M+E JOURNAL

The Future is Automated

The landscape ahead for M+E looks uncertain. Automation can ease the journey.

WORKFLOWS AND THE CLOUD
From cloud-based productions to unprecedented storage demands, the supply chain has never been more challenging

SMART CONTENT
The questions around AI, metadata, and analytics are endless. But we do have many of the answers already

SECURITY SOLUTIONS:
Cybersecurity and content protection in M&E is always on defense. Can automation can change that?

23.01

AUTOMATING THE WAY TO BETTER SECURITY OPERATIONS

ABSTRACT: Automation in film and TV production is increasing rapidly whether in visual effects and animation, AI in localization, motion capture or analyzing viewer reactions. Invariably automation involves cloud workflows and web facing applications where stringent security is paramount but not always configured correctly.

By Nipun Mehta, CTO, CISO, and
Jason Shea, Application Security Lead,
Convergent Risks

The advancements in technology have brought about unprecedented changes in the way businesses operate. The media and entertainment industry has also undergone a paradigm shift, where not only the creation but also the distribution and consumption of content have been transformed. It is hard to predict where this will ultimately lead, with a lot of potential yet to be unlocked.

Due to efficient workflows, content owners can speed up process, reduce costs and enhance the quality of products. The distribution of content can now reach a wider global audience with similar efficiencies and effectiveness.

However, the technological complexity and scale of production pose a significant challenge. As content and information security professionals, our primary objective is to safeguard the critical assets and the ecosystem through which they flow, from creation to distribution, "script to screen."

As technology advances security measures must keep up. How can you safely manage the increasing complexity when your security capabilities are limited?

Automation! Security operations must keep up with the need for speed, flexibility, excellence, and cost-effec-

CLOUD SECURITY AUTOMATION CAN IMPROVE THE EFFECTIVENESS and efficiency of an organization's security operations, reduce the risk of security incidents, and improve the overall security posture within a cloud environment.

tiveness. Security automation is essential, covering all the critical stages of security operations, from monitoring to analysis, reporting, and remediation. It's vital to use automation tools and techniques that don't disrupt the creative process. The mission to safeguard the "confidentiality, integrity, and availability" of content, systems, and workflows that support it, making automation a top priority.

What are the opportunities for automation and what will make the biggest impact?

Efficiency, consistency, and standardization: Automation in isolation is not a silver bullet for mitigating risks, using the best security tools and technologies is not always enough. Secure deployment, configuration, and response must be consistently managed to maintain efficiency, consistency, and standardization. Human error or malicious acts remain significant causes of security incidents and breaches. Automation can help prioritize and complete security tasks quickly, reducing risk and freeing up resources to complete critical security tasks that automation cannot perform. Automation provides opportunity for the consolidation of resources, reducing complexity and cost. By minimizing the likelihood and impact of human vulnerabilities being exploited, automation ensures that security tasks are executed according to established policies and standards, reducing the potential for compliance violations. This applies to legal, regulatory, or contractual obligations.

Enhanced visibility: Automated security tools offer improved visibility into security events, enabling swift identification and response to incidents. This helps prevent security breaches from escalating, crucially protecting internal networks and critical assets across all environments. As security professionals, we must assume that breaches WILL happen and should prioritize comprehensive protection rather than focusing solely on creating an impenetrable perimeter.

Improved compliance: Scanning systems via automation can identify compliance violations, generate reports, and trigger remediation. Given the increasing scale of cloud-based infrastructure, services, and workflows it is no longer feasible to follow manual processes to ensure that systems stay compliant.

Scalability: Automated security enables scalable security operations as business grows. Automated tools can help to manage security for large and complex environments, without the need for additional staff or resources.

What are some of the key specific areas where we can apply automation to ensure that our reach continues to align with our grasp?

Real-time threat detection and response: Automation can quickly identify and respond to security threats using machine learning algorithms that analyze network traffic. Automated responses may include isolating compromised systems or blocking incoming traffic from harmful IP addresses.

Automated identity and access management (IAM):

Nipun Mehta *Nipun Mehta is the chief technology officer at Convergent Risks and is responsible for the company's risk advisory and managed technical assurance services. Mehta has a pedigree of driving transformational change, helping technology organizations re-architect, modernize, and evolve for a digital future.*
nipun.mehta@convergentrisks.com @ConvergentRisks

Jason Shea *is the senior director of app and cloud security for Convergent Risks and is a key member the App Sec team providing security assessments and consultancy services to the ME supply chain. His major studio background brings considerable application security experience and supply chain understanding.*
jason.shea@convergentrisks.com @ConvergentRisks

Automating user access ensures appropriate access levels to systems and data, and prompt revocation of access when necessary.

DevSecOps: Security should be integrated into the software development lifecycle (SDLC) from the start, rather than waiting until the end. Automation is crucial for seamlessly and comprehensively integrating security into development workflows.

How can automation be applied to DevSecOps?

Continuous integration and continuous deployment (CI/CD): can create a continuous integration and continuous a deployment pipeline that incorporates security testing. Automation can include code analysis, vulnerability scanning, and penetration testing to identify and address security issues as you develop.

Static code analysis: application security tools can analyze source code for common security issues such as buffer overflows, SQL injection, and cross-site scripting.

Dynamic application security testing (DAST): application security testing tools scan running applications to identify vulnerabilities. DAST tools can simulate attacks on the application and identify vulnerabilities such as injection flaws, broken authentication/authorization, and insecure cryptographic practices.

Configuration management: configuration of infrastructure components e.g., servers, databases, and networking equipment can be automated to ensure that systems are configured securely, with appropriate access controls, encryption, and logging.

IMPLEMENTING AUTOMATION FOR CLOUD ENVIRONMENTS AND SAAS APPLICATIONS

Cloud security: Cloud security automation involves tools and processes to manage security in cloud environments. With the increasing use of cloud infrastructure, automation has become essential for securing cloud-based systems.

Cloud security monitoring: cloud security automation tools and processes secure cloud environments, this is essential to the growing use of cloud infrastructure.

Cloud security posture management: Cloud security posture management automates security configuration settings for consistent security settings across multiple cloud services and regions.

Infrastructure as code (IaC): infrastructure automation that involves using code to manage and provision infrastructure resources. IaC can improve security by enabling consistent and repeatable infrastructure configuration and reducing the risk of configuration drift.

Compliance automation: used to manage compliance with regulatory requirements and industry standards in the cloud environment. Automated tools scan cloud infrastructure for compliance violations, generate reports, and trigger remediation actions.

Vulnerability management: automated vulnerability management is crucial in today's environment where numerous systems require patches. It automates the detection, patching, and remediation of vulnerabilities in cloud infrastructure, ensuring it remains secure and protected from known vulnerabilities.

Incident response: automated incident response workflows ensure that incidents are properly triaged, and appropriate responses are taken to mitigate the impact of the incident.

SaaS security posture management (SSPM): As businesses increasingly adopt SaaS applications, security teams face new challenges in ensuring the security of pre-release content. SaaS offers benefits such as cost savings, scalability, and automatic updates, but can also create visibility gaps. SaaS security posture management (SSPM) can help address these challenges by providing visibility into where pre-release content is stored and controlled by third-party entities and assisting in protecting pre-release content through various security measures.

Improved visibility: SSPM provides organizations with a comprehensive view of their SaaS applications, including which applications are being used, who is using them, and how they are being used.

Enhanced security: SSPM helps to identify and address security vulnerabilities and misconfigurations within SaaS applications, thereby reducing the risk of data breaches and other security incidents.
Regulatory compliance: SSPM can help organizations comply with regulatory requirements by identifying

and addressing potential compliance issues within SaaS applications.

Cost savings: SSPM can help organizations optimize their SaaS usage and avoid unnecessary subscriptions, resulting in cost savings.

Better risk management: SSPM helps organizations identify and mitigate security risks associated with their SaaS applications, reducing the likelihood of security incidents and associated costs.

In summary cloud security automation can improve the effectiveness and efficiency of an organization's security operations, reduce the risk of security incidents, and improve the overall security posture within a cloud environment.

We hope this article provides insight and thought leadership on how automation can help us constantly improve our ability to secure pre-release content, the crown jewels of our industry. ⊞

Helping You Achieve TPN Gold

TPN TRUSTED PARTNER NETWORK

We are the principal provider of security assessments for the major content owners and their M&E vendor supply chain. Our assessor team offers the widest experience and guidance for your environment. We work with pre-production, production, post-production and distribution vendors across the globe through our offices in the Americas, EMEA and APAC.

In addition to helping you achieve TPN Gold assessment status, our services include cloud and application security consulting, web app and infrastructure penetration testing; internal vulnerability scanning as a managed service (cloud configuration & infrastructure), management policies; incident response; SOC2/ISO/NIST readiness; and privacy compliance.

convergent

Contact Us
For more information or general enquiries:
e: info@convergentrisks.com
w: www.convergentrisks.com
US Office: +1 (818) 452 9544
UK Office: +44 (0) 1276 415 725