DATASHEET

# Vulnerability Remediation Service

## Business challenge

Vulnerability management is critical to infrastructure security, but many organizations have not established an efficient, reliable process. The work is often manual and siloed, and it can take weeks for IT Ops teams to prioritize critical vulnerabilities, let alone to actually address them. As a result, vulnerability response is incredibly time-consuming, taking companies an average of 443 hours a week.

Puppet's Vulnerability Remediation service helps organizations streamline vulnerability management, using Puppet Remediate to identify the vulnerabilities in your estate, prioritize the most critical, and mitigate the top risks.

## Who will benefit?

The Vulnerability Remediation service is recommended for new Puppet Remediate customers who want help building remediation content and developing a framework for more efficient vulnerability management.

## Customer benefits

- Increase the speed of addressing security vulnerabilities
- Get a holistic view of vulnerability data from Qualys, Rapid7, or Tenable
- Prioritize vulnerabilities based on risk-based reporting
- Address high-risk vulnerabilities
- Mitigate risks associated with open vulnerabilities
- Reduce constraints on internal resources

puppet

## What you can expect

A Puppet professional acting as an extension of your team will help develop a more efficient vulnerability management workflow, using Puppet Remediate to identify the vulnerabilities that pose the greatest risk to your systems and quickly mitigate the most critical threats.

The Puppet consultant will develop content to address the critical vulnerabilities identified, remediate existing vulnerabilities, and document a remediation framework to enable your team beyond the engagement.

## Assumptions

- Customer will agree on the list of vulnerabilities to be addressed during the engagement.
- Customer can run Docker in their environment.
- Customer has access to a supported vulnerability scanner: Tenable, Tenable.io, Tenable.sc, Qualys, Qualys VM, Rapid7, Rapid7 Nexpose, or Rapid7 InsightVM.
- Customer has access to the necessary machines.
- Customer will provide Puppet consultant with an environment to test code for remediating vulnerabilities.
- Customer will work with Puppet consultant to understand the proposed framework to be extended to future security vulnerabilities.

### Expected outcomes

- Installation of Puppet Remediate
- Integration of supported vulnerability scanner
- Guidance on creating tasks to remediate vulnerabilities
- Creation of remediation content to address vulnerabilities
- Documented framework for vulnerability remediation beyond the engagement