IT RISK MANAGEMENT & GOVERNANCE

IT roulette – risk a breach or risk downtime

What is the scarier prospect? An unaddressed vulnerability leads to a breach where data is stolen and customers are negatively impacted? Or a patch is released and inadvertently takes down environments leaving angry customers and stakeholders? This is the conundrum facing IT teams every day, but why should they have to choose? Why can't there be balance? Today there is a lack of balance because of the SecOps Gap. Security fights for one agenda and Operations fights for the other – and unfortunately both a breach and downtime may be the consequence. You **can** close the SecOps gap and protect your business and company's reputation. You don't have to make a choice. You can achieve both objectives for security and operations with a strategic approach to integrating processes and automation.

While the Security team identifies the threat, it's up to the Operations team to implement the patch. Plus, while Security may in some circumstances also perform audits, it almost never makes its own changes. That responsibility remains with the Operations team. The Operations team may attempt to control change but because of limited resources, and the need to maintain a high level of performance and availability, it can take too long to resolve even known issues where fixes are available. The time between when security issues are identified and resolved can be weeks or even months. This situation can compromise business requirements for the speed and agility needed to stay competitive.

Fast track security with TrueSight Vulnerability Management for Third-Party Applications

Explore TrueSight Vulnerability Management for Third-Party Applications ›

See how you can accelerate vulnerability resolution, lower costs of remediation and avoid major security incidents.

- Prioritize and remediate vulnerabilities with TrueSight Vulnerability Management for Third-Party Applications
- Reduce time spent logging changes in CM system
- Improve systems stability through granular, role-based access
- Explore the security view to see predictive SLAs and burndown with TrueSight Vulnerability Management for Third-Party Applications

The cost of misalignment

Both teams need a better way to collaborate because the SecOps Gap is costly and risky. One-off, manual compliance and security efforts are falling short, particularly as the frequency of audits, regulatory changes, and new threats increase. More than 80 percent of attacks target known vulnerabilities and 79 percent of vulnerabilities have fixes available on the day of disclosure. The average cost of a data breach is $3.5 million. Breaches not only leave the business at risk but they can damage a company's reputation, bring staggering financial consequences, and distract the business.

Establish and automate processes to increase collaboration between Security and Operations

To address their most urgent compliance and security challenges, Security and Operations need to take a comprehensive, policy-based, and automated approach to identify threats and track them across their lifecycle to close the SecOps Gap. They must make vulnerability assessments much more actionable. This involves creating collaborative workflow processes used by Security, Operations, and business units. It entails establishing clear and targeted metrics that relate to actual business processes and functions. These metrics should account for the unique characteristics of each asset.

Instead of using static reports, these assessments need to provide Operations teams with rich, contextual insights so they can remediate problems quickly, understand how to prioritize remediation, determine how to schedule the remediation to minimize business impact, and so on.

It is also important to equip Security teams with the ability to conduct automated audits that offer live configurations to reference systems and make it easy to troubleshoot issues caused by discrepancies. In addition, it should be easy to evaluate the current state versus the last "known-good" state.

Remediation for known vulnerabilities should be automated. Manual remediation efforts carry a high opportunity cost for the business, as shown in Figure 2. These efforts require management and

oversight by seasoned, high-level personnel, who not only earn higher salaries but also may be diverted from strategic work. The manual and repetitive nature of the tasks causes many to consider drafting a small army of lower paid resources to pick up the burden. Unfortunately these folks may not have the expertise needed to be truly effective and will still rely on the more seasoned resources for guidance. Lastly, manual remediation takes more time, posing the risk that vulnerabilities and compliance violations may not be corrected promptly.

When known vulnerabilities are involved, automated remediation should be enabled to address any identified issues immediately and return the environment to the required state. Remediation should be scheduled or triggered on demand, without the need for developing scripts. If manager approvals are required as part of the remediation, they should also be automatically triggered as appropriate. If an issue arises, built-in mechanisms should enable the system to be rolled back to its last “known good” state.

Figure 2. The typical SecOps workflow involves extensive manual processes

In Figure 3, the automated processes dramatically expedite the time between a vulnerability is identified and remediated.

Figure 3. Automated processes can accelerate remediation in the typical SecOps workflow

The business benefits of establishing an effective SecOps strategy

There are many quantifiable benefits for the enterprise that can be realized with an effective strategy to close the SecOps Gap. These include:

- **Reduction in windows of vulnerability –** Automation can significantly reduce the elapsed time between identification and remediation of a vulnerability.
- **Reduction in labor costs –** By eliminating manual efforts such as patching and provisioning, organizations can save time and reduce labor costs.
- **Reduction in outages or performance issues arising from poorly applied patches –** When patches are applied manually to individual components, errors are likely. Quite often, these errors can lead to outages and performance issues. Effective automation significantly reduces the risk of human error.
- **Reduction in fines for noncompliance or breach –** By leveraging automation, organizations can more quickly and effectively address their SLA and regulatory mandates to reduce the frequency of compliance breaches and associated penalties.

Sidebar: Automation should enable a policy-based approach for IT administrators to manage their data centers with greater speed, quality, and consistency. It should provide broad support for all major operating systems on physical servers and leading virtualization and cloud platforms. The solutions should enable IT to install and configure server changes with ease and automate continuous compliance checks and remediation for regulatory requirements and security standards.

Develop a plan to close the gap

Security and Operations teams must have a plan to deal with vulnerability remediation, meet regulatory compliance standards, and ensure that their applications deliver the performance and availability needed to meet the demands of the digital enterprise. They must take control of issues that contribute to vulnerabilities and data breaches to protect their business and customers.

Just as ITIL best practices for service management focus on people, processes, and technology, these same elements can help organizations to develop a plan to close the SecOps gap. In terms of people-related objectives, the strategy should include having a consistent vision for Security and Operations teams with independent and shared goals to support security and compliance objectives. These teams need to balance their goals together to meet business requirements.

Processes should incorporate these shared goals and repetitive manual workflows should be reviewed. These workflows may become opportunities for automation. The flow of responsibilities between the two teams should be collaborative.

Automation can enable better coordination and collaboration and the technology used should resolve the root problem, rather than just segments of it. This technology should provide the ability to meet the needs and complexity of your business. For example, it should incorporate tools for automating corrective actions and providing a centralized view into vulnerabilities and remediation actions.

Keep in mind as you build your strategy that these important actions to help Security and Operations work together are essential for preventing security breaches and ensuring compliance with regulations. By taking this strategic approach, you can protect your enterprise and company's reputation, while maintaining the agility needed to meet the challenges of the digital economy.