an organization to know how it's performing. For example, this organization can now measure the time it takes to resolve an issue, which is a crucial metric for any business.

The enhanced visibility that ebrdige brought to this security team's environment, along with the more abundant data present in the CMDB, turned asset management into a science, rather than guesswork

With ebridge, the team now has the power of automation and reporting metrics. Therefore, they can focus on proactive, continuous improvement in their day-to-day work, instead of getting hung up on the lengthy alert-response or email-approval system.

This is an example of how ebridge can turn clunky processes into smart workflows that push businesses forward.

ebridge is a real-time interface from Champion Solutions Group that connects a business's enterprise IT and security applications within ServiceNow. Unlike any other solution, ebridge produces a fully collected data set that's quickly delivered to ServiceNow and integrated with security management processes.

Learn more about how ebridge can automate, streamline, and improve visibility for security teams, contact Champion Solutions Group today.

For more information, call 800-771-7000 or visit
www.championsg.com/ebridge