VULNERABILITY PATCH MANAGEMENT TEMPLATE

PURPLESEC

OFFENSIVE & DEFENSIVE
CYBER SECURITY

Burndown, remediate, and monitor vulnerabilities.

- Custom tailored plan
- Risk assessment
- Project Management
- Weekly & Monthly Reporting

GET IN TOUCH

(202) 556-3903
sales@purplesec.us
purplesec.us

WHAT IS PATCH MANAGEMENT?

Vulnerability patch management is a continuous process of identifying, prioritizing, remediating, and reporting on security vulnerabilities in systems.

There are 4 main steps in patch management including:

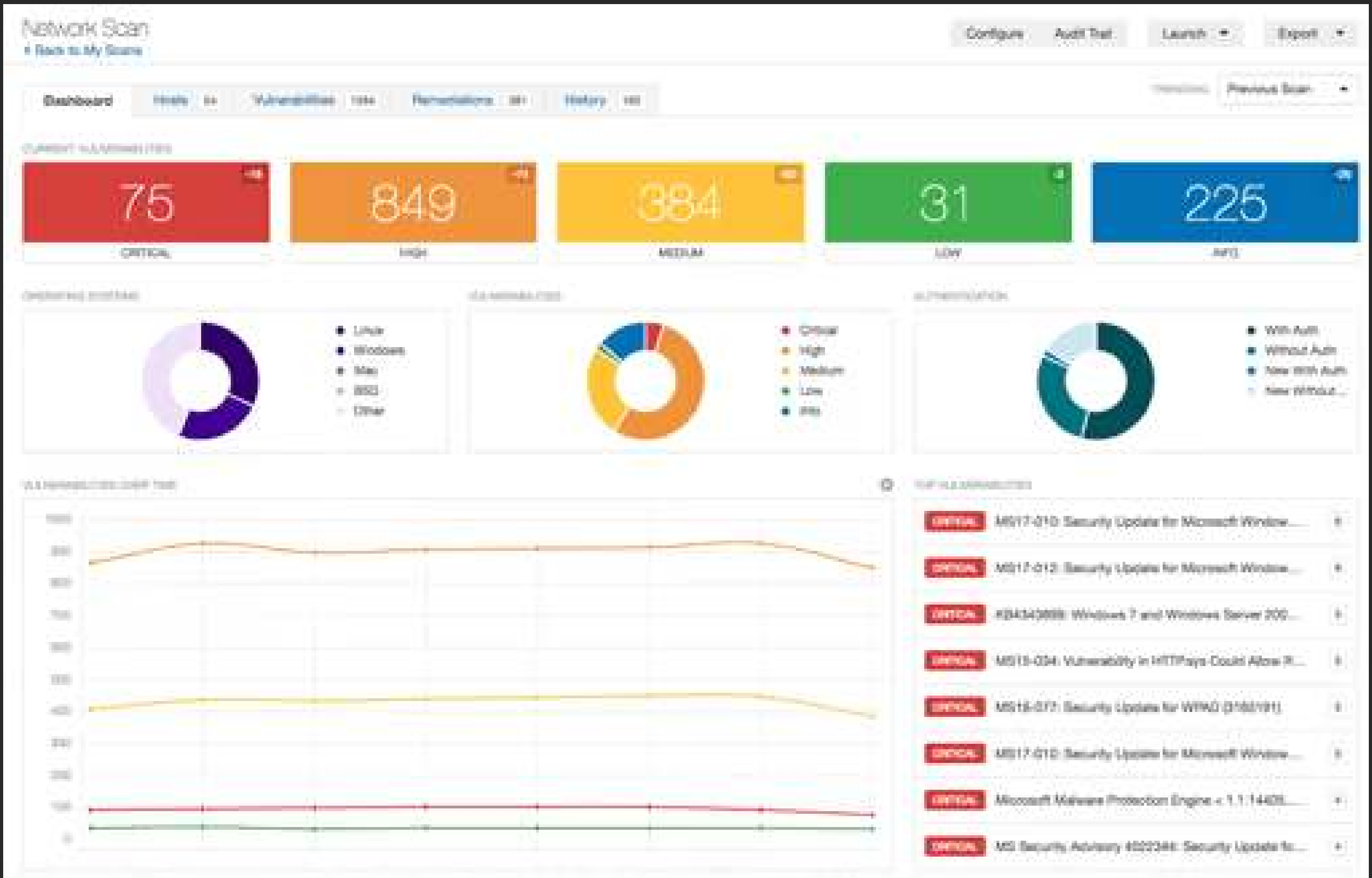
1. Risk Assessment
2. Remediation Plan
3. Project Management
4. Weekly And Monthly Updates

1.RISK ASSESSMENT

The highest priority items are determined based on the vulnerabilities found during scanning.

A senior security analyst analyzes the results and comes up with a list of prioritized patching recommendations.

We will help develop a patch management policy that works with not only Microsoft patch management but third party software as well based on your business needs and risks.



CRITICAL MS17-010: Security Update for Microsoft Window...
CRITICAL MS17-012: Security Update for Microsoft Window...
CRITICAL KB4343909: Windows 7 and Windows Server 200...
CRITICAL MS15-034: Vulnerability in HTTP.sys Could Allow R...
CRITICAL MS16-077: Security Update for WPAD (3165191)
CRITICAL MS17-010: Security Update for Microsoft Window...
CRITICAL Microsoft Malware Protection Engine < 1.1.14405...
CRITICAL MS Security Advisory 4022344: Security Update fo...

2. REMEDIATION PLAN

A patching plan to burn down the backlog of vulnerable systems is then drafted based on these prioritized recommendations.

This remediation plan will take into consideration the architecture that needs to be patched as well as software considerations.

We will work with the client to determine the best course of action for their business needs whether that be implementing SCCM, using third-party software, or some combination of both.

3. PROJECT MANAGEMENT

Our team of analysts is run by a project manager who will draft up the plan of action and milestones for the project with an executive report of the prioritized recommendations.

We will work with the client's staff and their current ticketing systems to submit recommendations and complete patching remediation in a trackable way so that we can deliver metrics as well as security value.

Our project management will help define the timeline of mitigation.

4. WEEKLY AND MONTHLY UPDATES

The patch management policy we develop will help keep your software and systems up-to-date every single week or month as patches come out.

In addition, we will provide semi-monthly and monthly statistics showing the reduction in your risk scores on your enterprise network as well as highlighting areas of greatest need and greatest improvement.

This will ensure that not only are your core operating systems and user systems updated but the software that runs on them are safe and secure as well.

OUR PATCH MANAGEMENT PROCESS

Our approach to patch management is a complete end to end process that begins with the evaluation of the output of scan results.

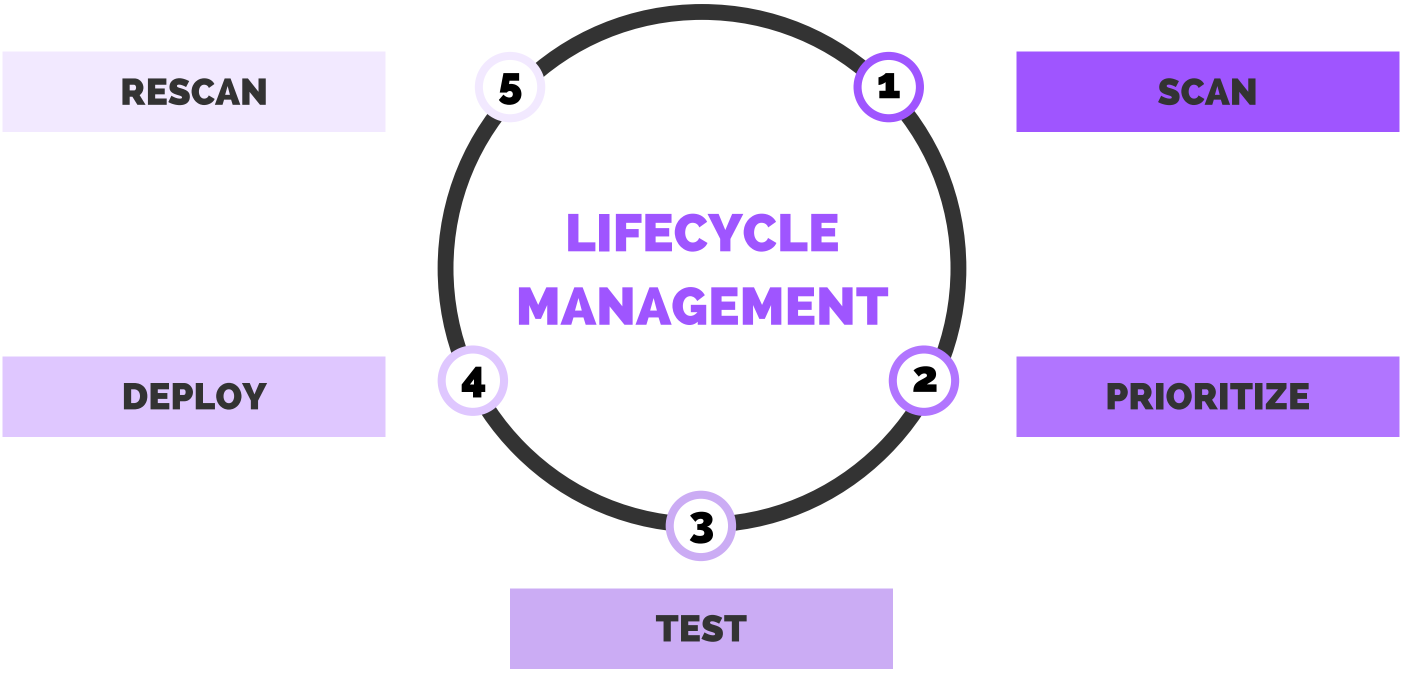
Next, we define the biggest risk to the organization as well as work with the clients to understand their greatest needs.

Finally, we identify the most important systems and the things that they need to keep protected to continue regular business operations.

VULNERABILITY MANAGEMENT LIFECYCLE

The vulnerability lifecycle is a 5 step process including:

1. Scan
2. Prioritize
3. Test
4. Deploy
5. Rescan



To that end, we begin with an evaluation and scope definition based on vulnerability scans obtained either through our services or through a previous vulnerability scanning assessment.

Using this information we define not only the risk but the scope as well and turn it into a project plan each of the vulnerabilities is classified given a plan for remediation and milestones aren't defined based on business needs a major milestone.

SPRINT PLANNING

- **Client delivers scans**
- **Risk categorization**
- **Remediation items prioritized**

PATCHES PACKAGED

- **Patch dependencies researched**
- **Verify Patches**
- **Impact Analyst (highest reward lowest risk to production)**

PACKAGE TESTED

- **Deploy patches to VM Lab**
- **Client's corporate image**
- **Patch quality testing**

TESTING RESULTS

- **Impact analysis**
- **Business considerations**
- **Client approval**

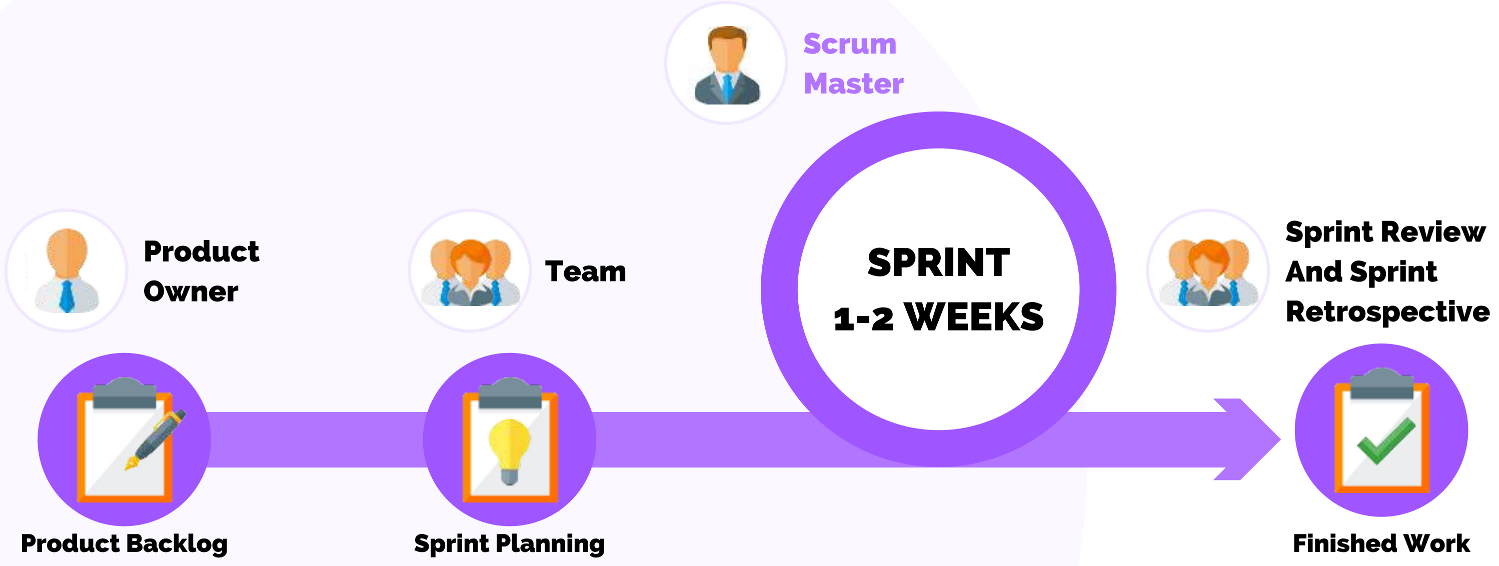
DEPLOYMENT

- **Schedule deployment within tools**
- **Waterfall rollout to avoid business impact**
- **Notify users**

POST DEPLOYMENT

- **Assess outcomes**
- **Recommend compensating controls**
- **Deliver activity reports**

Following the scoping, we then use the client's systems to set up a scrum or burned down project plan so that each of the items that need to be remediated is trackable from start to finish to ensure that the work is completed on time and it is auditable.



Our patch management process is designed to ensure that patching will have no impact on your day to day business activities.

We will use virtualization software working with client staff to test the patched systems for issues before deploying the patches to the fleet.

During the next phase of the project, we define the pace and turn around and begin our project burned down which includes creating weekly and monthly statements.

We will build out customized solutions for your business units who need certain programs and who may need justification for exceptions from patching.

Following each Sprint or set of sprints, we work with the clients to conduct another vulnerability assessment and obtain another baseline to validate that patch management has mitigated the risks.

VULNERABILITY PATCH MANAGEMENT AS A SERVICE

✓ **Our process is designed to help a customer maintain good patch management policies indefinitely.**

✓ **Unlike other patch management companies, we aren’t looking to just patch a subset of vulnerabilities and then leave you to your own devices.**

✓ **We have the capability to continue monitoring, patching, scanning, and remediating for as long as your business needs.**

GET A FREE CONSULTATION

HOW IT WORKS WITH PURPLESEC

We begin every engagement with a friendly chat to better understand your patch management needs.

A patching plan to burn down the backlog of vulnerable systems is then drafted based on prioritized recommendations.

A security engineer and project manager will create a custom plan of action and milestones for the project.

Observations and recommendations collected and formatted into a weekly and monthly executive reports.

SPEAK WITH AN EXPERT