Red Hat Insights 2023

使用 Insights for RHEL Malware 服务评估和报告 RHEL 系统上的 Malware 签名

知道 RHEL 基础架构中系统暴露给恶意软件风险

Last Updated: 2023-05-13

Red Hat Insights 2023 使用 Insights for RHEL Malware 服务评估和报告 RHEL 系统上的 Malware 签名

知道 RHEL 基础架构中系统暴露给恶意软件风险

法律通告

摘要

使用 Insights for Red Hat Enterprise Linux malware-detection 服务及 IBM X-Force 威胁智能签名，以了解您的基础架构中的系统何时是恶意攻击的影响。 红帽致力于替换我们的代码、文档和 Web 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-DETECTION 服务概述

Red Hat Insights for Red Hat Enterprise Linux malware-detection 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。malware-detection 服务包含与 YARA 模式匹配的软件和恶意检测签名。签名与 IBM X-Force 智能团队合作与红帽威胁智能团队紧密合作。

在 malware-detection 服务 UI 中，用户访问授权管理员和查看器可以

- 请参阅扫描 RHEL 系统的签名列表。
- 参阅在 Insights 客户端中启用了 malware-detection 功能的所有 RHEL 系统的汇总结果。
- 请参阅各个系统的结果。
- 知道系统何时显示存在恶意软件的证据。

这些功能为安全威胁评估者和 IT 事件响应团队提供了准备响应的宝贵信息。

malware-detection 服务不推荐解析或修复恶意事件。

解决恶意软件威胁的策略取决于许多特定于每个系统和组织的条件和注意事项。您的机构的安全事件响应团队最适合为每个缺陷设计并实施有效的缓解和补救策略。

1.1. YARA MALWARE 签名

YARA 签名检测是 Insights for Red Hat Enterprise Linux malware-detection 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定义规则的布尔值表达式组成。当扫描的 RHEL 系统上存在签名中的一个或多个条件时，YARA 会在那个系统上记录命中。

1.2. IBM X-FORCE THREAT INTELLIGENCE 签名

Insights for Red Hat Enterprise Linux malware-detection 服务包括由 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 智能团队编译的签名由 *XFTI-* 前缀在恶意软件检测服务中识别，例如 *XFTI_FritzFrog*。

第 2 章 使用 INSIGHTS FOR RHEL MALWARE-DETECTION 服务

要开始使用 malware-detection 服务，必须执行以下操作：本章遵循每个操作的步骤。

注意

有些流程需要系统的 sudo 访问权限，其他流程要求管理员执行该操作是具有 Malware 检测管理员角色的用户访问组的成员。

表 2.1. 设置恶意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 应用程序并配置 Insights 客户端以使用 malware-detection 服务	sudo 访问权限
在 Red Hat Hybrid Cloud 控制台中配置用户访问	在 Red Hat Hybrid Cloud Console > Settings 菜单(gear 图标)> Identity & Access Management > User Access > Groups, create malware-detection groups，然后将适当的角色和成员添加到组中	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 User Access 组成员资格

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 malware-detection 控制器，然后运行测试和完整的恶意检测扫描，并将数据报告给 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

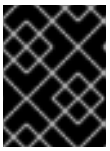
1. 安装 YARA。
   红帽客户门户网站上提供了适用于 RHEL8 和 RHEL9 的 YARA RPM：

```
$ sudo dnf install yara
```

注意

RHEL7 不支持 Insights for Red Hat Enterprise Linux malware-detection。

2. 如果尚未完成，请通过 Insights for Red Hat Enterprise Linux 注册系统。



重要

在可以使用 malware-detection 服务前，必须在系统中安装 Insights 客户端软件包，以及使用 Insights for Red Hat Enterprise Linux 的系统。

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。

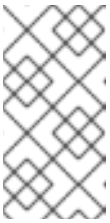
```
$ sudo insights-client --register
```

3. 运行 Insights 客户端 malware-detection 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 malware-detection 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的系统的最小扫描。测试扫描主要是为了帮助验证安装、操作和上传是否在 malware-detection 服务中正常工作。找到多个匹配项，但这意是有意关注的。初始测试扫描的结果不会出现在 malware-detection 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
```

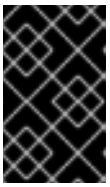
考虑设置以下选项来最小化扫描时间：

- **filesystem_scan_only** - 仅扫描系统上的某些目录
- **filesystem_scan_exclude** - 用来排除扫描某些目录
- **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。文件系统和进程扫描完成后，查看 Red Hat Enterprise Linux > Malware 的结果。



重要

默认情况下禁用扫描过程。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。这个问题将在即将发布的 YARA 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-detection-config.yml** 中设置 **scan_processes: true**。

```
scan_processes: true
```

注意

在您存在时请考虑设置这些进程相关选项：process_scan_only - 仅扫描系统上的某些进程，以仅扫描某些进程被扫描的 process_scan_since - 以仅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. 在 USER ACCESS 中配置 MALWARE-DETECTION 组、角色和成员

机构管理员必须在 Red Hat Hybrid Cloud Console > Settings 菜单(gear 图标)> Identity & Access Management > User Access > Groups 中创建 malware-detection 角色和成员（帐户中注册的用户）。

重要

malware-detection 服务用户没有 "default-group" 角色。要使用户能够查看 malware-detection 服务中的数据或控制设置，用户必须是一个或多个具有以下角色的用户访问组的成员：

- **malware 检测查看器**
- **malware 检测管理员**

注意

目前，这些角色的权限限制没有区别，但随着未来月内的新功能，某些操作只能供管理员用户使用。

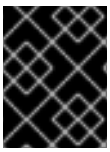
Resources

有关在 Red Hat Hybrid Cloud Console 上配置用户访问权限 *的完整文档：用户访问控制(RBAC)*。

2.2.1. 在用户访问中创建和配置恶意检测组

以下流程演示了帐户中的机构管理员如何创建用户访问组，并将 Malware 检测 *管理员角色添加到组中*，然后添加在 malware-detection 服务中具有管理员特权 *的成员*。

无论用途、角色或成员是什么，在 User Access 中创建任何组的说明都是相同的。机构管理员应该为管理员和另一个组创建一个组。



重要

目前，Malware 检测管理员和查看器角色限制了权限之间没有区别；但是，这将在以后的版本中有所变化。

先决条件

您必须以机构管理员身份登录到您的 Red Hat Hybrid Cloud Console 帐户。

流程

1. 单击应用程序窗口 **右上角的齿轮图标**，然后选择 **Settings**

2. 进入 Red Hat Hybrid Cloud Console > Settings menu (gear icon)> Identity & Access Management > User Access > Groups。
3. 点 **Create group**。
4. 输入 **组名称**，如 *Malware Administrators* 以及描述，然后单击 **Next**。
5. 选择要添加到此组的角色，例如 *Malware 检测管理员*。点该角色的复选框并点 **Next**。
6. 将成员添加到组中。根据用户名、电子邮件或状态搜索单个用户或过滤。选中每个预期成员名称旁边的复选框，然后单击 **Next**。
7. 查看详情以确保所有内容都正确。如果您需要返回并更改内容，请单击 **Back**。
8. 点 **Submit** 以完成组的创建。

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

在混合云控制台上查看系统扫描结果。

先决条件

- YARA 和 Insights 客户端使用本文档的第 2 章的步骤在 RHEL 系统上安装和配置。
- 您必须登录到混合云控制台。
- 您是 *Malware 检测管理员*或 *Malware 检测查看者*角色的成员。

流程

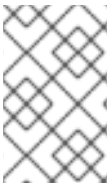
1. 进入 Red Hat Enterprise Linux > Malware > Systems 。
2. 查看仪表板，以快速了解所有 RHEL 系统，并启用了恶意检测和报告结果。

3. 要查看特定系统的结果，请使用 **Filter by name** 搜索框按名称搜索系统。

第 3 章 其他恶意检测服务概念

3.1. 系统扫描

在发布时，Malware 检测管理员必须根据需要启动 Insights for Red Hat Enterprise Linux malware-detection 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，由于扫描可能需要大量时间才能运行，所以 Insights for Red Hat Enterprise Linux malware-detection 服务团队建议每周运行恶意软件检测扫描。

3.1.1. 启动恶意检测扫描

执行以下步骤来运行恶意检测扫描。扫描完成后，Insights for Red Hat Enterprise Linux malware-detection 服务会报告数据。扫描时间取决于多个因素，包括配置选项、运行的进程数量等。

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. 查看 Red Hat Enterprise Linux > Malware 的结果。

3.2. 解释 MALWARE-DETECTION 服务结果

在大多数情况下，使用 YARA 运行恶意检测扫描将导致没有签名匹配。这意味着，在将已知软件签名与扫描中包含的文件进行比较时，YARA 找不到任何匹配的字符串或布尔值表达式。malware-detection 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，并在 Insights for Red Hat Enterprise Linux malware-detection 服务 UI 中缺少匹配项。

如果带有 YARA 的 malware-detection 扫描进行一个匹配项，它将发送与 Red Hat Insights 匹配的结果，您可以在 malware-detection 服务 UI 中看到匹配项详情，包括文件和日期。最后一次 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安全事件响应团队。例如，如果在一个扫描中找到了签名匹配，但没有在同一系统的下一次扫描中找到，这可能表示仅在某个进程运行时可以检测到的恶意软件。

3.3. MALWARE-DETECTION 收集器的额外配置选项

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

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哪些文件/目录。仅会扫描指定的项目。它可以是单个项目，也可以是项目列表（与 yaml 语法一致，用于指定项目列表）。如果此选项为空，它基本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，您可以在其中指定不扫描哪些文件/目录。已列出多个目录意味着默认排除它们。这包括虚拟文件系统目录、例如 /proc、/sys、/cgroup ；可能具有外部挂载的文件系统、如 /mnt 和 /media 的目录，以及建议不要扫描的其他目录，如 /dev 和 /var/log/insights-client （以防止假的正状态）。您可以自由修改列表来添加（或减去）文件/目录。

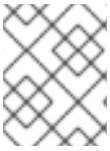
  请注意，如果在 filesystem_scan_only 和 filesystem_scan_exclude 中同时指定了同一项，如 /home，则 filesystem_scan_exclude 将为 'win'。也就是说，/home 不会被扫描。另一个示例，可以 filesysem_scan_only 一个父目录，例如 /var，然后在那个示例中包括 filesystem_scan_exclude 某些目录，如 /var/lib 和 /var/log/insights-client。然后，/var/lib 和 /var/log/insights-client 以外的所有内容都会被扫描。

- **filesystem_scan_since**
  仅扫描已修改 'since' 的文件，其中 since 可以是代表天前或'last' 表示自上次文件系统扫描以来的整数。例如： filesystem_scan_since: 1 表示扫描自 1 天前创建或修改的文件（以最后一天表示 filesystem_scan_since: 7 表示自 7 天前创建/修改的文件）和 filesystem_scan_since：last 表示从 malware-client 的最后成功 filesystem_scan 开始扫描已创建/修改的文件。

- **exclude_network_filesystem_mountpoints and network_filesystem_types**
  设置 **exclude_network_filesystem_mountpoints: true** 表示 malware-detection 收集器不会扫描挂载的文件系统的挂载点。这是默认设置，是防止扫描外部文件系统，从而导致不必要的和增加网络流量和较慢的扫描。它认为为网络文件系统的文件系统列在 **network_filesystem_types** 选项中。因此，在该列表中且挂载的任何文件系统类型都将不包括在扫描中。这些挂载点本质上添加到 **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 默认禁用，以防止在扫描大量或大型进程时对系统性能产生影响。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、如 123 或 PID 范围，如 1000..2000，或通过进程名称 eg Chrome 指定。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 process_scan_only 和 process_scan_exclude 中，则 processes_scan_exclude 将 'win' 排除。

- **processes_scan_since**
  这与 filesystem_scan_since 类似，但适用于进程。仅扫描已启动 'since' 的进程，其中 since 可以是代表天前或"last' 表示的整数，自上次成功进程扫描 malware-client 后。

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进行设置。使用环境变量会覆盖配置文件中相同选项的值。环境变量的名称与配置文件选项相同，但比较大写。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 **/etc**、**/tmp** 和 **/var/lib** 的目录，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

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

第 4 章 为恶意事件启用通知和集成

您可以在 Red Hat Hybrid Cloud Console 中启用通知服务，以便在 malware 服务至少检测到签名匹配并生成警报时发送通知。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 malware 服务检测到系统可能威胁时自动发送电子邮件消息，或者向 malware 服务每天生成的所有警报发送电子邮件摘要。

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 以了解事件数据
- 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，将恶意软件事件路由到应用程序仪表板

malware 服务通知包括以下信息：

- 受影响的系统的名称
- 系统扫描过程中可以找到多少签名匹配
- 查看 Red Hat Hybrid Cloud 控制台详情的链接

启用通知服务需要三个主要步骤：

- 首先，机构管理员创建一个带有 Notifications administrator 角色的用户访问组，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，行为组可以指定是否向所有用户发送电子邮件通知，还是只发送给机构管理员。
- 最后，从事件接收电子邮件通知用户必须设置其用户首选项，以便接收每个事件的独立电子邮件。

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 Red Hat Insights 通知 。

对红帽文档提供反馈

我们感谢您对我们文档的反馈。要提供反馈，请突出显示文档中的文本并添加注释。

先决条件

- 已登陆到红帽客户门户网站。
- 在红帽客户门户网站中，文档采用 **Multi-page HTML** 查看格式。

流程

要提供反馈，请执行以下步骤：

1. 点击 **文档** 右上角的反馈按钮查看现有的反馈。

注意

反馈功能仅在多页 HTML 格式中启用。

2. 高亮标记您要提供反馈的文档中的部分。
3. 点在高亮文本旁弹出的 **Add Feedback**。
   文本框会出现在页面右侧的反馈部分中。
4. 在文本框中输入您的反馈，然后点 **Submit**。
   已创建一个文档问题。
5. 要查看问题，请点击反馈视图中的问题链接。