7 STEPS TO ENSURING A “SECURITY-FIRST” MINDSET

October is Cybersecurity Awareness Month, and as organizations face an ever-evolving landscape of cyber threats, building a robust security posture is even more crucial. By incorporating good security practices and protocols, organizations can enhance their ability to protect sensitive data, prevent security breaches, and detect and respond to incidents. Here are our seven key recommendations to help bolster your security efforts.

1. Avoid friction points with a centralized approach to incident response.

Teams that operate in silos and follow manual processes make mistakes and create unnecessary delays. By bringing together incident management capabilities, organizations can efficiently detect, report, and respond to security incidents in a consistent and timely manner. This facilitates seamless communication, enhances incident resolution, and minimizes the impact of breaches.

2. Remain diligent with change management practices.

A strong security posture requires diligent change management practices. It’s essential to streamline the process for security-related changes such as system updates or access control modifications. By automating workflows and adhering to established change management procedures, vulnerabilities introduced during system changes can be minimized, ensuring a secure environment.

3. Maintain good management of security assets and configurations.

Proper management of security assets and configurations is critical to mitigating risks. Organizations need to maintain accurate, up-to-date information about hardware, software, network devices, and

user access rights. With comprehensive asset and configuration management, security teams gain enhanced visibility, enabling them to monitor, track, and secure critical resources effectively.

4. Streamline the remediation process with automation-driven vulnerability management.

Integrated vulnerability scanning tools help identify and prioritize vulnerabilities across an organization's infrastructure. By automating vulnerability assessments and linking them with asset management, the remediation process is streamlined. It enables security teams to prioritize patches or mitigation actions based on risk severity and impact. This helps organizations stay ahead of emerging threats and maintain a resilient security posture.

5. Ensure efficient request fulfillment.

Security-related requests, such as access control or security policy exceptions, need to be managed efficiently. Make sure you can facilitate the management of these requests through standardized and automated workflows. By ensuring that security controls are followed, organizations can reduce the risk of unauthorized access or policy violations, further enhancing their security posture.

6. Be prepared for a continual state of compliance.

Operations teams must continuously meet compliance and audit requirements. Automating workflows to document, track, and report on security-related activities helps demonstrate adherence to security policies, industry standards, and regulatory obligations. This ensures organizations are in a continual state of compliance and are prepared for audits.

7. Leverage good knowledge management for informed decision-making.

Create a centralized knowledge hub for security documentation, procedures, and best practices that is easily accessible to security personnel, empowering them with valuable information during incident response and security operations. By harnessing this knowledge base, organizations make informed decisions, share insights, and provide access to relevant resources, leading to a more proactive security posture.

Conclusion

Your business operations teams play a pivotal role in building a strong security posture across organization. It's imperative to stay ahead of evolving cyber threats by continuing to embed security practices within your operations management process to help accelerate the journey towards a resilient security posture. This is a powerful way to safeguard your digital assets, protect sensitive information, and maintain the trust of your stakeholders.

BMC Helix and Security

With BMC Helix, you have a powerhouse behind you to build a strong security posture across your organization. BMC Helix helps align IT and security teams around common workflows for handling security incidents, enables your teams to prioritize and remediate critical vulnerabilities, and systematically addresses compliance violations through an integrated and automated approach

across your multi-cloud environment.

Find out more about how BMC Helix can help you ensure a Security First Mindset.
https://www.bmc.com/it-solutions/secops-security-operations.html