Vulnerability Management Program Checklist

To strengthen your security posture and effectively protect against threats like WannaCry, your team must regularly apply patches and updates to your systems, devices and applications to prevent vulnerabilities from being exposed. But it shouldn't stop there. There are additional measures you can take to proactively mitigate the risk of a breach. This framework provides basic guidance that can help all businesses build a vulnerability management program foundation.

1 UNDERSTAND AND PRIORITIZE YOUR ASSETS

- Create a referenceable asset inventory of all authorized and unauthorized devices on the network; start by auditing your business' most critical information assets. Perform an initial discovery scan to identify your assets if necessary.
- Determine the criticality of each asset by assigning a criticality score based on importance to the business and the sensitivity of the information with which it interacts with.
- Define (technical) owners for each of the critical system(s) and/or groups of system(s) in your organization.

2 CONDUCT REGULAR VULNERABILITY SCANS

- Scan all internet and internal facing devices at least once a month.
- Always scan in authenticated mode, if possible.
- Use the same dedicated account to perform scan activity.
- Conduct a broad internal vulnerability scan at least once a year, including penetration testing.

3 AUGMENT VULNERABILITY MANAGEMENT

- Create a prioritization strategy based on your business' unique needs.
- Develop risk ratings based on the stated level of risk provided by vulnerability scan reporting compared to the criticality/sensitivity of associated items.

4 DEFINE PATCH MANAGEMENT

- Assign a process lead within your organization to manage the patch process.
- Develop and document a patch management process to address: patch assessment, harvest, testing and deployment.
- Create/revise a patch management/system update policy that reflects current patch management:
  - Systems attached to the network must be regularly patched to maintain the business' security stance and provide ongoing protection.
  - Critical security patches must be installed (after appropriate testing) within a defined timeframe, once released from the vendor.
  - Other non-critical patch application timelines should be defined within the policy.
- Patch often and proactively; always apply security updates.
- Subscribe to vendor press or news releases around patching and vulnerability reporting.
- Based on the risk ratings developed in the vulnerability management program, patch the highest risk vulnerabilities first.
- Ensure that all security infrastructure (e.g. firewalls, anti-virus, VPN, 2FA etc.) are running properly and regularly receiving updates.

5 EVALUATE COMPLIANCE REQUIREMENTS

- Identify and map compliance requirements associated with your industry and state.
- Run monthly and quarterly compliance reports to gauge alignment.
- Assess the status and success of the program, realign accordingly.

About eSentire

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-disrupting events. Protecting more than $5 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit www.eSentire.com and follow @eSentire.

esentire®