COHESITY

Cyberworld

如何部署 Cohesity Clean Room 解决方案

快速指南

Cohesity Clean Room 解决方案提供了一个可信的环境，可加快事件响应的速度，支持 SecOps 调查，同时最大限度地降低被二次攻击的风险。

由于采用了模块化设计，Cohesity能够快速创建一个隔离环境，支持响应和恢复过程，使团队能够更快地缓解威胁。

五个阶段

1. **准备** — 做好应对网络攻击的准备
2. **启动** — 最低可行响应能力 (MVRC)
3. **调查** — 确定攻击的范围和原因
4. **缓解** — 修复、补丁、加固、测试
5. **恢复** — 验证、可信的生产恢复

阶段 1

准备

准备阶段着重于采取主动措施，以减少攻击的影响，从而使企业在需要时能够拥有可信的资源。

COHESITY

Cyberworld

1

3-2-1 备份规则

至少创建 3 份数据副本。

2 份副本存储在本地的不同介质上，1 份副本存储在异地。

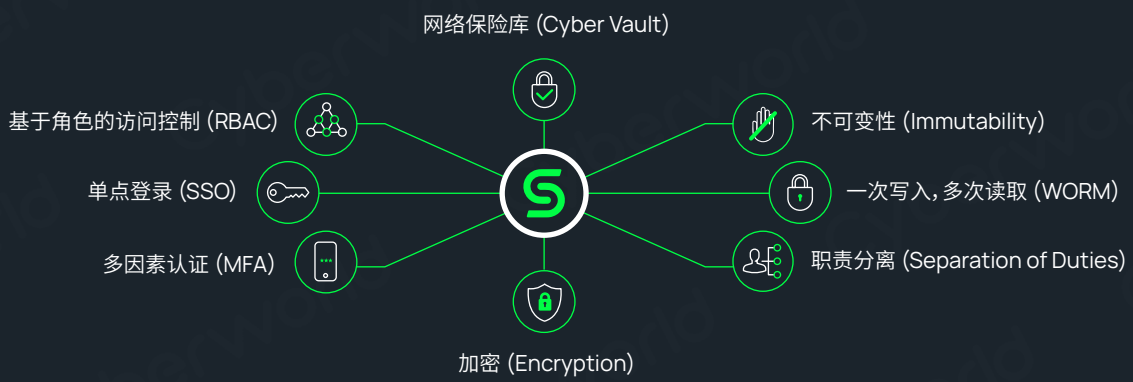
部署拓扑

		备份	复制	双重复制	归档	双重归档
基础 2 份或更少副本	拓扑 1	✓	-	-	-	-
	拓扑 2	✓	✓	-	-	-
	拓扑 3	✓	-	-	✓	-
增强 3 份副本	拓扑 1	✓	✓	-	✓	-
	拓扑 2	✓	-	✓	-	-
关键任务 4 份或更多副本	拓扑 1	✓	-	✓	✓	-
	拓扑 2	✓	✓	-	-	✓
	拓扑 3	✓	-	✓	-	✓

2

加固您的 Cohesity 平台

通过采取主动措施来提高数据的安全性，以减少漏洞并缓解潜在风险。



COHESITY

Cyberworld

3

准备好您的数字应急包 (digital jump bag™)

在 Cohesity SmartFiles View 上准备一个软件存储库，存储关键工作负载的黄金镜像 (golden image)，包括 ISO、软件、配置文件、文档、模板等，这些都是创建隔离环境所需的。

4

隔离您的网络

规划网络分段，以确保隔离环境完全与生产网络断开连接，可以使用专用网络交换机或虚拟局域网 (VLAN) 来实现。

5

建立通信协议

清晰的通信协议可确保高效的协调，减少混乱，并最大限度地缩短停机时间。

COHESITY

Cyberworld

流程	目的
角色与职责	确保问责制。您可以把具体任务分配给团队成员（事件协调员、IT 响应人员、法律顾问和高管），由他们做出决策。
通信渠道与工具	安全且集中的通信。建立专用渠道，例如用于内部通信的 Slack 或 Microsoft Teams（启用 VPN），以及用于安全外部通信的 ProtonMail 。
通信计划	有效协调。使用 Confluence 或 Google Docs 等工具制定一个结构化计划，详细说明在恢复阶段谁负责沟通什么内容以及何时沟通。
定期更新	实时更新。使用 ServiceNow 或 PagerDuty 中的仪表板，向所有利益相关者通报进展和后续步骤。

阶段 2

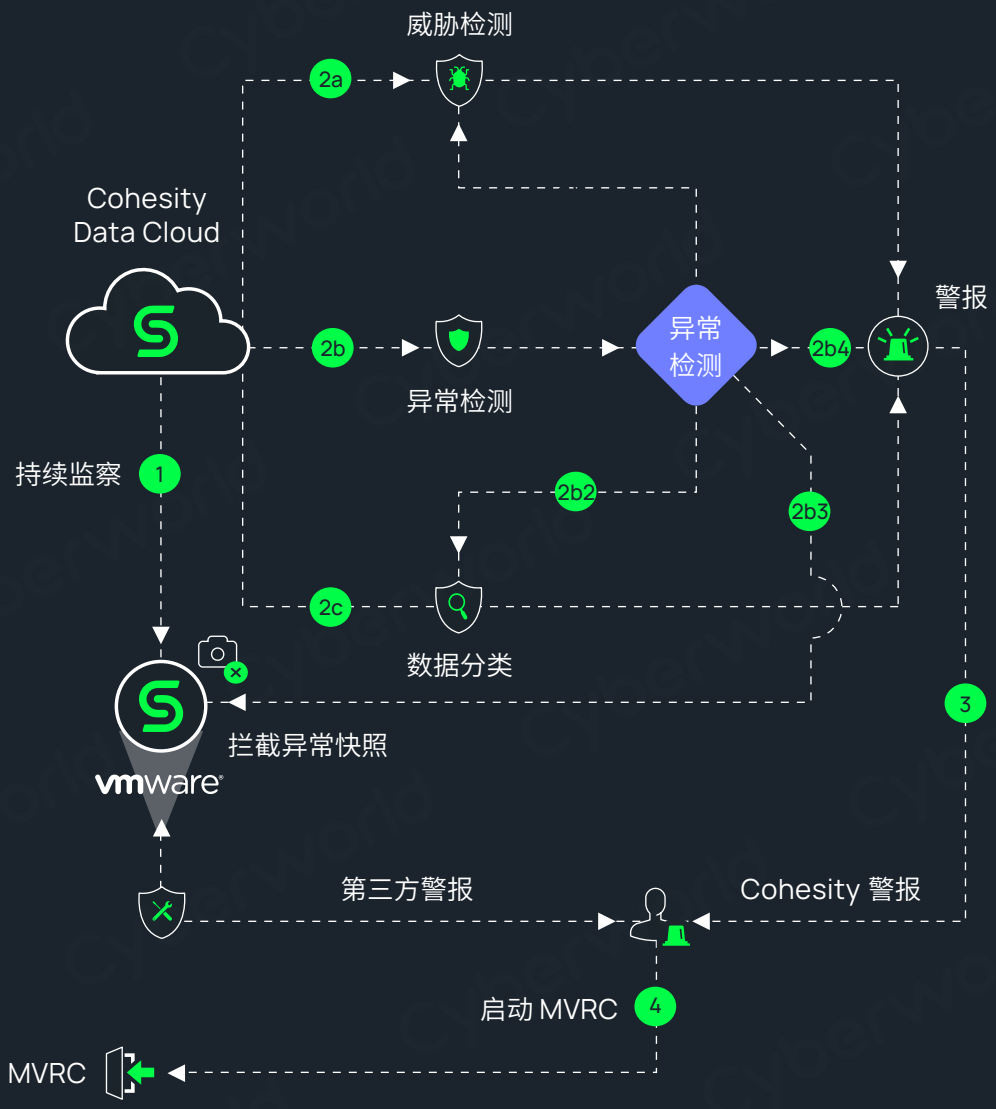
启动

启动阶段涉及建立最低可行响应能力 (Minimum Viable Response Capability, MVRC)，包括遏制漏洞、恢复基本操作和最大限度地减少停机时间所需的关键工具和流程，以帮助确保网络攻击期间的运营连续性。

1

检测网络攻击

网络攻击要么由 Cohesity 的异常和威胁检测功能自动检测到，要么由客户使用其他安全工具检测到。一旦检测到网络攻击，启动阶段即刻开始。

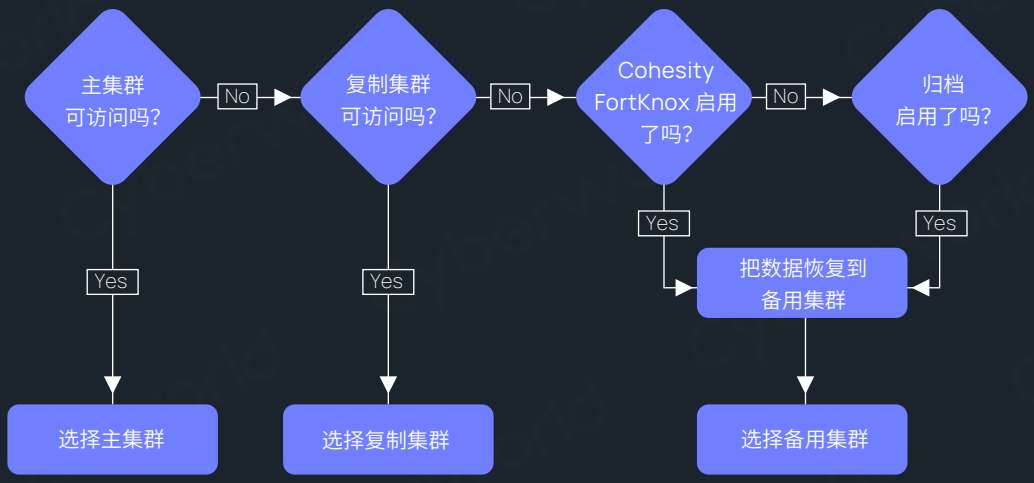


识别 Cohesity Source Cluster（源集群）

要确定从哪个 Cohesity Source Cluster 中检索数据或快照，以便用于在 Clean Room 进行取证分析。
从该 Cohesity Source Cluster 中选择用于取证分析的数据或快照。

位置	形式
用户自己管理的 本地数据中心	· 主集群 (Primary Cluster) · 复制集群 (Replication Cluster) · 虚拟隔离 (Virtual air-gapped) 复制集群 · NAS 归档
云	· FortKnox（虚拟隔离网络保险库） · 云归档 (AWS、Azure、GCP)

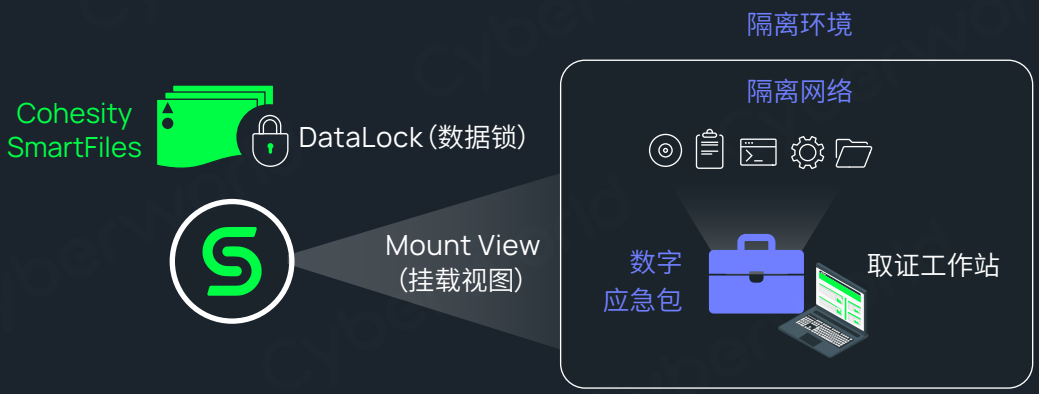
Cohesity 可以从上述任何形式中恢复数据。



3

检索您的数字应急包

把数字应急包挂载到 Clean Room 的主机上。
正如准备阶段所述，数字应急包位于 Cohesity SmartFiles View 中。



数字应急包检索策略

位置	描述	用例
主集群	数据中心或生产位置的 Cohesity Cluster	· 当您的生产环境是可信的时候 · 用于安全演练
隔离开来的复制集群	灾难恢复 (DR) 站点上的 Cohesity Cluster 拥有复制的副本	· 当主集群宕机的时候 · 在 DR 站点上检索数字应急包
FortKnox	Cohesity 安全保险库解决方案	· 当主集群和复制集群都无法访问的时候

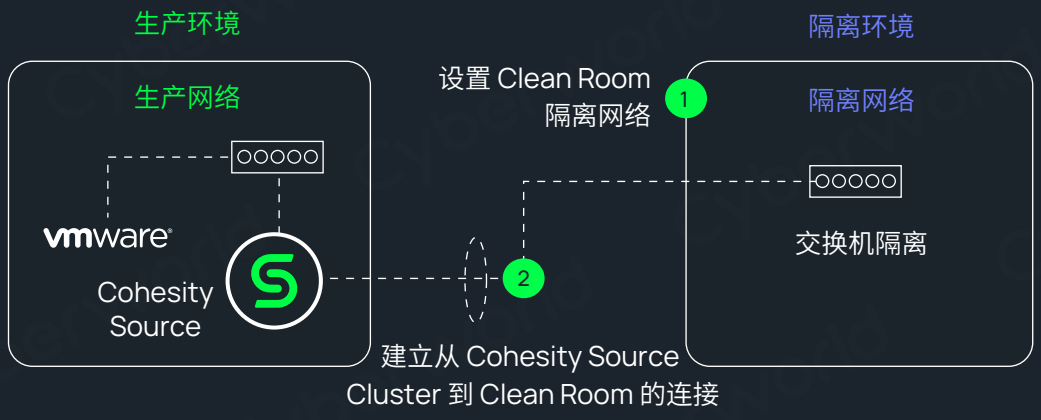
COHESITY

Cyberworld

4

设置隔离的 Clean Room 网络

正如准备阶段所述，在 Clean Room 中设置一个隔离网络，
并建立 Clean Room 与您的 Cohesity Source（在上一步中选定）之间的连接。

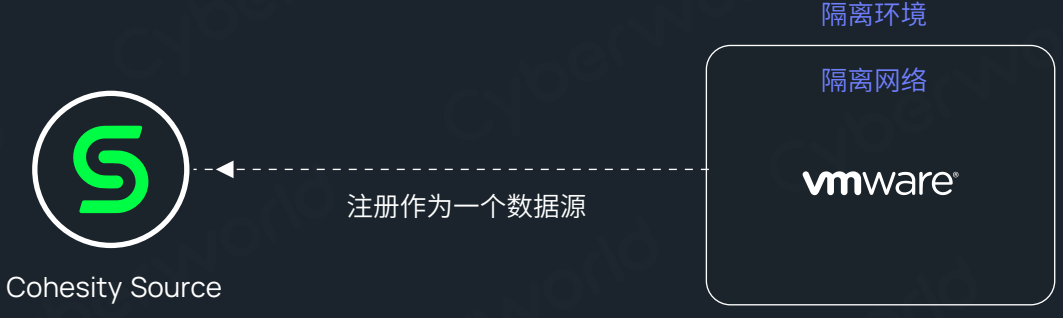


5

设置您的 Clean Room 基础设施

使用数字应急包组件构建您的 Clean Room 基础设施。使用数字应急包在 Clean Room 中设置网络组件、虚拟环境和拨号音应用程序 (Dial Tone Applications)。

在 Clean Room 中安装的虚拟环境，必须在 Cohesity Source Cluster（生产或复制）上注册，作为一个数据源，以便您从中把快照恢复到 Clean Room 进行调查。



* 拨号音应用程序 (Dial Tone Applications) 是指一些基本的业务工具和系统，例如电话系统、身份与访问管理 (IAM)、电子邮件、域名系统 (DNS)、安全工具等。

COHESITY

Cyberworld

阶段 3

调查

调查阶段侧重于了解网络攻击的范围和影响，确定攻击原因，
评估其对系统的影响程度，并保存证据以供进一步调查。

1

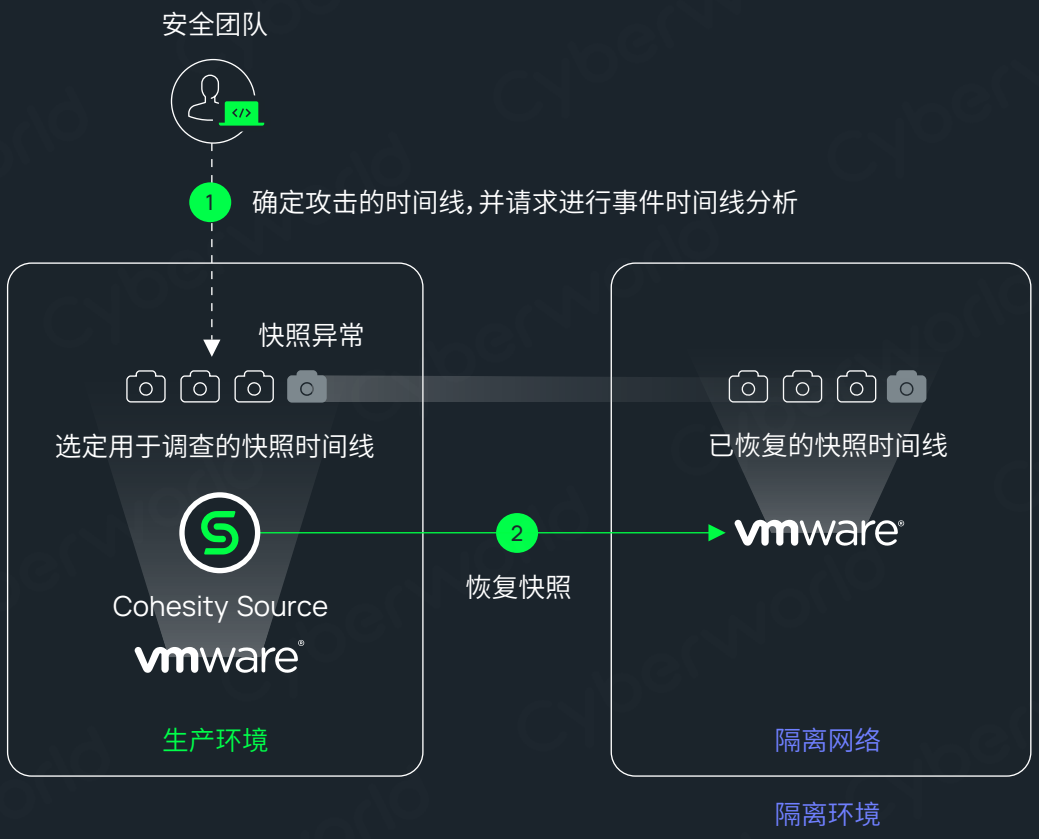
创建取证调查视图

在 Cohesity SmartFiles View 上准备取证存储库，用于收集证据。然后，把这个取证调查视图挂载到 Clean Room 中的取证工作站上。

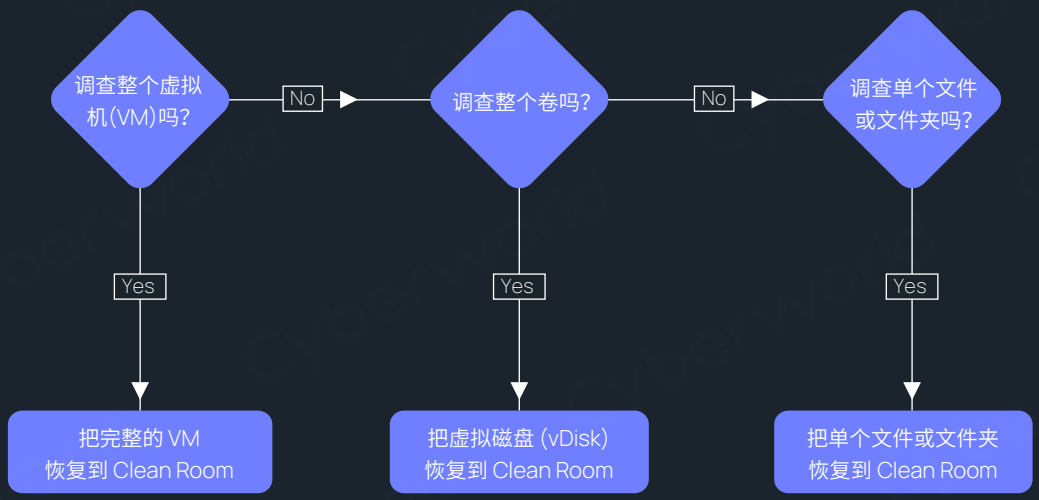
2

恢复用于调查的系统和数据

把您需要的系统、卷、文件、文件夹与其他收集的证据一起恢复到 Clean Room 中。
确定事件的时间线，并关联攻击的细节，以便用于缓解措施。



选择恢复方法



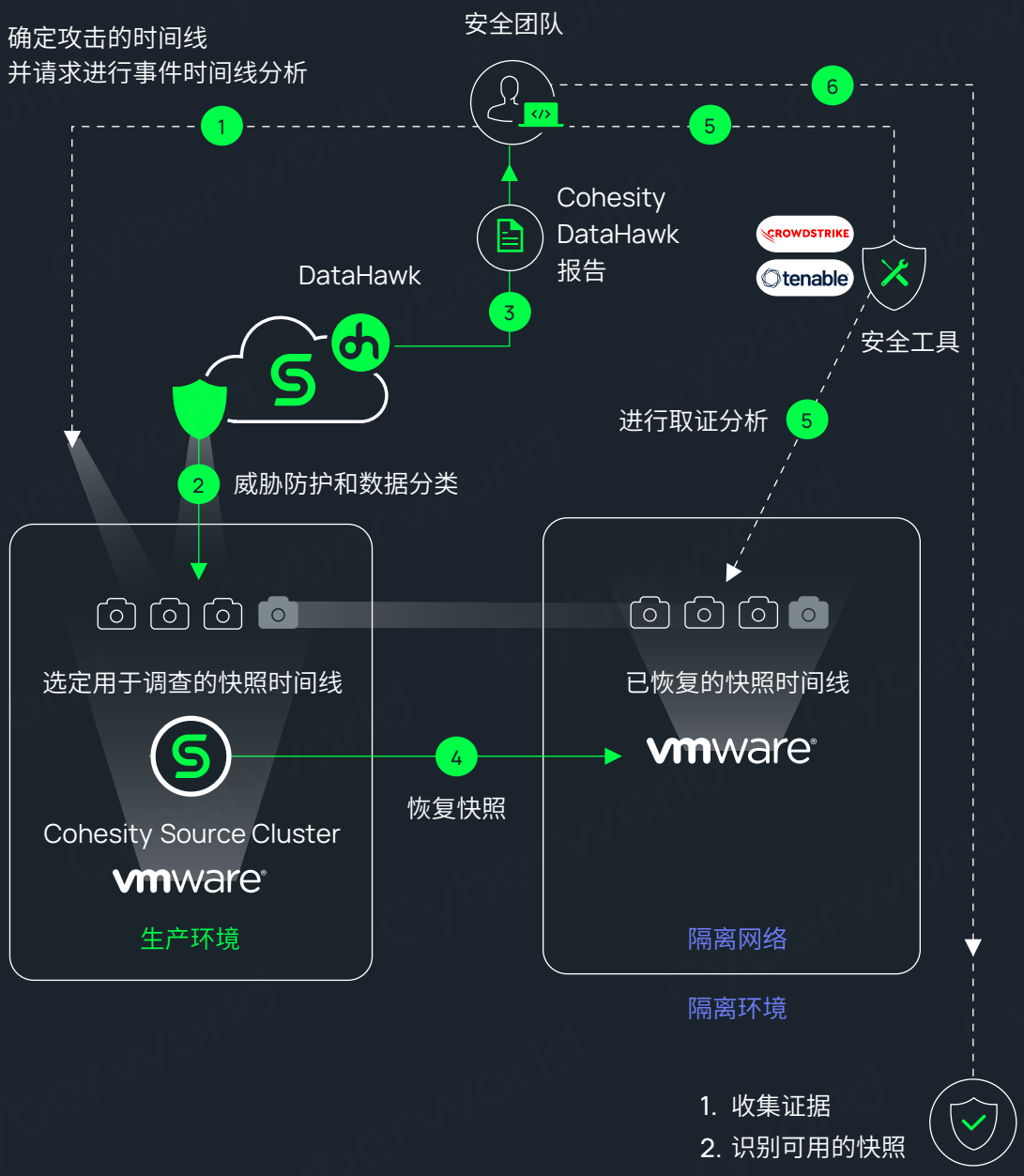
* 根据您的 SecOps 决策，选择是否恢复整个卷、单个文件夹或文件。

进行取证调查

使用安全工具和 Cohesity DataHawk 报告，在 Clean Room 中对已恢复的快照进行取证检查。

COHESITY

Cyberworld



- 在取证调查期间，让您的事件响应团队参与进来。
- 比较 Active Directory (AD, 活动目录) 的更改，以确保用户帐户、权限和配置的完整性。

建议

使用 Cohesity DataProtect 来保护您的 AD，并轻松地比较您的 AD 快照。

[1] 在您选定的时间段内，对所需范围的快照执行 DataHawk 操作。

[2] 所需范围的快照会被恢复到 Clean Room，并对其进行调查。

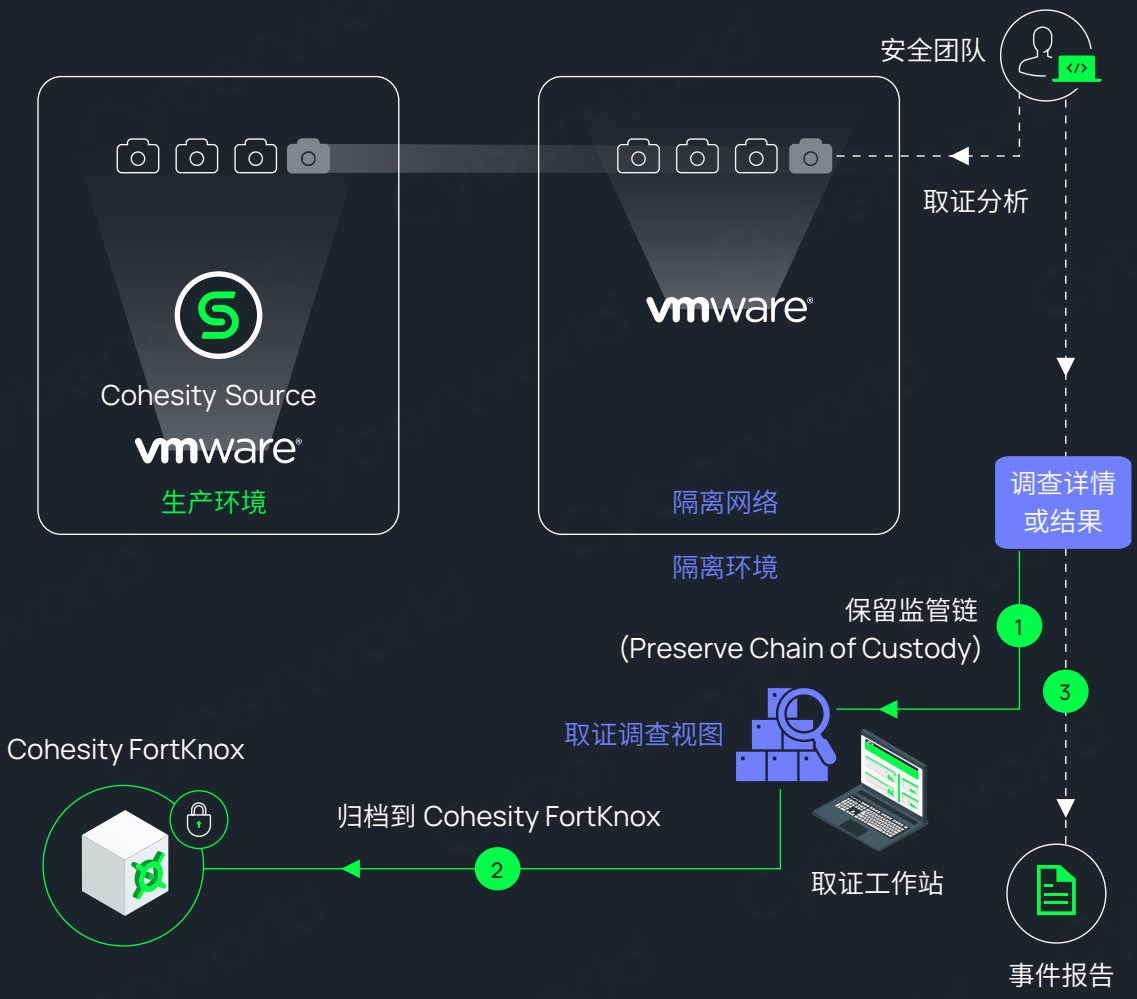
COHESITY

Cyberworld

4

保留证据

收集所有取证调查的详情和结果，把它们保存在第 1 步创建的取证调查视图中。



调查阶段的成果

- 创建可用的快照，用于缓解措施。
- 创建事件报告，详细说明修复和根除步骤。

阶段 4

缓解

缓解阶段着重于采取措施限制损害程度，在暂存环境中恢复和测试受影响的系统，从网络中移除恶意软件，并防止进一步感染。

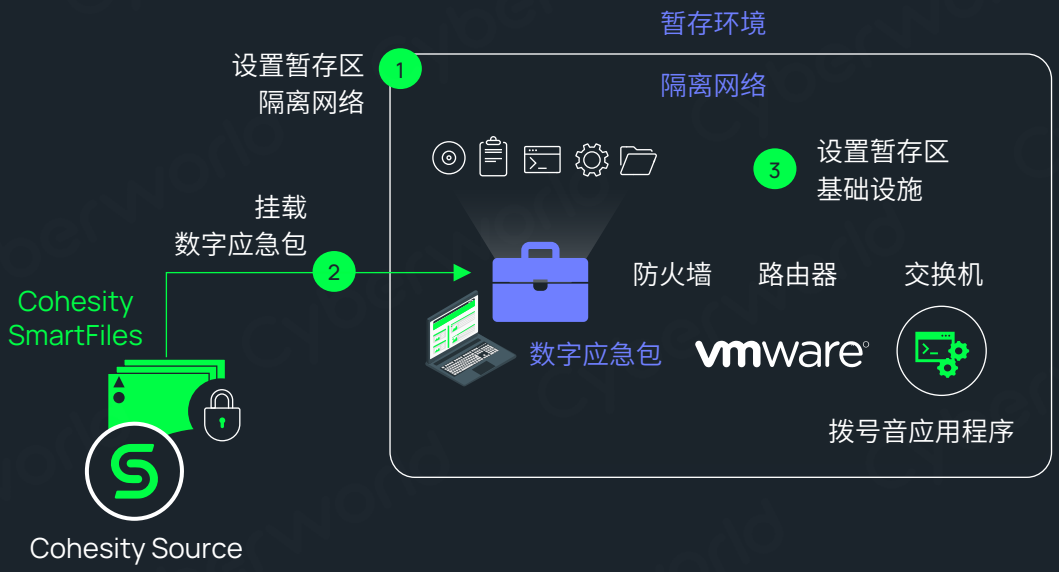
COHESITY

Cyberworld

1 设置暂存区 (Staging Room)

暂存区是一个隔离且受控的环境，类似于 Clean Room。在暂存区，数据和系统会进行全面的修复和验证，以确保它们没有受到威胁或损坏。

按照准备 Clean Room 的相同步骤来准备暂存区。详情请参阅“启动阶段”。



---

2 恢复系统和数据

把系统和数据恢复到暂存区进行修复。

决定是否恢复或重建系统和数据

1. 从 Cohesity 备份中将系统和数据一起恢复到暂存区，并对其进行修复。
2. 用黄金镜像在暂存区中重建系统。从 Cohesity 备份中恢复数据到暂存区进行修复。

COHESITY

Cyberworld

3

修复

使用调查阶段的事件报告来修复受影响的工作负载。

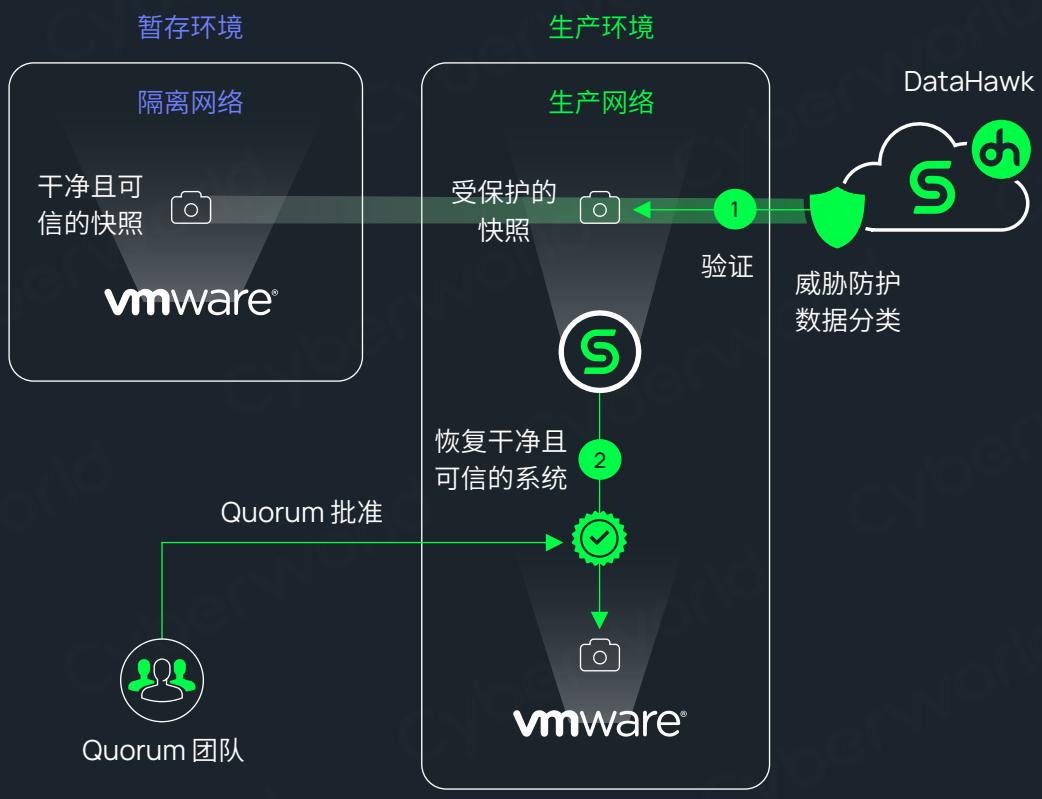
修复步骤

步骤	目的	责任方
补丁	解决已知问题或更新软件系统，以防止威胁利用漏洞。	IT 团队
漏洞修复	解决系统中的安全弱点和漏洞，以防止被利用和攻击，包括修补系统。	IT 团队
系统加固	通过减少攻击面和应用安全控制来增强系统的安全性，以防范威胁和未经授权的访问。	IT 或安全团队
集成测试	确保不同组件和系统能够无缝协作，在部署到生产环境之前识别并解决任何问题。	IT 或安全团队

阶段 5

恢复

恢复阶段着重于最终验证和将干净的系统安全恢复至生产环境。同时，IT 和安全团队需要实施长期的改进或调整，避免未来再次发生类似的攻击。



Cyberworld
广州科明大同科技有限公司

COHESITY
中国区总代理

公司网站 www.cyberworld.com.cn
业务电邮 info@cyberworldchina.com
服务专线 400-9988-792