敏感数据检测

以下主题介绍敏感数据检测及其配置方式：

敏感数据检测基础知识

敏感数据（如社会保障号码、信用卡号码、驾驶证号码等）可能会被有意或无意地在互联网上泄露。系统提供了一种敏感数据预处理器，可在 ASCII 文本中检测和生成关于敏感数据的事件，这在检测意外数据泄露时特别有用。

全局敏感数据检测选项用于控制预处理器的工作方式。可以修改指定以下内容的全局选项：

- 预处理器是否在触发数据包中替换信用卡号或社会保障号的最后四位数
- 网络上的哪些目标主机监控敏感数据
- 单个会话中所有数据类型总共出现多少次会产生事件

具体数据类型确定了在指定目标网络流量中可以针对其进行检测并生成事件的敏感数据。可以为指定以下内容的数据类型选项修改默认设置：

- 某种检测到的数据类型必须达到才能生成单个会话事件的阈值
- 每种数据类型要监控的目标端口

- 每种数据类型要监控的应用协议

可以创建和修改自定义数据类型以检测指定的数据模式。例如，医院可以创建一种数据类型来保护患者编号；再如，大学可以创建一种数据类型来检测具有唯一编号模式的学号。

系统通过将各个数据类型与流量进行比对来检测每个 TCP 会话中的敏感数据。可以为每种数据类型和适用于入侵策略中所有数据类型的全局选项修改默认设置。Firepower 系统提供了常用的预定义数据类型。您也可以创建自定义数据类型。

敏感数据预处理器规则与每种数据类型关联。可通过为数据类型启用相应的预处理器，为每种数据类型启用敏感数据检测和事件生成。配置页面上的链接会将您指向“规则”(Rules) 页面上的敏感数据规则的过滤视图，可以在其中启用和禁用规则以及配置其他规则属性。

保存对入侵策略所做的更改时，如果与数据类型相关的规则已启用且敏感数据检测已禁用，可以选择自动启用敏感数据预处理器。

提示 敏感数据预处理器可以检测使用 FTP 或 HTTP 上传和下载的未加密 Microsoft Word 文件中的敏感数据；之所以可以这样，大概是因为 Word 文件单独分组 ASCII 文本和格式命令的方式。

系统不会检测经过加密的或模糊的敏感数据，也不会检测压缩或编码格式（例如 Base64 编码邮件附件）的敏感数据。例如，系统会检测电话号码 (555)123-4567，但不会检测该号码经过模糊处理的版本，即，每个数字用空格分开，例如 (5 5 5) 1 2 3 - 4 5 6 7，或者通过 HTML 代码介入，例如 (555)-123-4567。但是，系统会检测采用 HTML 代码的号码 (555)-123-4567，在该号码中，没有介入代码中断编号模式。

全局敏感数据检测选项

全局敏感数据选项是特定于策略的并适用于所有数据类型。

掩码

在触发数据包中用 X 替换信用卡号或社会保障号的最后四位数。掩码数字显示在 Web 界面中的入侵事件数据包视图中和下载的数据包中。

网络

指定监控敏感数据的目标主机。可以指定单个 IP 地址、地址块或者 IP 地址和/或地址块的逗号分隔列表。系统会将空白字段解读为任意 (any)，意指任何目标 IP 地址。

全局阈值

指定在生成全局阈值事件之前，预处理器必须在任何组合中检测的单个会话中所有数据类型出现的总次数。可以指定 1 至 65535 之间的数字。

思科建议将此选项的值设置为大于在策略中启用的任何单个数据类型的最高阈值。

关于全局阈值，请注意：

- 必须启用预处理器规则 139:1 才能检测并生成事件并在内联部署中丢弃攻击性数据包关于数据类型出现次数的事件。
- 在每个会话中，预处理器最多生成一个全局阈值事件。
- 全局阈值事件与具体数据类型事件无关；也就是说，预处理器会在达到全局阈值时生成事件，而不管任何具体数据类型的事件阈值是否达到，反之亦然。

单个敏感数据类型选项

每种自定义数据类型至少必须指定一个事件阈值和至少一个要监控的端口或应用协议。

每种系统提供的预定义数据类型使用一种其他方法无法访问的 `sd_pattern` 关键字来定义用于在流量中进行检测的内置数据模式。您还可以创建自定义数据类型，然后可以使用简单的正则表达式为这些数据类型指定自己的数据模式。

敏感数据类型显示在“敏感数据检测”(Sensitive Data Detection) 功能已启用的所有入侵策略中。系统提供的数据类型显示为只读。对于自定义数据类型，名称和模式字段显示为只读，但是可以将其他选项设置为策略特定的值。

表 *1:* 单个数据类型选项

选项	说明
数据类型	指定数据类型的唯一名称。
阈值	指定系统生成事件时数据类型出现的次数。可以指定 1 至 255 之间的数字。 请注意，在每个会话中，预处理器为检测到的数据类型生成一个事件。另请注意，全局阈值事件与具体数据类型事件无关；也就是说，预处理器会在达到数据类型事件阈值时生成事件，而不管全局事件阈值是否达到，反之亦然。
目标端口 (Destination Ports)	为数据类型指定要监控的目标端口。可以指定单个端口、端口的逗号分隔列表或 `any`（表示任何目标端口）。
应用协议	最多可以为数据类型指定八个要监控的应用协议。必须激活应用检测器来识别要监控的应用协议。 请注意，对于典型设备，此功能需要控制许可证。
模式	指定要检测的模式。此字段仅为自定义数据类型提供。

相关主题

激活和停用检测器

系统提供的敏感数据类型

每个入侵策略包括用于检测常用数据模式的系统提供的数据类型，例如，信用卡号、邮箱地址、美国电话号码以及带有和不带破折号的美国社会保障号。

每种系统提供的数据类型都与一个生成器 ID (GID) 为 138 的敏感数据预处理器规则相关联。必须启用入侵策略中的关联敏感数据规则才能为要用于策略中的每种数据类型生成事件并在内联部署中丢弃攻击性数据包。

下表介绍每个数据类型并列出了相应的预处理器规则

表 *2:* 系统提供的敏感数据类型

数据类型	说明	预处理器规则
信用卡号	匹配 15 位和 16 位数字的 Visa®、MasterCard®、Discover® 和 American Express® 信用卡号（无论是否带正常分隔破折号或空格）；也可以使用 Luhn 算法来验证信用卡校验位。	138:2
邮箱地址	匹配邮箱地址。	138:5
美国电话号码	匹配符合 `(\d{3}) ?\d{3}-\d{4}` 模式的美国电话号码。	138:6
不带破折号的美国社会保障号	匹配包含有效的 3 位数区域号码、有效的 2 位数群组号码且不带破折号的 9 位数美国社会保障号。	138:4
带破折号的美国社会保障号	匹配包含有效的 3 位数区域号码、有效的 2 位数群组号码且带破折号的 9 位数美国社会保障号。	138:3

为了减少对社会保障号以外的 9 位数号码的误报，预处理器使用一种算法来验证 3 位数区域号码和 2 位数群组号码；在每个社会保障号中，这两组号码位于 4 位数序列号的前面。预处理器可验证 2009 年 11 月之前的社会保障号中的群组号码。

敏感数据检测的许可证要求

威胁防御 许可证

IPS

敏感数据检测的要求和前提条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员

配置敏感数据检测

由于敏感数据检测可能会对系统的性能产生重大影响，思科建议遵循以下准则：

- 选择“无活动规则”(No Rules Active) 默认策略作为基本入侵策略。
- 确保在相应的网络分析策略中已启用以下设置：
  - **应用层预处理器 (Application Layer Preprocessors)** 下的 **FTP 和 Telnet 配置 (FTP and Telnet Configuration)**。
  - **Transport/Network Layer Preprocessors** 下的 **IP Defragmentation** 和 **TCP Stream Configuration**。

开始之前

对于典型设备，此程序需要 保护 或 控制 许可证。

过程

步骤 1 选择 **策略 > 访问控制标题 > 入侵**

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图** ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 如果**特定威胁检测 (Specific Threat Detection)** 下的**敏感数据检测 (Sensitive Data Detection)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**敏感数据检测 (Sensitive Data Detection)** 旁边的 **编辑** ( )。

步骤 6 有以下选项可供选择：

- 修改全局设置，如全局敏感数据检测选项，第 2 页中所述。
- 在**目标 (Targets)** 部分中选择数据类型，然后修改数据类型配置，如单个敏感数据类型选项，第 3 页中所述。
- 如果要检查自定义敏感数据，请创建自定义数据类型；请参阅自定义敏感数据类型，第 8 页。

步骤 7 为数据类型添加或删除要监控的应用协议；请参阅受监控应用协议和敏感数据，第 6 页。

注释
要检测 FTP 流量中的敏感数据，请执行以下操作：

- 确保为访问控制策略启用了文件策略。
- 您必须添加 `Ftp 数据` 应用协议。

步骤 8 或者，要显示敏感数据预处理器规则，请点击**配置敏感数据检测的规则 (Configure Rules for Sensitive Data Detection)**。

可以启用或禁用所列的任何规则。还可以为 Rules 页面上可用的任何其他操作（例如规则抑制、基于速率的攻击防御，等等）配置敏感数据规则；有关详细信息，请参阅入侵规则类型。

步骤 9 要保存自上次策略提交以来在此策略中进行的更改，请点击导航面板中的**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在策略中启用敏感数据预处理器规则而未启用敏感数据检测，在保存策略更改时，系统会提示启用敏感数据检测。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 如果要生成入侵事件，请启用敏感数据检测规则 138:2、138:3、138:4、138:5、138:6、138:>999999 或 139:1。有关详细信息，请参阅入侵规则状态、全局敏感数据检测选项，第 2 页、系统提供的敏感数据类型，第 4 页和自定义敏感数据类型，第 8 页。
- 部署配置更改；请参阅 部署配置更改。

相关主题

特殊情况：FTP 流量中的敏感数据检测，第 8 页

受监控应用协议和敏感数据

最多可以为每种数据类型指定八个应用协议进行监控。必须为选择的每个应用协议至少启用一个检测器。默认情况下，系统提供的所有检测器均已激活。如果没有为应用协议启用检测器，则系统会为该应用自动启用所有系统提供的检测器；如果不存在检测器，则系统为该应用启用最新修改的用户定义的检测器。

必须为每种数据类型至少指定一个要监控的应用协议或端口。但是，除了要检测 FTP 流量中的敏感数据的情况之外，思科建议在指定应用协议时指定相应的端口，以便实现最全面覆盖。例如，如果指定 HTTP，还可以配置通用的 HTTP 端口 80。如果网络上的新主机实施 HTTP，系统会在其发现新 HTTP 应用协议的时间间隔内监控端口 80。

如果要检测 FTP 流量中的敏感数据，必须指定 `FTP data` 应用协议；在这种情况下，指定端口号没什么好处。

相关主题

激活和停用检测器

特殊情况：FTP 流量中的敏感数据检测 ，第 8 页

选择要监控的应用协议

可以指定要在系统提供的和自定义的敏感数据类型中监控的应用协议。选择的应用协议为策略特定的。

开始之前

对于典型设备，此程序需要 控制 许可证。

过程

步骤 1 选择**策略** > **访问控制标题** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图** ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 如果**特定威胁检测 (Specific Threat Detection)** 下的**敏感数据检测 (Sensitive Data Detection)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**敏感数据检测 (Sensitive Data Detection)** 旁边的 **编辑** ( )。

步骤 6 点击**数据类型 (Data Types)** 下的数据类型名称。

步骤 7 点击**应用协议 (Application Protocol)** 字段旁边的 **编辑** ( )。

步骤 8 有以下选项可供选择：

- 要添加用于监控的应用协议，请从**可用 (Available)** 列表中选择一个或多个应用协议，然后点击右箭头 (>)。最多可以添加八个应用协议用于监控。
- 要删除进行监控的应用协议，请从**已启用 (Enabled)** 列表中选择，然后点击左箭头 (<)。

步骤 9 点击**确定 (OK)**。

步骤 10 要保存自上次策略提交以来在此策略中进行的更改，请点击导航窗格中的**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

相关主题

特殊情况：FTP 流量中的敏感数据检测 ，第 8 页

特殊情况：FTP 流量中的敏感数据检测

通常，可通过指定要监控的端口或在部署中指定应用协议来确定要监控敏感数据的流量。

但是，对于检测 FTP 流量中的敏感数据来说，指定端口或应用协议并不足够。在 FTP 应用协议的流量中找到 FTP 流量中的敏感数据，这种情况间歇出现并使用临时端口号，因此难以检测。要检测 FTP 流量中的敏感数据，**必须**在配置中包括以下几项：

- 指定 `FTP 数据 (FTP data)` 应用协议以启用 FTP 流量中的敏感数据检测。

  对于检测 FTP 流量中的敏感数据这种特殊情况，指定 `FTP data` 应用协议不会调用检测功能；而是会调用 FTP/Telnet 预处理器的快速处理功能来检测 FTP 流量中的敏感数据。

- 确保 FTP Data 检测器已启用（默认情况下已启用）。
- 确保配置包括至少一个要监控敏感数据的端口。
- 确保为访问控制策略启用了文件策略。

请注意，不需要指定 FTP 端口（只要检测 FTP 流量中的敏感数据这种罕见情况除外）。大多数敏感数据配置将包括其他端口（例如 HTTP 或邮件端口）。如果只要指定一个 FTP 端口进行监控，思科建议指定 FTP 命令端口 `23`。

相关主题

FTP/Telnet 解码器
激活和停用检测器
配置敏感数据检测 ，第 5 页

自定义敏感数据类型

创建的每种自定义数据类型还会创建一个敏感数据预处理器规则，该规则的生成器 ID (GID) 为 138，Snort ID (SID) 为大于或等于 1000000（也就是本地规则的 SID）。

必须启用关联的敏感数据规则才能为要用于策略中的每种自定义数据类型启用检测、生成事件并在内联部署中丢弃攻击性数据包。

为了帮助启用敏感数据规则，配置页面上的链接会将您指向入侵策略“规则”(Rules) 页面的过滤视图，其中显示所有系统提供和自定义的敏感数据规则。您还可以通过在入侵策略“规则”(Rules) 页面上选择本地过滤类别，使自定义敏感数据规则与任何自定义本地规则一起显示。请注意，自定义敏感数据规则不会列于入侵规则编辑器页面（**对象** > **入侵规则**）。

创建自定义数据类型后，您可以在系统中的任何入侵策略中启用该自定义数据类型。要启用自定义数据类型，必须在要用于检测该自定义数据类型事件的任何策略中启用关联敏感数据规则。

自定义敏感数据类型中的数据模式

可使用一组由以下部分组成的简单正则表达式来定义自定义数据类型的数据模式：

- 三个元字符
- 允许将元字符用作原义字符的转义字符
- 六个字符类

元字符是在正则表达式中具有特殊含义的原义字符。

表 *3:* 敏感数据模式元字符

元字符	说明	示例
?	匹配前面的字符或转义序列零次或一次；也就是说，前面的字符或转义序列是可选的。	`Colou?r` 匹配 `color` 或 `colour`
{n}	匹配前面的字符或转义序列 n 次。	例如，`\d{2}` 匹配 `55`、`12` 等；`\l{3}` 匹配 `AbC`、`www` 等；`\w{3}` 匹配 `a1B`、25C 等；`x{5}` 匹配 `xxxxx`
\	元字符可用作实际字符，还可用于指定预定义的字符类。	`\?` 匹配问号，`\\` 匹配反斜杠，`\d` 匹配数字字符等

必须将反斜杠用于转义某些字符，这样敏感数据预处理器才能将它们正确解释为原义字符。

表 *4:* 转义敏感数据模式字符

使用的转义字符...	代表的原义字符...
\?	?
\{	{
\}	}
\\	\

在定义自定义敏感数据模式时，可以使用字符类。

表 *5:* 敏感数据模式字符类

字符类	说明	字符类定义
\d	匹配任何 ASCII 数字字符 0-9	0-9

字符类	说明	字符类定义
\D	匹配不是 ASCII 数字字符的任何字节	不是 0-9
\l（小写“ell”）	匹配任何 ASCII 字母	a-zA-Z
\L	匹配不是 ASCII 字母的任何字节	不是 a-zA-Z
\w	匹配任何 ASCII 字母数字字符 请注意，与 PCRE 正则表达式不同，此项不包括下划线 (_)。	a-zA-Z0-9
\W	匹配不是 ASCII 字母数字字符的任何字节	不是 a-zA-Z0-9

预处理器将直接输入（而不是作为正则表达式的一部分输入）的字符视为原义字符。例如，数据模式 1234 匹配 `1234`。

以下数据模式示例（用于系统提供的敏感数据规则 138:4）使用转义的数字字符类、乘数和选项说明符元字符、文字破折号 (-) 和左右括号 () 字符来检测美国电话号码：

```
(\d{3}) ?\d{3}-\d{4}
```

创建自定义数据模式时务必谨慎。考虑将下列备选数据模式用于检测电话号码，尽管使用的是有效语法，但可能会导致许多误报：

```
(?\d{3})? ?\d{3}-?\d{4}
```

由于第二个示例结合了可选括号、可选空格和可选破折号，它会在下列所需模式中检测电话号码及其他方面：

- `(555)123-4567`
- `555123-4567`
- `5551234567`

但是，除此之外，第二个示例模式还会检测以下可能无效的模式及其他方面，从而造成误报：

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

最后举一个极端的例子（仅作说明用途）：创建一种数据模式，用以在小型企业网络上的所有目标流量中使用一个低事件阈值来检测小写字母 `a`。这种数据模式可能在短短几分钟内生成数百万的事件，令系统不堪重负。

配置自定义敏感数据类型

如果在任何入侵策略中启用某个数据类型的敏感数据规则，则不能删除该数据类型。

过程

步骤 1 选择 **策略** > **访问控制标题** > **入侵**

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图** ()，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 如果**特定威胁检测 (Specific Threat Detection)** 下的**敏感数据检测 (Sensitive Data Detection)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**敏感数据检测 (Sensitive Data Detection)** 旁边的 **编辑** ()。

步骤 6 点击**数据类型 (Data Types)** 旁边的 **添加** ()。

步骤 7 输入数据类型的名称。

步骤 8 输入要使用此数据类型检测的模式；请参阅自定义敏感数据类型中的数据模式，第 9 页。

步骤 9 点击**确定 (OK)**。

步骤 10 或者，点击数据类型名称，并修改单个敏感数据类型选项，第 3 页中所述的选项。

步骤 11 或者，通过点击 **删除** () 删除自定义数据类型，然后点击**确定 (OK)** 以确认。

注释
如果在任何入侵规则中启用该数据类型的敏感数据规则，则系统会发出警告，表明不能删除该数据类型。再次尝试删除之前，必须禁用受影响策略中的敏感数据规则；请参阅设置入侵规则状态。

步骤 12 要保存自上次策略提交以来在此策略中进行的更改，请点击导航面板中的**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 在要使用该数据类型的每个策略中启用关联的自定义敏感数据预处理规则；请参阅设置入侵规则状态。
- 部署配置更改；请参阅部署配置更改。

相关主题

编辑自定义敏感数据类型，第 12 页

编辑自定义敏感数据类型

您可以编辑自定义敏感数据类型中的所有字段。但请注意，当修改名称或模式字段时，这些设置在系统上的所有入侵策略中都会更改。可以将其他选项设置为策略特定值。

过程

步骤 1 选择 **策略** > **访问控制标题** > **入侵**

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

如果显示**视图** ( )，则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 点击导航面板中的**高级设置 (Advanced Settings)**。

步骤 4 如果**特定威胁检测 (Specific Threat Detection)** 下的**敏感数据检测 (Sensitive Data Detection)** 已禁用，请点击**已启用 (Enabled)**。

步骤 5 点击**敏感数据检测 (Sensitive Data Detection)** 旁边的**编辑 (Edit)**。

步骤 6 在**目标 (Targets)** 部分中，点击自定义数据类型的名称。

步骤 7 点击**编辑数据类型名称和模式 (Edit Data Type Name and Pattern)**。

步骤 8 修改数据类型名称和模式；请参阅自定义敏感数据类型中的数据模式，第 9 页。

步骤 9 点击**确定 (OK)**。

步骤 10 将其余选项设置为策略特定值；请参阅单个敏感数据类型选项，第 3 页。

步骤 11 要保存自上次策略提交以来在此策略中进行的更改，请点击导航面板中的**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改；请参阅部署配置更改。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。