Alerting is either not available or only available within security-specific technologies.

### Change Management

Some changes related to vulnerability management directives are applied to the software and/or hardware that is treated as standard changes. Reasons related to standard changes, are treated as standard changes.

### Patch Management

Patches are applied manually or submitted by teams and/or users.

### Configuration Management

Configuration requirements are not well-defined and changes are either applied manually or through a directed set of procedures, some of which are only available for a subset of staff.

**Vulnerability Management Maturity Model**

**LEVEI 1** Initial

- **Policy & Standards**
  - Policy and standards are undocumented or in a state of change.

- **Context**
  - Contextual data (e.g., asset details, compliance, operational) is available from data repositories or from systems themselves in a piecemeal basis.

- **Automated**
  - Infrastructure and applications are scanned ad-hoc or irregularly for vulnerability details, or vulnerability details are acquired from existing data repositories or from the systems themselves at random.

- **Manual**
  - Manual testing or review occurs when specifically requested or required.

- **External**
  - External vulnerability reports and disclosures are handled on a case-by-case basis.

- **Prioritization**
  - Prioritization is performed based on patch management directives provided by identification technology or indicated in reports.

- **Analyse**
  - Root cause analysis is performed based on out-of-the-box information such as threat intelligence, vulnerabilities, and other investigative reports (e.g., DAST, Fuzzing, and/or other categorised reports (e.g., NMAP Top 100).

- **Metrics & Reporting**
  - Simple, post-time operational metrics are available primarily tracked from systems but not necessarily leveraging customisation or tailoring.

- **Communicate**
  - Alerting is either not available or only available within security-specific technologies.

- **Treat**
  - Configuration requirements are not well-defined and changes are either applied manually or through a directed set of procedures, some of which are only available for a subset of staff.

**LEVEI 2** Managed

- **Policy & Standards**
  - Policy and standards are defined in specific instances with minimal open and integrated security frameworks and are updated as needed in a state of change.

- **Context**
  - There is a central repository of contextual information and applications are defined and followed for certain departments or the organization.

- **Automated**
  - The process, configuration, and schedule for vulnerability management and applications are defined and followed for certain departments.

- **Manual**
  - Manual testing or review processes are established or updated.

- **External**
  - External vulnerability reports and disclosures are handled on a case-by-case basis.

- **Prioritization**
  - Prioritization also includes analysis of other shared, collaborative, and contextual data repositories or data exist within confidence scores.

- **Analyse**
  - Data are also identified, grouped, and/or filtered by location or region. This may require more detailed analysis and customization or ongoing maintenance.

- **Metrics & Reporting**
  - Custom reporting is available as a service or sub-service option, or feedback is typically solicited but responses are updated to higher-level root cause impediments, or via self-service options, or feedback is regularly solicited and reports are updated to higher-level root cause impediments.

- **Communicate**
  - Visibility and both timing and detail of response to alerts is measured and tracked.

- **Treat**
  - Deviations from configuration requirements and associated service impacts are measured and tracked.

**LEVEI 3** Defined

- **Policy & Standards**
  - Policy and standards are carefully documented in specific instances with minimal open and integrated security frameworks and are updated as needed.

- **Context**
  - The central repository requires that certain contextual information and applications are defined and followed for certain departments or the organization.

- **Automated**
  - Scanning coverage is measured and includes the measurement of automated response to alerts for common vulnerabilities.

- **Manual**
  - Scanning coverage is measured and includes the measurement of automated response to alerts for common vulnerabilities.

- **Prioritization**
  - Scanning coverage is measured and includes the measurement of automated response to alerts for common vulnerabilities.

- **Analyse**
  - Data from patch management activities, security incidents, and threat intelligence are used to size reporting timelines and to identify vulnerabilities.

- **Metrics & Reporting**
  - Data from patch management activities, security incidents, and threat intelligence are used to size reporting timelines and to identify vulnerabilities.

- **Communicate**
  - Deviations from configuration requirements and associated service impacts are measured and tracked.

- **Treat**
  - Data from the configuration process along with security incidents and threat intelligence are used to size reporting timelines and to identify vulnerabilities.

**LEVEI 4** Quantitatively Optimizing

- **Policy & Standards**
  - Policies and standards are carefully documented in specific instances with minimal open and integrated security frameworks and are updated as needed.

- **Context**
  - The central repository requires that certain contextual information and applications are defined and followed for certain departments or the organization.

- **Automated**
  - Automated, proactive control enforcement policy and requirements is defined and followed for certain departments or the organization.

- **Manual**
  - Automated or technology-assisted processes are developed or updated based on previous measurements.

- **Prioritization**
  - Automated or technology-assisted processes are developed or updated based on previous measurements.

- **Analyse**
  - Automated or technology-assisted processes are developed or updated based on previous measurements.

- **Metrics & Reporting**
  - Automated or technology-assisted processes are developed or updated based on previous measurements.

- **Communicate**
  - Automated or technology-assisted processes are developed or updated based on previous measurements.

- **Treat**
  - Automated or technology-assisted processes are developed or updated based on previous measurements.