JESKELL Systems, LLC | Best Practices

Cybersecurity Best Practices: Assess, Improve, Repeat

Cybersecurity is one IT project that is never completed. That's because there is a global, growing community of sophisticated criminals dedicated to breaking through your organization's latest defenses. As a result, cybersecurity requires continual reassessment and retuning to minimize the impact of an attack. Wait? Does that mean the risk of a breach cannot be eliminated? Correct. All organizations will face attacks, if they haven't already. The strategy is to minimize risk and get smarter from experiencing a breach.

In this climate, it's no surprise that a report by MarketsandMarkets pegs the cybersecurity market at $248.26 billion by 2023 with a compound annual growth rate of 10.2%. Despite this investment, stretched IT teams and systems integrators often lack the resources to develop the security expertise needed to evaluate gaps, and select and deploy optimal solutions. In the federal space, for example, the Continuous Diagnostics and Mitigation (CDM) program provides agencies with funding for cybersecurity tools but not always the services to deploy them.

That's where Jeskell steps in. We're a systems integrator with decades of experience building and deploying advanced security systems for federal agencies, commercial firms, and IT consultants. We offer deep security skills and knowledge of the latest security trends, along with high-value gap analysis, infrastructure planning, and deployment services. Jeskell has a long track record of providing optimal security outcomes with maximum speed and efficiency and at lower cost compared to other firms.

In this eBook, we share with you several best practices related to four cybersecurity technologies that are critical to protection of your infrastructure:

- Security information event management (SIEM)
- Endpoint management and automation
- Identity and access management (IAM)
- Incident response (IR)

SIEM: ALL EYES ON DECK

As the intelligent foundation of any cybersecurity environment, a security information event management (SIEM) solution keeps administrators informed of incidents and vulnerabilities in real time and can significantly reduce risk of a breach. SIEM collects, correlates, and analyzes data from security tools, such as vulnerability scanners, anti-virus solutions, and endpoint monitoring.

Unlike basic log managers, which collect logs with limited correlation and analysis, SIEM provides comprehensive, real-time protection across your enterprise. The most effective SIEM strategy unifies and monitors physical, virtual, mobile, and Internet of Things (IoT) environments.

Jeskell was an early adopter of IBM QRadar, one of the industry's most widely used SIEM tools, and has extensive experience with other security solutions as well. Using built-in analytics, QRadar reduces the impact of threats with accurate, high-speed detection and analysis.

We work with customers to ensure their SIEM solution is capturing and reporting on all relevant activity in the most streamlined, efficient way possible. For first-time SIEM customers, we conduct a gap analysis, identify the best tool, and tightly integrate it with other tools in use. We also analyze existing SIEM environments and plug any gaps by better integrating SIEM with the other tools.

ENDPOINT MANAGEMENT AND AUTOMATION: THE BEST DEFENSE IS A SMART, AUTOMATED ONE

Endpoint management is a vital layer that improves your protection while simplifying systems administration. This is music to the ears of many IT professionals who must manage growing, increasingly complex infrastructure while staff resources are maintained or even reduced.

We've worked with several endpoint management solutions, but we would like to highlight IBM BigFix, a top solution in this category. IBM BigFix will:

- Centralize and automate software patching and remediation
- Help IT operations and security teams collaborate better
- Reduce risk by preventing users from making unauthorized changes to endpoints
- Monitor and analyze software usage and other user activity
- Scale up to 250,000 endpoints
- Reduce costs by eliminating redundant tools and tasks

We help our customers identify their risk factors and build custom security policies. Further, by correctly automating tasks, such as patching, you keep your environment up to date and protected against the latest threats while reducing complexity and operational costs.

IAM: PROTECTING YOUR MOST VALUABLE RESOURCE

One of the industry's best tool sets in identity and access management (IAM) is IBM IAM, which provides an ideal balance of silent security operating in the background while providing users with a positive digital experience. IBM IAM's key capabilities include:

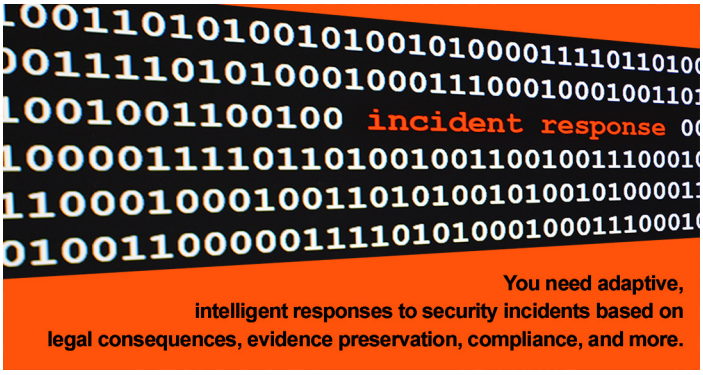
- **Access management**—Deliver the correct level of access to the right people across web, mobile, cloud, and legacy environments with risk-based access, single sign-on, integrated access management control, identity federation, mobile multi-factor authentication and more.
- **Identity governance**—Securely grant access rights and entitlements; report on user access and activity, prioritize compliance actions with risk-based insights; make better governance decisions, and intervene only when risk is detected.
- **Privileged account management**—Protect privileged accounts from abuse and misuse with enforcement of least privilege policies and efficiently discover, manage, and audit privileged account access.

As an IBM preferred provider, Jeskell has deployed some of the largest and most sophisticated IAM projects in the U.S. We often recommend that our customers integrate IAM with the HR system and make HR the identity of record. That way, information about new hires is automatically sent to the IAM system, avoiding the need to enter data twice. We also assist our customers with integrating their IAM and SIEM environments to help them efficiently assess employee behavior and assign risk scores.

With our industry-leading security skills and knowledge, we help our customers build IAM systems that greatly improve governance, efficiency, and user productivity.

INSTANT RESPONSE AND NOTHING LESS

Automated incident response (IR) tools are gaining in popularity, especially in the federal and foreign government markets. Traditionally, ticketing systems treat security incidents, which require specialized security expertise and instantaneous response, and IT incidents the same way. Today's IR tools provide adaptive, intelligent responses to security incidents based on legal consequences, evidence preservation, compliance, and other factors.



IBM Resilient Incident Response Platform, one of the industry's most advanced IR solutions, automates and orchestrates IR workflow and provides recommended steps to responders. Constantly collecting and analyzing data, Resilient helps organizations handle complex attacks and adapt to fast-changing conditions.

Designed for streamlined integration with SIEM, Resilient provides responders with a single dashboard to view incidents across the enterprise and actions of other responders. Not only does this make responders more productive, but it provides senior management with real-time updates on IR status. Resilient also analyzes archival data to identify trends and areas for improvement.

Jeskell is one of the only firms in the U.S. with proven experience in deploying advanced IR solutions. We use this knowledge to help our customers design advanced IR systems and policies that help simplify and accelerate their response to complex threats.

QUICKER TIME TO VALUE

Jeskell has extensive experience in delivering large hardware and software reseller projects and offers highly skilled engineering services that include security risk assessment, integration, implementation, and delivery of advanced security solutions. In addition to holding a facilities clearance, we have staff with top secret/sensitive compartmented information (TS/SCI) clearances.

We offer a wide array of cybersecurity capabilities, including data integrity preservation, security analytics and machine learning, orchestration, and TSG-approved phone systems, among other services. As a small-to-medium business, we are more agile and cost-efficient, and offer quicker time to value compared to larger systems integration firms.

Here are some valuable security best practices that we suggest you embrace:

- **Comprehensive gap analysis**—Identify and prioritize the risks of your various processes and measure the potential consequences.
- **Security Expertise**—Determine if you will invest in training your staff in security tools or hire an outside firm with security expertise.
- **Enterprise-wide alignment**—Ensure that business and technical leaders have reached agreement on the top security priorities and requirements.
- **No such thing as one and done**—Even if you have the latest security solutions, guard against becoming overly confident. The goal is to minimize the likelihood and impact of a breach and continue to adapt your response.
- **Continuous reassessment**—Commit to a quarterly plan for evaluating system health and any new gaps and requirements.

Following these best practices and integrating all or at least some of the highlighted solutions will significantly fortify your infrastructure and organization against evolving, nefarious cybersecurity threats. Through automation and orchestration, productivity and efficiency will improve for users and IT and security operations, generating cost savings for your organization. Perhaps most importantly, your organization will be able to focus more wholly on its mission with confidence.

Wondering where you stand? At Jeskell, we meet with our prospective and existing customers to provide an initial, complimentary assessment of their cybersecurity infrastructure on a quarterly basis. We would be happy to evaluate your security environment and discuss your goals.

IBM Platinum Business Partner

Schedule a consultation with Joseph L. Swartz, Jr., Account Executive, 612-296-0109, jswartz@jeskell.com.