Server Automation Maturity Model
Lifecycle Management

**AD-HOC**
Collaboration does not occur across teams, defined processes either do not exist or are rudimentary. Automation is not in use, nor are scripts or comprehensive spreadsheets. Security vulnerability management, patching, and configuration changes are done manually and on an as-required basis. Compliance management is done manually and only in preparation for an audit. Audit failures occur and findings require corrective action. Configurations are managed manually, and configuration drift adversely affects service performance and availability. Minimal use of metrics, and reporting is very limited. Discovery and change management are done manually.

**INITIAL**
Some collaboration across teams, and procedures are in place within individual teams. Security scanners may be deployed but follow-up is manual, tedious, and limited. Some patching is done, usually with tools provided by OS vendors. Regulatory and policy compliance management is done manually and prior to audits, but audit failures still occur and require follow-up. Golden configuration images are available and are deployed manually, configuration drift is manually remediated when problems arise (reactive). Some metrics are in place and reporting is done manually. Discovery and change management are performed using tools such as spreadsheets and email.

**INTERMEDIATE**
Cross-team collaboration within organizational domains occurs. Automation is adopted for certain tasks and select use cases. Security vulnerability scanners are deployed and data is manually analyzed, scripts are used for patching and configuration changes, approximately 10-15% of vulnerabilities are remediated. Internal audits assess compliance with regulations and policies, results are documented and follow-up is usually completed prior to formal audits – which still generate findings requiring attention. Golden configuration images are deployed, configuration drift and unauthorized changes are remediated using internally developed tools. Discovery and change management are done manually. Key metrics are manually collected, tracked, and reported for each organizational domain.

**ADVANCED**
Enterprise-wide collaboration across teams is in place, focus is shifting from tactical to strategic use of IT. Security scanner data is augmented with discovery integration for vulnerability blind spot detection. Vulnerability analysis, prioritization, and remediation are automated. Compliance templates are in place and are periodically updated, automated detection and remediation of
non-compliant conditions is deployed. A state of continuous compliance and audit readiness is achieved. Detection and remediation of configuration drift from golden master images is automated. Enterprise-wide, common reporting is being adopted or is in place.

Organizations at Level 4 and Level 5 (below) often shift from on-premises automation solutions to hybrid cloud, SaaS-based offerings to reduce procurement, deployment, and maintenance costs, receive enhancements more frequently and increase efficiency.

**INTELLIGENT**

High degree of collaboration across organizational domains. Proactive, automated, integrated solutions are in use. Task automation has evolved to process orchestration, which is in place across the organization for discovery, vulnerability management, compliance, configuration management, provisioning, ITSM, CMDB. Proactive, automated discovery of vulnerabilities (including blind spots), intelligence and advanced analytics are applied for vulnerability prioritization based on severity and business services exposed. Remediation is completed within SLAs and prior to availability of vulnerability exploit kits to attackers. Automated remediation is integrated with change management system via process orchestration. A state of continuous compliance is achieved via intelligent, automated remediation of non-compliant conditions. Automation is used to detect and remediate configuration drift. Enterprise-wide common reporting with metrics is in place, along with a management system designed to deliver continuous improvement.

**FOR MORE INFORMATION**

To learn more about managing server automation