Red Hat Insights 1-latest

在 RHEL 系统上评估和报告 Malware 签名

了解 RHEL 基础架构中的系统何时暴露给恶意软件风险

Last Updated: 2024-06-28

Red Hat Insights 1-latest 在 RHEL 系统上评估和报告 Malware 签名

了解 RHEL 基础架构中的系统何时暴露给恶意软件风险

法律通告

摘要

将 Insights for Red Hat Enterprise Linux malware 检测服务与 IBM X-Force 威胁智能签名一起使用，以了解您基础架构中的系统何时是恶意软件攻击的影响。 红帽承诺替换我们的代码、文档和网页属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于此项工作十分艰巨，这些更改将在即将推出的几个发行版本中逐步实施。详情请查看 CTO Chris Wright 信息。

目录

第 1 章 INSIGHTS FOR RHEL MALWARE 检测服务概述

Red Hat Insights for Red Hat Enterprise Linux malware 检测服务是一个监控和评估工具，用于扫描 RHEL 系统是否存在恶意软件。恶意软件检测服务融合了 YARA 模式匹配软件和恶意软件检测签名。为与 IBM X-Force 威胁智能团队合作提供签名，与红帽威胁智能团队紧密合作。

在恶意软件检测服务 UI 中，User Access-authorized 管理员和 viewers 可以

- 请参阅其 RHEL 系统被扫描的签名列表。
- 请参阅 Insights 客户端中启用了 malware 检测的所有 RHEL 系统的汇总结果。
- 查看各个系统的结果。
- 知道系统何时显示恶意软件存在的证据。

这些功能为安全威胁评估者和 IT 事件响应团队提供宝贵的信息，以准备响应。

恶意软件检测服务不推荐解析或修复恶意软件事件。

处理恶意软件威胁的策略取决于特定于每个系统和机构的很多标准和注意事项。您的组织的安全事件响应团队最适合为每个环境设计和实施有效缓解和补救策略。

1.1. YARA MALWARE 签名

YARA 签名检测是 Insights for Red Hat Enterprise Linux malware 检测服务的基础。YARA 签名是 malware 类型的描述，以模式表示。每个描述由一组字符串和一个定义规则的布尔值表达式组成。当扫描的 RHEL 系统中存在一个或多个条件时，YARA 记录了该系统上的命中。

1.2. IBM X-FORCE THREAT INTELLIGENCE 签名

Insights for Red Hat Enterprise Linux malware 检测服务包括 IBM X-Force Threat Intelligence 团队开发的预定义签名，以公开在 RHEL 系统上运行的恶意软件。X-Force 威胁智能团队编译的签名在 XFTI - 前缀（如 *XFTI_FritzFrog* ）中的 malware 检测服务中是可识别的。

第 2 章 使用 INSIGHTS FOR RHEL MALWARE 检测服务

要开始使用恶意软件检测服务，您必须执行以下操作。本章中每个操作的流程。

注意

有些流程需要系统上的 sudo 访问权限，而其他步骤要求管理员执行该操作是具有 **Malware 检测管理员角色** 的 User Access 组的成员。

表 2.1. 设置恶意软件检测服务的流程和访问要求。

操作	描述	所需的权限
安装 YARA 并配置 Insights 客户端	安装 YARA 应用程序并将 Insights 客户端配置为使用恶意软件检测服务	sudo 访问
在 Red Hat Hybrid Cloud Console 中配置用户访问权限	在 Red Hat Hybrid Cloud Console > **Settings** 图标(PROFILE)> Identity & Access Management > User Access > Groups 中，创建 malware 检测组，然后在组中添加适当的角色和成员	红帽帐户的机构管理员
查看结果	请参阅混合云控制台中的系统扫描结果	带有 Malware 检测查看器角色的用户访问组中的成员资格

2.1. 安装 YARA 并配置 INSIGHTS 客户端

执行以下步骤在 RHEL 系统上安装 YARA 和恶意软件检测控制器，然后运行测试和完整的恶意软件检测扫描，并将数据报告到 Insights for Red Hat Enterprise Linux 应用程序。

先决条件

- 系统操作系统版本必须是 RHEL8 或 RHEL9。
- 管理员必须具有系统的 sudo 访问权限。
- 系统必须安装 Insights 客户端软件包，并注册到 Insights for Red Hat Enterprise Linux。

流程

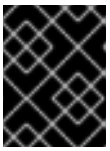
1. 安装 YARA。
   红帽客户门户网站上提供了适用于 RHEL8 和 RHEL9 的 YARA RPM：

```
$ sudo dnf install yara
```

注意

RHEL7 不支持 Insights for Red Hat Enterprise Linux malware 检测。

2. 如果还没有完成，请将系统注册到 Insights for Red Hat Enterprise Linux。



重要

必须在系统上安装 Insights 客户端软件包，并通过 Insights 为 Red Hat Enterprise Linux 注册的系统，然后才能使用恶意软件检测服务。

a. 安装 Insights 客户端 RPM。

```
$ sudo yum install insights-client
```

b. 测试与 Insights for Red Hat Enterprise Linux 的连接。

```
$ sudo insights-client --test-connection
```

c. 使用 Insights for Red Hat Enterprise Linux 注册系统。

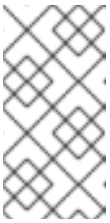
```
$ sudo insights-client --register
```

3. 运行 Insights 客户端恶意软件检测收集器。

```
$ sudo insights-client --collector malware-detection
```

收集器对此初始运行执行以下操作：

- 在 **/etc/insights-client/malware-detection-config.yml** 中创建一个恶意软件检测配置文件
- 执行测试扫描并上传结果



注意

这是使用简单测试规则对系统进行非常小的扫描。测试扫描主要是为了帮助验证安装、操作和上传是否在恶意软件检测服务正常工作。将会发现几个匹配项，但这意图且无需担心。初始测试扫描的结果不会出现在恶意软件检测服务 UI 中。

4. 执行完整的文件系统扫描。

a. 编辑 **/etc/insights-client/malware-detection-config.yml**，并将 **test_scan** 选项设置为 false。

```
test_scan: false
```

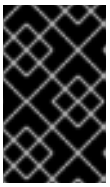
考虑设置以下选项以最小化扫描时间：

- **filesystem_scan_only** - 仅扫描系统上的某些目录
- **filesystem_scan_exclude** - 排除正在扫描的某些目录
- **filesystem_scan_since** - 仅扫描最近修改的文件

b. 重新运行客户端收集器：

```
$ sudo insights-client --collector malware-detection
```

5. （可选）扫描进程。这将首先扫描文件系统，然后扫描所有进程。在文件系统和进程扫描完成后，在 Security > Malware 中查看结果。



重要

默认情况下禁用扫描进程。在 Linux 系统上有 YARA 和扫描进程存在一个问题，这可能会产生不佳的系统性能。这个问题将在 YARA 即将推出的发行版本中解决，**但建议不要扫描进程**。

a. 要启用进程扫描，请在 **/etc/insights-client/malware-config.yml** 中设置 **scan_processes: true**。

```
scan_processes: true
```

注意

考虑在存在时设置这些与进程相关的选项： processes_scan_only - 只扫描系统上 processess_scan_exclude - 排除某些进程被扫描的 processes_scan_since - 只扫描最近启动的进程

a. 保存更改，然后再次运行收集器。

```
$ sudo insights-client --collector malware-detection
```

2.2. RED HAT HYBRID CLOUD 控制台中的用户访问设置

用户访问是红帽实施基于角色的访问控制(RBAC)。机构管理员使用 User Access 来配置用户在 Red Hat Hybrid Cloud Console （控制台）上可以看到和执行的操作：

- 通过组织角色而不是单独为用户分配权限来控制用户访问权限。
- 创建包含角色及其对应权限的组。
- 将用户分配给这些组，以便用户继承与其组角色关联的权限。

2.2.1. 预定义的用户访问组和角色

为了便于管理组和角色，红帽提供了两个预定义的组和一组预定义的角色。

2.2.1.1. 预定义的组

Default access 组包含 您机构中的所有用户。很多预定义角色被分配给此组。红帽会自动更新。

注意

如果机构管理员对 **Default access** 组进行了更改，则其名称会更改为 **Custom default access** 组，且不再由红帽更新。

Default admin access 组仅包含具有机构管理员权限的用户。这个组会自动维护，且无法更改此组中的用户和角色。

在 Hybrid Cloud Console 中，导航到 Red Hat Hybrid Cloud Console > **Settings** 图标(wagon)> Identity & Access Management > User Access > Groups 来查看您的帐户中的当前组。此视图仅限于机构管理员。

2.2.1.2. 分配给组的预定义角色

Default access 组包含许多预定义的角色。由于您机构中的所有用户都是 **Default access** 组的成员，因此它们会继承分配给该组的所有权限。

Default admin access 组包括许多（但不包括所有）提供更新和删除权限的预定义角色。此组中的角色通常会将 **管理员** 包含在其名称中。

在 Hybrid Cloud Console 中，导航到 Red Hat Hybrid Cloud Console > **Settings** 图标(wagon)> Identity & Access Management > User Access > Roles 以查看您的帐户中的当前角色。您可以查看每个角色分配到的组数量。此视图仅限于机构管理员。

如需更多信息，请参阅基于角色的访问控制(RBAC)的用户访问配置指南。

2.2.2. 访问权限

预定义角色提供您必须具有的权限的每个流程列表 **的先决条件**。作为用户，您可以进入 Red Hat Hybrid Cloud Console > **Settings** 图标(wagon)> My User Access 来查看当前继承的角色和应用程序权限。

如果您尝试访问 Insights for Red Hat Enterprise Linux 功能，并查看您没有执行此操作的消息，则必须获得额外的权限。您的机构的机构管理员或 User Access 管理员配置这些权限。

使用 Red Hat Hybrid Cloud Console Virtual Assistant 来询问"联系我的机构管理员"。该助手可代表您向机构管理员发送电子邮件。

2.2.3. Malware 检测服务的用户访问角色

Red Hat Hybrid Cloud Console 的以下预定义角色可以访问 Insights for Red Hat Enterprise Linux 中的 malware 检测功能：

重要

对于 malware 检测服务用户，没有 "default-group" 角色。要使用户能够查看恶意软件检测服务中的数据或控制设置，它们必须是具有以下角色之一的用户访问组的成员：

- **malware 检测查看器**
- **恶意软件检测管理员**

2.3. 在 RED HAT HYBRID CLOUD CONSOLE 中查看恶意软件检测扫描结果

查看混合云控制台上的系统扫描结果。

先决条件

- 在 RHEL 系统上安装并配置 YARA 和 Insights 客户端。
- 您必须登录 Hybrid Cloud Console。

- 您是 *Malware 检测管理员*或 *Malware 检测查看者*角色的成员。

流程

1. 进入 Security > Malware > Systems 。
2. 查看仪表板，以获得所有启用了恶意软件检测和报告结果的 RHEL 系统。
3. 要查看特定系统的结果，请使用 **Filter by name** 搜索系统。

第 3 章 其他恶意软件服务概念

以下附加信息在使用恶意软件检测服务时可能很有用。

3.1. 系统扫描

在本发行版本中，Malware 检测管理员必须根据需要启动 Insights for Red Hat Enterprise Linux malware 检测服务收集器扫描。或者，管理员也可以作为 playbook 运行 collector 命令，或使用其他自动化方法。

注意

推荐的扫描频率是您的安全团队；但是，扫描可能需要大量时间才能运行，因此 Red Hat Enterprise Linux 的 Insights 检测服务团队建议每周运行恶意软件检测扫描。

3.1.1. 启动恶意软件检测扫描

执行以下步骤来运行恶意软件检测扫描。扫描完成后，在 Insights for Red Hat Enterprise Linux malware 检测服务中报告数据。扫描时间取决于多个因素，包括配置选项、正在运行的进程数等。

先决条件

运行 Insights 客户端命令需要系统上的 sudo 访问权限。

流程

1. 运行 **$ sudo insights-client --collector malware-detection**。
2. 在 Security > Malware 中查看结果。

3.2. 禁用 MALWARE 签名

可能有一些不感兴趣的恶意软件签名。这可能是因为设计的配置、测试扫描或高问题问题（在恶意软件检测服务报告中报告不适用于您的安全优先级）。

例如，使用签名 **XFTI_EICAR_AV_Test** 和 **XFTI_WICAR_Javascript_Test** 来检测 EICAR Anti Malware Testfile 和 WICAR Javascript Crypto Miner test malware。它们是有意设计的测试签名，但不代表实际的恶意软件威胁。可以禁用这些签名，以便在 Red Hat Hybrid Cloud Console 中不会报告与它们匹配的签名。

禁用签名后，恶意软件检测服务会从混合云控制台中删除与该签名的现有匹配，并忽略以后扫描中的签名。如果重新启用了签名，则恶意软件检测服务会在将来的恶意软件检测扫描中再次查找签名，并显示生成的匹配项。

注意

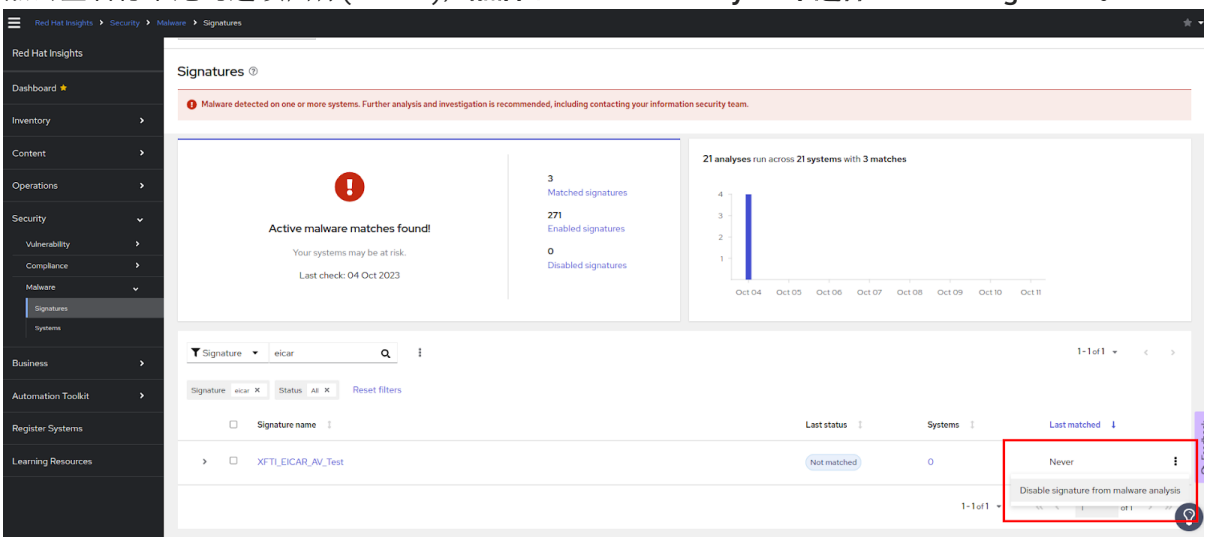
禁用签名不会清除之前与该签名匹配的历史记录。

先决条件

- 您是带有 **Malware 检测管理员角色** 的 Hybrid Cloud Console User Access 组的成员。只有具有此角色的用户才能禁用和重新启用签名。

禁用签名的步骤

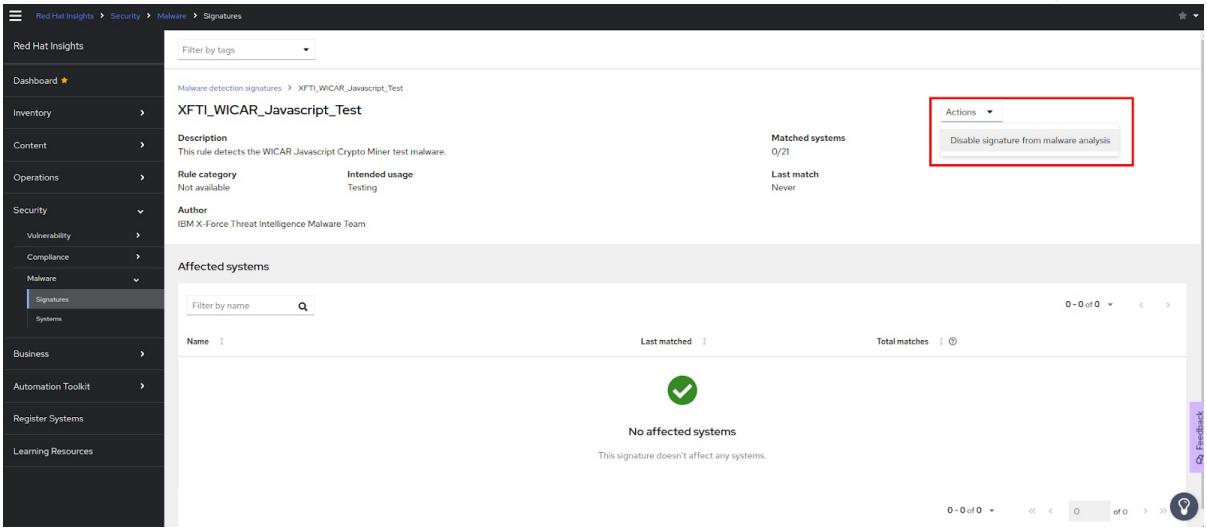
1. 进入 Security > Malware > Signatures 。
2. 找到要禁用的签名。
3. 点击签名行末尾的选项图标(HBAC)，**然后从 malware analysis 中选择 Disable signature**。



禁用签名的替代步骤

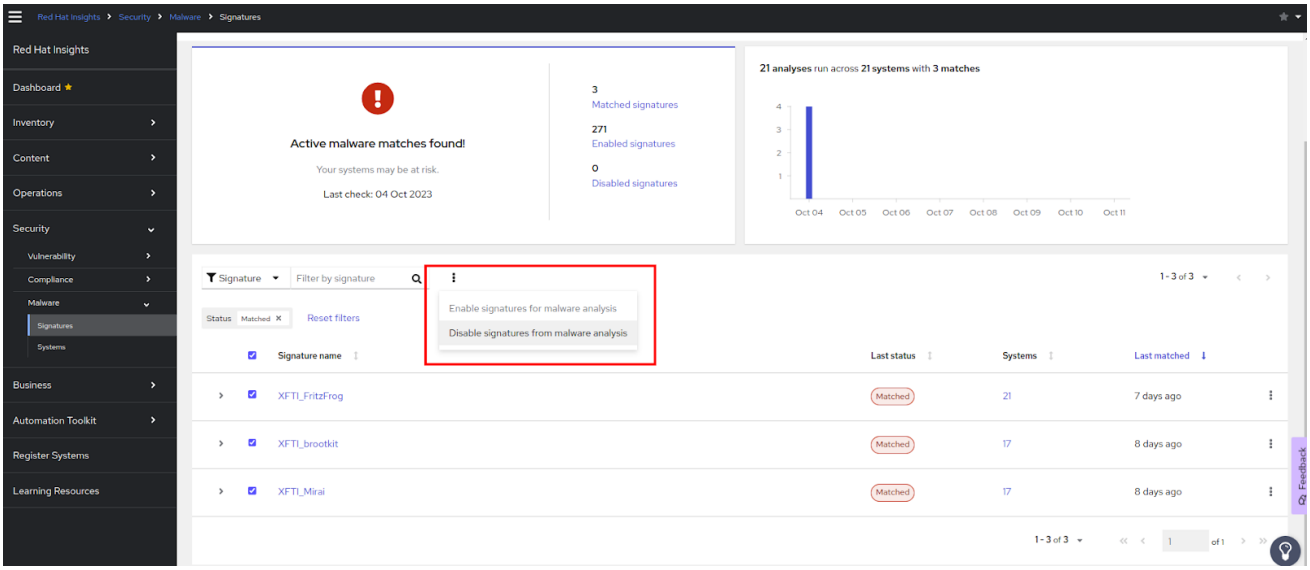
您还可以从签名信息页面禁用签名。

1. 进入 Security > Malware > Signatures 。
2. 找到要禁用的签名。
3. 点签名名称。
4. 在签名详情页面上，单击 **Actions** 下拉菜单，**然后从 malware 分析中选择 Disable signature**。



同时禁用多个签名

您可以通过选中每个签名行开头的框来禁用多个签名，然后点击过滤器字段旁的选项图标(RCU)，**并从 malware 分析中选择 Disable signatures**。



查看禁用的恶意软件签名

所有用户都可以查看禁用的恶意软件签名。

1. 进入 Security > Malware > Signatures。在页面顶部的仪表板中查看禁用 malware 签名的数量。
2. 设置过滤器以显示禁用的签名。
   a. 将主过滤器设置为 **包含在恶意软件分析中的签名**。
   b. 将 secondary 过滤器设置为 **Disabled 签名**。

重新启用恶意软件签名

按照与之前启用之前禁用的签名相同的步骤。

3.3. 解释恶意软件检测服务结果

在大多数情况下，使用 YARA 运行恶意软件检测扫描将导致没有签名匹配。这意味着，当将已知 malware 签名与扫描中包含的文件进行比较时，YARA 没有找到任何匹配的字符串或布尔值表达式。恶意软件检测服务会将这些结果发送到 Red Hat Insights，您可以看到系统扫描的详情，并缺少 Insights for Red Hat Enterprise Linux malware 检测服务 UI 中的匹配项。

如果使用 YARA 的恶意软件检测扫描检测到匹配项，它将发送与 Red Hat Insights 匹配的结果，您可以在恶意软件检测服务 UI 中看到匹配项的详细信息，包括文件和日期。最后 14 天会显示系统扫描和签名匹配历史记录，以便您可以检测模式并将这些信息提供给您的安全事件响应团队。例如，如果在一个扫描中找到签名匹配，但无法在同一系统的下一次扫描中找到，这可能表示仅在特定进程运行时可以检测到的恶意软件。

3.4. 恶意软件检测收集器的其他配置选项

/etc/insights-client/malware-detection-config.yml 文件包括几个配置选项。

配置选项

- **filesystem_scan_only**
  这基本上是一个允许列表选项，您可以在其中指定要扫描的文件/目录。仅扫描指定的项目。它可以是单个项目，也可以是项目列表（与 yaml 语法用于指定项目列表）的列表。如果此选项为空，本质上意味着扫描所有文件/目录（取决于其他选项）。

- **filesystem_scan_exclude**
  这基本上是一个 denylist 选项，其中您可以指定哪个文件/目录不扫描。许多目录已经列出，默认情况下将排除这些目录。这包括虚拟文件系统目录、例如 /proc、/sys、/cgroup、/cgroup、具有外部挂载的文件系统、如 /mnt 和 /media 的目录，以及建议不扫描的其他目录、eg /dev 和 /var/log/insights-client （以防止假的正客户端）。您可以自由修改列表来添加（或减）文件/目录。

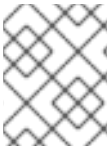
  请注意，如果在 filesystem_scan_only 和 filesystem_scan_exclude 中同时指定了同一项，如 /home，则 filesystem_scan_exclude 将为 'win'。也就是说，/home 将不会被扫描。另一个示例是 filesysem_scan_only 一个父目录，例如 /var，然后 filesystem_scan_exclude 在其中的特定目录，如 eg /var/lib 和 /var/log/insights-client。然后，/var 以外的 /var/lib 和 /var/log/insights-client 都会被扫描。

- **filesystem_scan_since**
  仅修改 'since' 的扫描文件，其中 since 可以是代表天前的整数，或者自上次文件系统扫描以来的"last"含义。例如，system_scan_since: 1 表示自 1 天前创建或修改过的文件（在最后一天之后），filesystem_scan_since: 7 意味着仅扫描自 7 天前创建/修改的文件（在上周内）；而 filesystem_scan_since：仅扫描自上次成功创建/修改后创建/修改的文件。

- **exclude_network_filesystem_mountpoints 和 network_filesystem_types**
  设置 **exclude_network_filesystem_mountpoints: true** 表示恶意软件检测收集器不会扫描挂载的网络文件系统的挂载点。这是默认设置，是为了防止扫描外部文件系统，从而造成不必要的和增加网络流量和速度较慢的扫描。它认为是网络文件系统的文件系统列在 **network_filesystem_types** 选项中。因此，该列表和挂载的任何文件系统类型都会被排除在扫描中。这些挂载点基本上添加到 **filesystem_scan_exclude** 选项中排除的目录列表中。如果设置了 **exclude_network_filesystem_mountpoints: false**，您仍然可以使用 **filesystem_scan_exclude** 选项排除挂载点。

- **network_filesystem_types**
  定义网络文件系统类型。

- **scan_processes**



注意

Scan_process 默认被禁用，以防止在扫描大量或大型进程时影响系统性能。当状态为 false 时，不会扫描任何进程，并忽略以下的 processes_scan 选项。

+ 在扫描中包含正在运行的进程。

- **processes_scan_only**
  这与 filesystem_scan_only 类似，但适用于进程。进程可以指定为单个 PID、eg 123 或 PID 范围、eg 1000.2000 或进程名称，如 Chrome。例如，以下值：123, 1000..2000, and Chrome 表示只扫描 PID 123、PID 从 1000 到 2000（包括这两个值）、以及包括字符串 'chrome' 的进程名称的 PID。

- **processes_scan_exclude**
  这与 filesystem_scan_exclude 类似，但适用于进程。与 processes_scan_only 一样，进程可以指定为单个 PID、PID 范围或进程名称。如果进程同时出现在 processes_scan_only 和 processes_scan_exclude 中，则 processes_scan_exclude 将为 'win'，该过程将被排除。

- **processes_scan_since**
  这与 filesystem_scan_since 类似，但适用于进程。只有已启动的"since"的扫描进程，其中因为 可以是代表天前的整数，或"last"表示自上次成功过程扫描以来。

环境变量

/etc/insights-client/malware-detection-config.yml 文件中的所有选项也可以使用环境变量设置。使用环境变量会覆盖配置文件中同一选项的值。环境变量的名称与配置文件选项的名称相同，但大写。例如，配置文件选项 **test_scan** 是环境变量 **TEST_SCAN**。

对于 **FILESYSTEM_SCAN_ONLY**, **FILESYSTEM_SCAN_EXCLUDE**, **PROCESSES_SCAN_ONLY**, **PROCESSES_SCAN_EXCLUDE**, 和 **NETWORK_FILESYSTEM_TYPES** 环境变量，使用以逗号分隔的列表。例如，要只扫描目录 **/etc**、**/tmp** 和 **/var/lib**，请使用以下环境变量：

```
FILESYSTEM_SCAN_ONLY=/etc,/tmp,/var/lib
```

要在命令行中指定它（以及禁用测试扫描），请使用：

```
$ sudo FILESYSTEM_SCAN_ONLY=/etc,/tmp,/var/lib TEST_SCAN=false insights-client --collector malware-detection
```

Resources

有关 Insights 客户端的更多信息，*请参阅 Red Hat Insights 的客户端配置指南*。

3.5. 为恶意软件事件启用通知和集成

当恶意软件服务检测到至少一次系统扫描并生成一个警报时，您可以在 Red Hat Hybrid Cloud Console 上启用通知服务来发送通知。使用通知服务可自由地检查 Red Hat Insights for Red Hat Enterprise Linux 仪表板 是否有警报。

例如，您可以将通知服务配置为在恶意软件服务检测到可能威胁到您的系统时自动发送电子邮件消息，或者发送恶意服务每天生成的所有警报的电子邮件摘要。

除了发送电子邮件信息外，您还可以将通知服务配置为以其他方式发送事件数据：

- 使用经过身份验证的客户端查询 Red Hat Insights API 获取事件数据
- 使用 Webhook 将事件发送到接受入站请求的第三方应用程序
- 将通知与 Splunk 等应用程序集成至应用程序仪表板

malware 服务通知包括以下信息：

- 受影响系统的名称
- 在系统扫描过程中找到多少个签名匹配
- 查看 Red Hat Hybrid Cloud Console 的详情的链接

启用通知服务需要三个主要步骤：

- 首先，机构管理员会创建一个具有 Notifications 管理员角色的用户访问权限组，然后将帐户成员添加到组中。
- 接下来，通知管理员为通知服务中的事件设置行为组。行为组指定每个通知的交付方法。例如，行为组可以指定电子邮件通知是否发送到所有用户，或者只向机构管理员发送。
- 最后，从事件接收电子邮件通知的用户必须设置其用户首选项，以便他们为每个事件接收单独的电子邮件。

其他资源

- 有关如何为恶意软件警报设置通知的更多信息，请参阅在 *Red Hat Hybrid Cloud Console 中配置通知*。

对红帽文档提供反馈

我们非常感谢并对我们文档的反馈进行优先排序。提供尽可能多的详细信息，以便快速解决您的请求。

先决条件

- 已登陆到红帽客户门户网站。

流程

要提供反馈，请执行以下步骤：

1. 点击以下链接： Create Issue
2. 在 **Summary** 文本框中描述问题或功能增强。
3. 在 **Description** 文本框中提供有关问题或请求的增强的详细信息。
4. 在 **Reporter** 文本框中键入您的名称。
5. 点 **Create** 按钮。

此操作会创建一个文档票据，并将其路由到适当的文档团队。感谢您花时间来提供反馈。