Im Laufe des Lebenszyklus von industriellen Komponenten können Schwachstellen in der Software auftreten. Die Informationen dazu wie auch die dazugehörigen Informationen zum Beheben von Schwachstellen in Form der Sicherheitshinweise (Security Advisories) werden von den Komponentenherstellern zur Verfügung gestellt. Dies geschieht traditionell über individuelle Beschreibungen durch die Komponentenhersteller in PDF-Dokumenten oder über neue Standards wie z.B. dem Common Security Advisory Framework (CSAF). Dabei ist oft kein eindeutiges Mapping der Schwachstellen und Sicherheitshinweisen mit den im Unternehmen verwendeten Komponenten gegeben. Folglich müssen die Schwachstellen und Sicherheitshinweise der Hersteller manuell mit viel Aufwand mit den im Unternehmen vorhandenen Komponenten abgeglichen werden. Zum einen gibt es Unterschiede bei der Benennung, zum anderen setzt dies ein umfassendes Asset Inventar mit detaillierten Komponenteninformationen voraus, welches jedoch oft nicht in dem gewünschten Umfang vorhanden ist.

Ziel des Teilmodells **"Vulnerability Management"** ist es, eine eindeutige Zuordnung zwischen Schwachstellen, Sicherheitshinweisen und verwendeten Komponenten der Industrieanlagen herzustellen. Dabei kann unter Vermeidung von Doppelstrukturen auf dem CSAF-Standard aufgebaut werden. Das Teilmodell soll beispielsweise die Metainformation, die einheitliche Datenstruktur und die Informationen über die von den Komponentenherstellern spezifizierten Schwachstellen und Sicherheitshinweise enthalten.

Hinweis: Die Schwachstellenbewertung folgt dem CVSS-Standard und verweiset auf die entsprechenden Einträge in den öffentlichen Registern, wie National Vulnerability Database und VDE CERT. Die Sicherheitshinweise werden in der Regeln im offenen JSON-basiertem CSAF-Format erstellt. Die existierenden Referenzen zum Informationsaustausch von Schwachstellen und Sicherheitshinweisen sollen berücksichtigt werden, wie z.B. Common Security Advisory Framework.

Das Teilmodell **"Vulnerability Management"** hat einen breiten Anwendungsbereich, insbesondere ermöglicht es die ressourcensparende Identifikation und die eindeutige, maschinenlesbare Beschreibung von sicherheitsrelevanten Schwachstellen sowie den entsprechenden Gegenmaßnahmen für Industrieanlagen. Folglich kann die IT-Sicherheit deutlich erhöht werden.