# Die 15 Best Practices für ein gutes Security Advisory im CASF-Format

Ein Security Advisory im CSAF-Format soll mit seinem guten Format und seiner Verständlichkeit eine gute Informationsquelle sein, um den Sachverhalt klar darzustellen und möglichst wenige Fragen aufkommen zu lassen. Um dieses Ziel zu erreichen sollten die folgenden Regeln berücksichtigt werden (Die nachfolgenden Regeln beziehen sich auf das Security Advisory, für das Sie bitte das *csaf\_security\_advisory* Profil benutzen sollten).

## Regeln, die den Unterbereich *document* eines CSAF-Dokuments betreffen

1. Für die Eigenschaft *tlp* sollte der TLP-Wert auf *WHITE* gesetzt werden, um keine Einschränkungen bei der Verteilung des Advisories zu haben (*/document/distribution/tlp/label*).
2. Die Zusammenfassung eines *revision\_history* Eintrags sollte dazu dienen, kurz, klar und gut lesbar zu beschreiben, was sich gegenüber der vorherigen Revision geändert hat. Dies ermöglicht eine schnelle Entscheidung, ob eine neue Revision von Bedeutung ist oder nicht (*/document/tracking/revision\_history[]/summary*).
3. Die Nutzung von Dokuemnten-IDs sollte innerhalb einer Organisation einheitlich sein. Die Dokument-ID wird zur Bildung des Dateinamens und zur eindeutigen Identifizierung des Dokuments verwendet (*/document/tracking/id*). Zusammen mit dem namespacedes Herausgebers kann ein Dokument dadurch global eindeutig identifiziert werden*.*
4. Der Dateiname muss den im CSAF-Standard definierten Regeln entsprechen ([Kapitel 5.1](https://docs.oasis-open.org/csaf/csaf/v2.0/cs02/csaf-v2.0-cs02.html#51-filename)).
5. Die kanonische URL in */document/references* ermöglicht es, automatisch die neueste Version eines CSAF-Dokuments abzurufen.
6. Die Informationen an Hand derer der Herausgeber eines CSAF-Dokuments identifiziert werden kann, sollten während des Lebenszyklus eines Dokuments nicht geändert werden. Ausnahmen sind wichtige Ereignisse wie z.B. die Änderung eines Firmennamens (*/document/publisher*).

## Regeln, die den Unterbereich *product\_tree* eines CSAF-Dokuments betreffen

1. Geben Sie so genaue und detaillierte Produktinformationen wie möglich an, indem Sie */product\_tree/branches*, einschließlich der *category*, *vendor*, *product\_name* und *product\_version* befüllen.
2. Die Produktversionen sollten nach Möglichkeit unter Verwendung von *product\_version* einzeln aufgezählt werden, da der Abgleich von Produkten aus einer Bestandsdatenbank oder SBOM mit einem *product\_version\_range*-Element komplex, nicht deterministisch oder fehleranfällig sein kann. Wenn die ausstellende Partei nicht über genügend Informationen verfügt, um die Produkte nach Version aufzulisten, ist die Verwendung eines *product\_version\_range*-Elements akzeptabel.
3. Stellen Sie detaillierte Informationen zur Verfügung, die es dem Benutzer/Kunden ermöglichen, ein verwendetes Produkt richtig zu identifizieren. Verwenden Sie die *product\_identification\_helper* um diese Informationen zu vermitteln *(/product\_tree/\*/product/product\_identification\_helper*).
4. Die Trennung von Hard- und Software (Firmware) kann hilfreich sein. Verdeutlichen Sie, wie das Produkt selbst und die installierte Softwareversion, die derzeit von dem Produkt verwendet wird, identifiziert werden können. Verwenden Sie *relationship* Objekten, um diese Informationen zu vermitteln.

## Regeln, die den Unterbereich *vulnerabilities* eines CSAF-Dokuments betreffen

1. Machen Sie deutlich, welche Produkte betroffen sind und welche nicht (*fixed* oder *not\_affected*) (*/vulnerabilities[]/product\_status*). Wenn Sie "nicht betroffene" Produkte auflisten, sollten Sie das Profil CSAF VEX verwenden. Es wird jedoch empfohlen, im Detailfeld von */vulnerabilities[]/threats* zumindest eine kurze Erklärung abzugeben, warum das Produkt nicht betroffen ist.
2. Tragen Sie CVSS V3.1 Bewertungen ein (*/vulnerabilities[]/scores[]*).
3. Tragen Sie eine CVE Tracking Nummer ein (*/vulnerabilities[]/cve*).
4. Stellen Sie ausreichende Informationen zu den Möglichkeiten der Schadensbegrenzung in */vulnerabilities[]/remediations* bereit. Verwenden Sie z. B. *no\_fix\_planned*, wenn ein Produkt am Ende seiner Lebensdauer ist, und *none\_available*, wenn die Behebung derzeit in Entwicklung ist.
5. Eine Schwachstelle sollte mindestens eine kurze Beschreibung haben, die als Zusammenfassung genutzt werden kann (*vulnerabilities[]/notes*). Dies kann die CVE-Beschreibung (mit Titel *CVE description* und Kategorie *description*) oder eine Zusammenfassung der Schwachstelle (mit Titel *Vulnerability summary* und Kategorie *summary*) sein.