

SERVICE DESCRIPTION

Puppet Enterprise Security Compliance Enforcement Capability Pack Service Description

Setup CIS compliance rules for your Puppet* controlled infrastructure

* Requires either Puppet Enterprise or Open Source Puppet

Contents

Overview.....	2
Components	2
Recommended for	2
Consulting Services Description.....	2
Deliverables	4
Delivery Approach	4
Phase 0: Preparation and Initial Discovery	4
Phase 1: Discovery	4
Phase 2: Installation.....	4
Phase 3: Workflow	4
Phase 4: Deployment.....	4
Phase 5: Documentation.....	4
Timeline	5
Fees.....	5
Key Assumptions.....	6
Appendix 1: Engagement Technical Requirements	6

Overview

Puppet consultants will provide services to help the customer deploy Puppet SCE (Security Compliance Enforcement) configurations and successfully integrate them into their infrastructure. The engagement will consist of knowledge transfer and paired configuration.

The objective is a working implementation of Puppet solutions that are designed to meet the customer's configuration management automation goals, and a customer team that is well prepared to continue its configuration management automation effort.

Puppet SCE requires either Open Source Puppet or Puppet Enterprise.

Components



- PE – Puppet Enterprise
- CD – Continuous Delivery
- IA – Impact Analysis
- SCE – Security Compliance Enforcement
- SCM – Security Compliance Management

Recommended for

- Customers interested in enforcing CIS compliance rules to improve the security compliance of their Puppet nodes.
- Customers who want to focus on making their infrastructure more secure and reducing their attack surface.
- Customers with Windows and/or Linux Puppet nodes

Consulting Services Description

Puppet will provide the following services related to the implementation of PuppetEnterprise:

1. Pre-engagement planning and preparation

- a. Discovery call(s)
- b. Draft project plan
- c. Other preparation items as needed (research, testing, etc.)
- d. To be completed by the Customer prior to the start of the engagement:
 - i. Validate appropriate compute, network, and storage has been provisioned
 - ii. Confirm full-time availability of at least one technical contact for the duration of the engagement

2. Discovery and concept review

- a. Determine goals and business needs
- b. Provide high-level overview of Puppet concepts, if needed

3. Install Security Compliance Enforcement

- a. Install/validate SCE Modules for Windows/Linux
- b. Prepare Hieradata for defining enforcement rules

4. Test and Validate Compliance Rule Enforcement

- a. Place test nodes in noop
- b. Review available rules for the OS under test
- c. Configure rules for validation in Hieradata configuration
- d. Run test in enforcement

5. Create Hieradata rule set for a Role

- a. Create 1 set of Compliance Rules to enforce on a Node
- b. Review changes made through enforcement

6. Recap meeting to close out engagement and to reinforce all concepts covered

Deliverables

1. Puppet SCE Installation
2. Configuration overview of Hieradata for SCE
3. Enforcement of a selection of CIS Compliance Rules for 1 node
4. Post-engagement documentation, including:
 - a. Installation details
 - b. Workflow summary
 - c. Recap of work performed
 - d. Recommendations

Delivery Approach

Our delivery approach is designed to effectively deliver fast time to value with Puppet solutions. We work with you throughout the engagement to implement initial base configuration of the solutions and prepare the Customer to extend configuration to align to expanding business objectives.

Phase 0: Preparation and Initial Discovery

The Puppet Consultant will spend up to half a day performing preparation and discovery work prior to the engagement. This includes pre-engagement call(s) with the Customer to discuss logistics and begin the discovery phase, project planning and preparation.

Phase 1: Discovery

The Puppet Consultant collaborates with the Customer to understand their technical and business goals, checks their high-level understanding of how the solutions work and how it will be implemented into the Customer's organization.

Phase 2: Installation

The Puppet Consultant and Customer installs the agreed solutions and validates their operation. Time is spent reviewing the architecture of these systems to ensure the Customer understands and can maintain them.

Phase 3: Workflow

The Puppet Consultant collaborates with the Customer team to design and implement a workflow that works for the organizational structure. Aligning the capabilities of the solution with the technical and business objectives.

Phase 4: Deployment

The Puppet Consultant pairs with the Customer team to bring the installed services into production readiness in line with the business and technical objectives and finish the commissioning.

Phase 5: Documentation

The Puppet Consultant will provide engagement documentation within five (5) business days of the end of the engagement, and will consist of the following:

- Engagement recap
- Architecture description and diagrams
- Workflow description and usage
- Recommendations for future enhancements to the Puppet Enterprise solution

Timeline

For every capability pack, one day (eight hours) is set aside for preparation and documentation, each requiring approximately half a day (four hours). Additional capability packs can be added to engagement to further evolve core concepts dependent on Customer requirements.

	Roles
Base	1
Additional Packs will add	Up to 5

Maximum of 4 capability packs, Customers with larger needs are encouraged to have a custom Statement of Work scoped to ensure their project needs are addressed.

For larger customers, we advise engaging Professional Services to size compilers appropriately.

Fees

Product Description	Duration	Cost
This is Security Compliance Enforcement Capability Pack	40 Hours	\$11,995

Puppet will use best efforts to complete the Services within this timeframe, but this project will be deemed completed if the maximum number of hours is reached.

Services for this engagement will be provided remotely, unless Customer and Puppet mutually agree that the Services will be performed on-site. In addition to the fees above, Customer will be responsible for reasonable travel and expenses for on-site Services.

Key Assumptions

The following assumptions are reflected in the services, timeline, and estimated effort outlined in this service description:

1. Phases 1-4 of the engagement (as outlined in this service description) will be performed during normal business hours (Monday through Friday, 8:00 a.m. - 5:00 p.m. local time), unless otherwise agreed to in writing by the parties.
2. Customer staff has completed PE10x, PE20x, PE30x courses within the last 12 months or has equivalent operational experience with Puppet.
3. Customer will provide prompt feedback on all deliverables.
4. Customer will provide prompt access to all systems and resources that Puppet will need to complete the work.
5. Customer must provide a single point of contact that will be available at least 75% of the time throughout the duration of the engagement.
6. Customer will provide Puppet with documentation and access to subject matter experts for non-Puppet systems/ software within the scope of the engagement.
7. Customer will have identified key personnel prior to the beginning of the engagement.
8. Customer will have all necessary security exceptions, firewall rules, network routers, computer and storage resources available prior to the start of the engagement, as detailed in Appendix 1 of this service description.
9. Puppet does not provide support for third-party software that is implemented as part of a Puppet Enterprise solution, such as version control systems, repository management, packaging, and other software that is not part of the Puppet Enterprisestack.
10. Forge modules may not exist for the Customer's specific use case. Puppet makes no guarantees about specific modules being available on the Puppet Forge. Any alteration to pre-existing Forge modules to meet Customer needs will be at Puppet's discretion and will be the responsibility of the Customer to support and maintain post-engagement.
11. Module development and/or automation task implementation is confined to work that can be reasonably completed within the engagement's allocated hours. As a result, such work may not occur, may be incomplete, and/or may require further effort from the Customer to complete post-engagement.

Appendix 1: Engagement Technical Requirements

A successful consulting engagement requires advance preparation. Failure to meet these pre-engagement requirements will have a direct impact on the completion of all the goals of the engagement.

The Customer is expected to review all requirements. Any requirements that are not met should be reported during the pre-engagement call or earlier. Puppet and the Customer will discuss the issues and determine whether to delay the engagement or attempt to work around the issue during the engagement.

BASIC CAPABILITY PACK REQUIREMENTS

The pre-engagement technical requirements as discussed in the pre-engagement call must be verified and completed by the Customer prior to the engagement. Failure to complete this will negatively impact Puppet's ability to meet all deliverables in the time allotted. Puppet bears no responsibility for delays due to incomplete pre-engagement requirements.