Security Day 亚马逊云中的扩展的威胁检测与响应

2021 年 3 月 12 日

概述

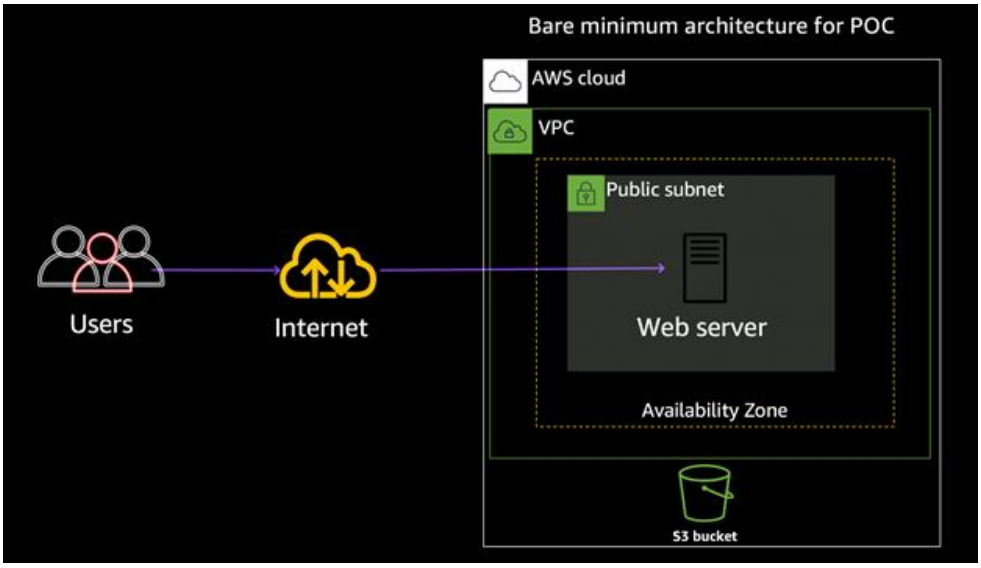
本研讨会旨在帮助您熟悉 AWS 安全服务，并学习如何使用它们来识别和修复环境中的威胁。您将使用诸如 Amazon GuardDuty（威胁检测）、Amazon Macie（发现、分类和保护数据）、Amazon Inspector（漏洞和行为分析）、 Security Hub（集中式安全视图）等服务。您将学习如何使用这些服务在攻击期间和之后调查威胁，设置通知和响应管道，以及添加其他保护以改善环境的安全状况。

背景

您的公司是云计算的新手，最近为试点目的对您的基础设施进行了提升和转移。您是一名系统管理员，负责 AWS 环境中的安全监控。作为维护的一部分，您还负责响应环境中的任何安全事件。

建筑

对于本次实验，您将在美东一（us-west-1）区域设置一个实例。由于这是一个用于试点的“升降式”迁移，您还需要在应用程序中构建冗余，因此您只有一个面向公共的 web 服务器。web 服务器可以通过弹性网络接口访问 Internet 网关。客户通过指向弹性网络接口的 DNS 条目访问您的 web 服务器。您将静态内容存储在 S3 bucket 中，并使用 vpc s3 端点网关从 web 服务器进行访问。



地区

请使用 us-east-1（弗吉尼亚北部）地区进行本次研讨会。

模块

本研讨会分为以下四个模块：

1. 环境构建和配置
2. 攻击模拟
3. 检测和补救
4. 回顾

模块 1：环境构建和配置

在第一个模块中，您将为您的环境配置检测和响应控件。您将运行两个 CloudFormation 模板中的第一个，该模板将自动创建其中一些控件，然后手动配置其余控件。如果尚未登录 AWS 控制台，请登录。

议程

1. 运行初始 CloudFormation 模板
2. 在电子邮件中确认 SNS 订阅
3. 创建 CloudWatch 规则
4. 手动启用检测控制

启用 Amazon GuardDuty

我们的第一步是启用 Amazon GuardDuty，它将持续监视您的环境中是否存在恶意或未经授权的行为。

- 转到 Amazon GuardDuty 控制台（us-east-1）。
- 如果“开始使用”按钮可用，请单击它。如果未启用 GuardDuty，则跳过第三步。
- 在下一个屏幕上，单击 Enable GuardDuty 按钮。

GuardDuty 现在已启用，并持续监视您的 CloudTrail 日志、VPC 流日志和 DNS 查询日志以查找您环境中的威胁。

部署 AWS CloudFormation 模板

要启动场景并配置环境，您需要运行模块 1 CloudFormation 模板，你可以通过下面的链接获得该模版：https://gcrsecurityworkshopcftempate1.s3.amazonaws.com/01-environment-setup-nom.yml

1. 在 Console 界面右上角确认使用的区域是美东一弗吉尼亚北部 us-east-1，在服务列表中选择 AWS cloudformation，点击右边的“创建堆栈”按钮，选择“模版已就绪”，指定模版部分选择“Amazon S3 bucket”，在下面的输入框粘贴上面的 yaml 文件的链接地址。点击“下一步”
2. 在“指定详细信息”部分输入必要的参数，如下所示。

   堆栈名称：ThreatDetectionWksp 环境设置（根据自己喜好输入）
   电子邮件地址：输入你可以访问的有效 Email 地址
3. 单击“下一步”，
4. 该页面内容在本 workshop 不需要输入，保持默认值即可，再次单击“下一步”
5. 在该页面预览输入的内容，勾选“我确认，AWS CloudFormation 可能创建具有自定义名称的 IAM 资源。”内容前面的复选框。点击“创建堆栈”

回到 CloudFormation 控制台。您可以刷新页面以查看开始创建的堆栈。在继续之前，请确保堆栈处于 CREATE\u COMPLETE 状态，如下所示。

别忘了检查你的电子邮件！

您将收到一封来自 SNS 的电子邮件，要求您确认订阅。确认订阅，以便您可以在研讨会期间接收来自 AWS 服务的电子邮件警报。电子邮件可能需要 2-3 分钟才能到达，如果未在该时间段内到达，请检查您的垃圾邮件/垃圾邮件文件夹。

设置 Amazon CloudWatch 事件规则和自动响应

刚才运行的 CloudFormation 模板创建了用于警报和响应的 CloudWatch 事件规则。下面的步骤将引导您创建最终规则。在此之后，您将有规则接收电子邮件通知，并触发 AWS Lambda 函数来响应威胁。

下面是通过控制台创建规则的步骤，但您也可以通过查看 Amazon GuardDuty 文档了解更多有关以编程方式执行规则的信息。

1. 打开 CloudWatch 控制台（us-east-1）
2. 在左侧导航窗格的“事件”下，单击“规则”
3. 单击“创建规则”
4. 选择事件模式单击标有 Build Event Pattern 的下拉列表按服务匹配事件，然后在下拉列表中选择 Custom Event Pattern。

在下面的自定义事件模式中复制并粘贴：

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail": {
    "type": [
      "UnauthorizedAccess:EC2/MaliciousIPCaller.Custom"
    ]
  }
}
```

1. 对于目标，单击添加目标，选择 Lambda 函数，**threat-detection-wksp-remediation-nacl**。单击底部的配置详细信息。
2. 在 Configure rule details 屏幕上填写名称和描述（建议如下）

名称：threat-detection-wksp-guardduty-finding-ec2-maliciousip
描述：GuardDuty Finding: UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

3. 单击创建规则。可选：考虑检查 Lambda 函数以查看它的功能。打开 Lambda 控制台。单击名为 threat detection wksp 的函数

启用 AWS 安全中心 Security Hub

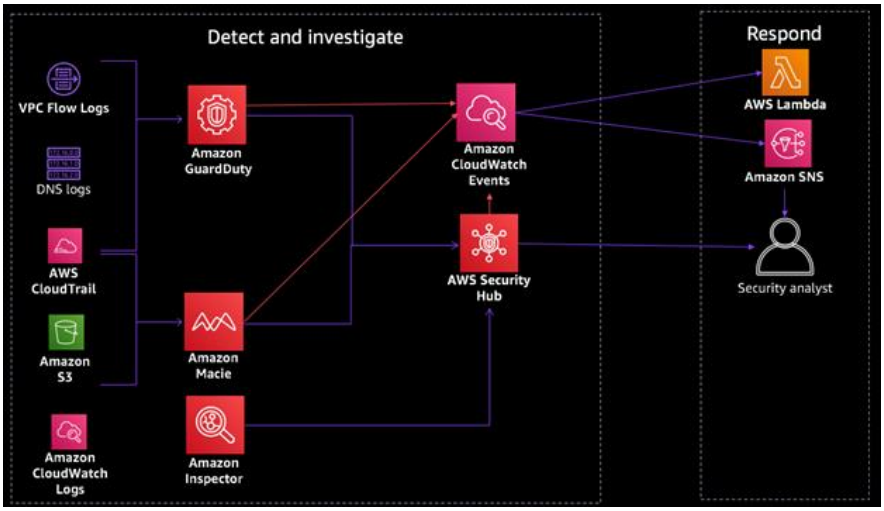
现在您的所有检测控件都已配置，您需要启用 AWS Security Hub，它将为您提供 AWS 环境的安全性和法规遵从性的全面视图。

1. 转到 AWS 安全中心控制台。
2. 单击转到安全中心按钮。
3. 在下一个屏幕上，单击启用 AWS 安全中心按钮。

如果您在安全中心控制台中看到红色文本 AWS Config is not enabled on some accounts in the Security Hub Console，您可以安全地忽略。AWS Security Hub 现已启用，并将开始收集和汇总我们迄今启用的安全服务的结果。

体系结构概述

您的环境现在已经配置好，可以进行操作了。下面是一个图表来描述侦探控制你现在有地方。



成功设置环境后，可以继续下一个模块。

模块 2：攻击模拟

现在您已经设置了 detective 和 responsive Control，您将运行另一个 CloudFormation 模板，该模板将模拟您将要调查的实际攻击。

部署 CloudFormation 模板

要启动攻击模拟，您需要运行 CloudFormation 模块 2：
https://gcrsecurityworkshopcftempate1.s3.amazonaws.com/02-attack-simulation-nom.yml

1. 在 Console 界面右上角确认使用的区域是美东一弗吉尼亚北部 us-east-1，在服务列表中选择 AWS CloudFormation，点击右边的“创建堆栈”按钮，选择“模版已就绪”，指定模版部分选

择“Amazon S3 bucket”，在下面的输入框粘贴上面的 yaml 文件的链接地址。点击“下一步”

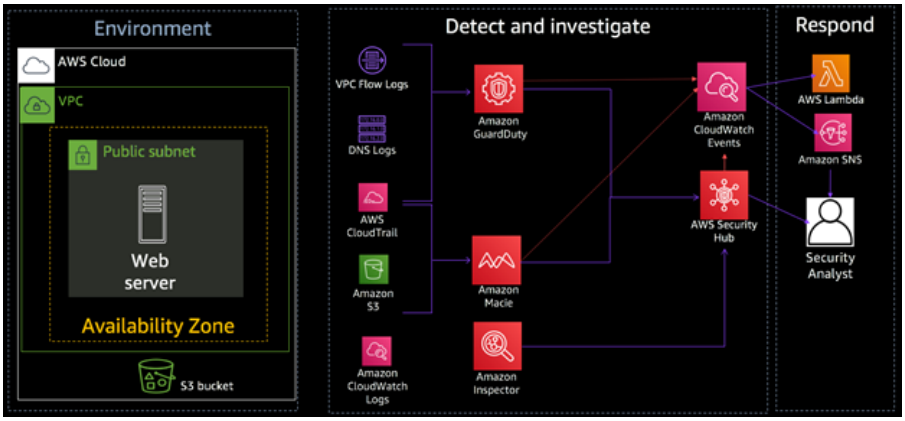
2. 在“指定详细信息”部分输入必要的参数，如下所示。堆栈名称：Attacksimulation（根据自己喜好输入），Resource Prefix：保留缺省不变
3. 单击“下一步”，
4. 该页面内容在本 workshop 不需要输入，保持默认值即可，再次单击“下一步”
5. 在该页面预览输入的内容，勾选“我确认，AWS CloudFormation 可能创建具有自定义名称的 IAM 资源。”内容前面的复选框。点击“创建堆栈”

您将回到 CloudFormation 控制台。您可以刷新页面以查看开始创建的堆栈。在继续之前，请确保堆栈处于 CREATE\u COMPLETE 状态，如下所示。

如果失败并显示错误消息[IAM\U CAPABILITY]，请确认模板将从上一步创建 IAM 角色

体系结构概述

下面是创建模块 2 云信息堆栈后的设置示意图。



请注意，在第二个 CloudFormation 模板完成后至少需要 20 分钟，您才能开始看到发现。

模块 3：检测、调查和响应

不幸的是，由于环境中的错误配置，攻击者可能已经能够访问 web 服务器。您将收到来自已安装的安全服务的警报，表明存在恶意活动。这些警报包括与已知恶意 IP 地址通信、帐户侦察、更改 Amazon S3 存储桶配置以及禁用安全配置。您必须确定入侵者可能执行了什么活动以及他们是如何执行的，这样您就可以阻止入侵者的访问，修复漏洞，并将配置恢复到正确的状态。

议程

1. 泄露 AWS IAM 凭据
2. 泄露 EC2 实例

第 1 部分-AWS IAM 认证

发现和调查

到目前为止，您已收到来自启用的安全服务的电子邮件警报。现在怎么办？作为风险驱动检测策略的一部分，贵公司已决定优先考虑 AWS IAM 相关发现。

1. 对电子邮件警报进行排序，并识别与 AWS IAM 主体相关的警报，**亚马逊 GuardDuty 发现：未经授权 zedAccess:IAMUser/MaliciousIPCaller.Custom**
2. 从电子邮件警报复制。**<访问密钥 ID>探索与访问密钥相关的发现（Amazon GuardDuty）**

现在您已经有了一个资源标识符，您可以使用 amazonguardduty 开始对这些发现进行初步调查。

1. 转到 Amazon GuardDuty 控制台（us-east-1）。
2. 在“添加筛选条件”框中单击，选择“访问密钥 ID”，然后粘贴从电子邮件复制的内容，然后选择“应用”。<访问密钥 ID>
3. 单击其中一个 Finding type 名称中包含 IAMUser 的结果查看详细信息。
4. 检查“受影响的资源”下的 Iam 实例配置文件，可以看到此查找中引用的访问密钥来自 Iam 假定的角色。
5. 检查受影响资源下的 Iam 实例配置文件，您将发现两个字符串用新行分隔。第一个是 IAM 角色的 Amazon 资源名（ARN）。第二行是 IAM 角色的唯一 ID。

您可能需要通过向左拖动中间的垂直滚动条来调整屏幕大小，以查看整个文本

1. IAM 实例配置文件包含发出 API 请求的实体的唯一 ID，当使用临时安全凭据（这是假定角色调用的情况）发出请求时，它还包含会话名称。在这种情况下，会话名称是 EC2 实例 ID，因为假设角色调用是使用 EC2 的 IAM 角色完成的。
2. 复制完整的 Iam 实例配置文件，其中包含角色的唯一 ID 和 Iam 角色 ARN：“Iam 实例配置文件”：<ARN> <唯一 ID>″
3. 检查受影响资源下的 Iam 实例配置文件并将其复制下来。这与所涉及的 IAM 角色的名称相对应，因为用于进行 API 调用的临时凭据来自附加了 IAM 角色的 EC2 实例。

回应

现在，您已经确定攻击者正在使用来自 EC2 的 IAM 角色的临时安全凭据，因此决定立即轮换凭据，以防止任何进一步的误用或潜在的权限提升。

撤消 IAM 角色会话（IAM）

1. 浏览至 AWS IAM 控制台。
2. 单击“角色”，使用先前复制的用户名（这是附加到受损实例的角色）查找上一节中标识的角色，然后单击该角色名称。
3. 单击吊销会话选项卡。
4. 单击 Revoke active sessions。
5. 单击确认复选框，然后单击撤消活动会话。

重新启动 EC2 实例以旋转访问键（EC2）

已损坏的 IAM 角色的所有活动凭据都已失效。这意味着攻击者不能再使用这些访问密钥，但也意味着任何使用此角色的应用程序都不能使用。您知道会发生这种情况，但认为这是必要的，因为 IAM 访问密钥泄露的风险很高。为了确保应用程序的可用性，您需要通过停止和启动实例来刷新实例上的访问密钥。简单的重启不会改变密钥。如果您等待实例上的临时安全凭据将被刷新，但此过程将加快速度。由于您在 EC2 实例上使用 AWS Systems Manager 进行管理，因此可以使用它来查询元数据，以验证实例重新启动后是否轮换了访问密钥。

1. 在 EC2 控制台中，停止名为 threat-detection-wksp: Compromised Instance 的实例。
2. 选中实例旁边的框，选择 Actions（操作）菜单、instance State（实例状态）、Stop（停止），然后按 Yes（是）、Stop（停止）确认
3. 等待实例状态说 stopped under Instance State（您可能需要刷新 EC2 控制台），然后启动实例。

验证访问密钥是否已旋转（Systems Manager）

1. 转到 AWS Systems Manager 控制台，单击左侧导航栏上的 Session Manager，然后单击 Start Session。您应该会看到一个名为 threat-detection-wksp: Compromised Instance 的实例，其实例状态为 running。
2. 要查看实例上当前处于活动状态的凭据，请单击该实例旁边的单选按钮，然后单击“开始会话”。
3. 在 shell 中运行以下命令，并将访问 Access Key ID 与电子邮件警报中找到的 ID 进行比较，以确保其已更改：

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/threat-detection-wksp-compromised-ec2
```

此时，您已经成功地从 AWS IAM 角色吊销了所有活动会话，并在 EC2 实例上旋转了临时安全凭据。

第 2 部分-泄露的 EC2 实例

发现和调查

现在您已经解决了受损的 IAM 凭据问题，您需要关注攻击者是如何危害 EC2 实例的。正是这种折衷允许他们查询实例元数据并窃取凭据。

探索与实例 ID（AWS 安全中心）相关的发现

在调查受损的 IAM 凭据时，您发现它来自 EC2 的 IAM 角色，并根据查找的主体 ID 标识了 EC2 实例 ID。使用实例 ID（您以前复制的，它以“i”开头，例如 i-08fa26ffb15a66f5a），您可以使用 AWS Security Hub 开始调查发现。首先，您将研究与 EC2 实例相关的 GuardDuty 发现。

1. 转到 AWS Security Hub 控制台。
2. 您将被带到“调查结果”部分（如果没有，请单击左侧导航中的“调查结果”）。

1) 建立过滤器：通过在过滤器输入框单击，向下滚动到“产品名称”，输入“GuardDuty”在输入框中

2) 使用浏览器的查找功能 Control+F，输入 instance ID（前面步骤复制所留），搜索内容

3) 从第一个匹配的资源中从 Resource ID 复制 ARN（格式类似：arn:aws:ec2:us-east-1:166199753942:instance/i-0efc5172a5d7ecc6b

4) 在过滤器处继续添加过滤条件：用资源 ID 字段过滤，输入值为上一步获得的 arn。

您看到了哪些与此实例 ID 相关的 GuardDuty 发现？其中一个发现应该表明 EC2 实例正在与威胁列表（不允许的 IP）上的 IP 地址通信，这进一步证明了实例已被破坏的结论。另一个发现应该表明特定 IP 地址的系统正在对您的实例执行 SSH 暴力攻击。现在需要调查 SSH 暴力攻击是否成功，以及这是否允许攻击者访问实例。

确定是否在 EC2 实例（AWS Security Hub）上启用了 ssh 密码身份验证

自动响应威胁可以做很多事情。例如，您可以有一个触发器来帮助收集有关威胁的信息，然后安全团队可以在调查中使用这些信息。考虑到这个选项，我们有了一个 CloudWatch 事件规则，当 GuardDuty 检测到一个特定的攻击时，它将触发 Amazon Inspector 对 EC2 实例的扫描。我们将使用 AWS Security Hub 查看检查员的调查结果。我们要确定 SSH 配置是否遵循最佳实践。

1. 转到 AWS Security Hub 控制台。
2. 到“调查结果”部分（如果没有，请单击左侧导航中的“调查结果”）。
3. 建立过滤器：通过在过滤器输入框单击，向下滚动到“产品名称”，输入“Inspector”在输入框中
4. 使用浏览器的查找功能 Control+F，输入 password authentication over SSH，搜索内容
5. 调查结果可能不在调查结果的第一页，请使用移至下一页。

单击有关密码验证 SSH 的发现，查看经历 SSH 暴力攻击的实例。

如果您在一段时间后没有看到任何发现，您的 inspector agent

可能有问题。转到控制台，单击评估模板，检查以“threat-detection-wksp”开头的模板，然后单击运行。请留出 15 分钟扫描完成。您还可以查看评估运行并检查状态。请继续学习，稍后检查结果。

检查之后，您应该看到在实例上配置了 SSH 上的密码身份验证。此外，如果您检查一些其他检查器发现，您将看到没有密码复杂性限制。这意味着该实例更容易受到 SSH 暴力攻击。

确定攻击者是否能够登录到 EC2 实例（CloudWatch 日志）

既然我们知道这个实例更容易受到 SSH 暴力攻击，让我们看看 CloudWatch 日志并创建一个度量来查看是否有任何成功的 SSH 登录（最终回答 SSH 暴力攻击是否成功的问题）。

1. 转到 CloudWatch 日志。
2. 单击 log group/threat detection wksp/var/log/secure
3. 如果有多个日志流，请使用先前复制的实例 ID 进行筛选，然后单击该流。
4. 在“筛选器事件”文本框中，放置以下筛选器模式：**[Mon, day, timestamp, ip, id, msg1= Invalid, msg2 = user, ...]**

   您是否看到任何失败的（无效用户）登录实例的尝试？这和 SSH 暴力攻击一致吗？

5. 现在将筛选器替换为成功尝试的筛选器：**[Mon, day, timestamp, ip, id, msg1= Accepted, msg2 = password, ...]**

您是否看到成功登录实例的尝试？哪个 linux 用户受到了威胁？

回应

修改 EC2 安全组（EC2）

通过更新实例所在子网上的 NACL，攻击者的活动会话自动停止。这是由一个 CloudWatch 事件规则触发器完成的，该触发器是基于某些 GuardDuty 发现调用的。您已经决定对 EC2 实例的所有管理都将通过 AWS Systems Manager 完成，因此您不再需要打开管理端口，因此下一个好的步骤是修改与 EC2 实例关联的安全组，以防止攻击者或任何其他人连接。

1. 转到 amazon ec2 控制台。
2. 查找名为 threat-detection-wksp: Compromised Instance 的运行实例。
3. 在“描述”选项卡下，单击受损实例的安全组。
4. 查看“入站”选项卡下的规则。
5. 单击编辑并删除入站 SSH 规则。SSM 代理在初始配置期间安装在 EC2 实例上。
6. 单击“保存”

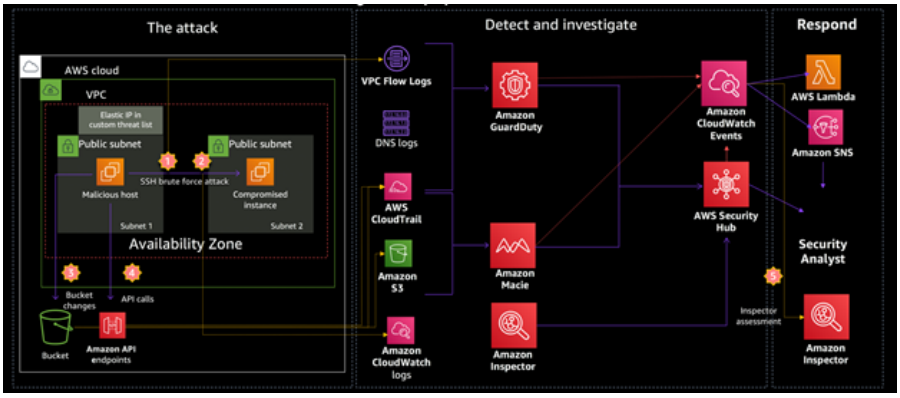
祝贺你！您已经成功地修复了事件，并进一步加强了您的环境。这显然是一个模拟，我们无法在分配的短时间内涵盖响应功能的各个方面，但希望这能让您了解 AWS 上检测、调查和响应威胁和攻击的可用功能。

单元 4：回顾

在最后一个模块中，我们将进行简短的讨论，并讨论到底发生了什么。我们还会复习一些问题来测试你的知识。

体系结构概述

下面是整个实验的设置的示意图：



到底是怎么回事？

在研讨会的模块 1 中，您将设置基础结构的初始组件，包括 GuardDuty、Inspector、SecurityHub 等检测控件以及简单的通知和修正管道。有些步骤需要手动配置，但是您还运行了一个 CloudFormation 模板来设置一些组件。

在模块 2 中，您启动了第二个 CloudFormation 模板，该模板启动了本研讨会模拟的攻击。CloudFormation 模板创建了两个 EC2 实例。一个实例（名为恶意主机）附加了一个 EIP，该 EIP 已添加到 GuardDuty 自定义威胁列表中。尽管恶意主机与另一个实例位于同一个 VPC 中，但为了实现该场景（并防止需要提交渗透测试请求），我们将其视为在 Internet 上并代表攻击的计算机。另一个实例（名为受损实例）是您的 web 服务器，它被恶意主机接管。

在模块 3 中，您调查了攻击，修复了损坏，并为将来的攻击设置了一些自动修复。

以下是袭击中发生的情况：

1. 模块 2 CloudFormation 模板创建了两个实例。它们位于同一专有网络的不同子网中。恶意主机代表我们假装在互联网上的攻击者。恶意主机上的弹性 IP 位于 GuardDuty 中的自定义威胁列表中。另一个名为 convented instance 的实例表示被提升并转移到 AWS 的 web 服务器。

2. 尽管公司的政策是只应为 SSH 启用基于密钥的身份验证，但在某个时候，已在受损实例上启用了 SSH 的密码身份验证。此错误配置在由 GuardDuty 发现触发的 Inspector 扫描中标识。

3. 恶意主机对受损实例执行了强制 SSH 密码攻击。暴力攻击是为了成功而设计的。

4. 防范发现：未经授权 zedAccess:EC2/SSHBruteForce

5. SSH 暴力攻击成功，攻击者能够登录到受损实例。

6. 在 CloudWatch 日志（/threat-detection-wksp/var/log/secure）中确认成功登录。

1. 被破坏的实例还有一个 cron 作业，它会持续 ping 恶意主机，以根据自定义威胁列表生成一个 GuardDuty 查找。

   GuardDuty **Finding**：UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

2. 生成 API 结果的 API 调用来自恶意主机。这些调用使用来自在恶意主机上运行的 EC2 的 IAM 角色的 temp cred。由于连接到恶意主机的 EIP 位于自定义威胁列表中，因此生成了 GuardDuty 发现。

   GuardDuty Finding: Recon:IAMUser/MaliciousIPCaller.Custom or GuardDuty Finding: UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

3. 许多 CloudWatch 事件规则由 GuardDuty 发现引发，然后这些规则触发各种服务。

   a. **CloudWatch Event Rule**：GuardDuty 查找调用 CloudWatch 事件规则，该规则触发 SNS 发送电子邮件。

   b. **CloudWatch Event Rule**： SSH brute force attack finding 调用 CloudWatch 事件规则，该规则触发 Lambda 函数，通过 NACL 以及在 EC2 实例上运行 Inspector 扫描的 Lambda 函数阻止攻击者的 IP 地址。

   c. **CloudWatch Event Rule**：未经授权的访问自定义 MaliciousIP 查找调用 CloudWatch 事件规则，该规则触发 Lambda 函数以通过 NACL 阻止攻击者的 IP 地址。

清理

为了防止向您的帐户收费，我们建议清理创建的基础结构。如果你打算继续工作，这样你可以检查实验多一点，请记住做清理时，你完成了。这是很容易让事情运行在一个 AWS 帐户，忘记了它，然后累算费用。如果您在讲师指导的课程中使用此功能，则使用 AWS 事件引擎时，无需运行清理步骤。如果你是用自己的帐户运行这个。在删除 CloudFormation 堆栈之前，您需要手动删除一些资源。

1. 删除创建的 inspector 对象。

2. 删除受损 EC2 实例的 IAM 角色和 Inspector 的服务链接角色（如果尚未创建此角色）。
3. 删除由模块 1 CloudFormation 模板创建的所有三个 S3 bucket（**threat-detection-wksp** 开始，以-data、-threatlist 和-logs 结束的 bucket）
4. 删除模块 1 和 2 CloudFormation 堆栈

在删除第二个堆栈之前，不需要等待第一个堆栈被删除。

5. 删除 GuardDuty 自定义威胁列表并禁用 GuardDuty（如果在研讨会之前尚未配置）。
6. 禁用 AWS Security Hub
7. 删除您创建的手动 CloudWatch 事件规则和生成的 CloudWatch 日志。
   Rules: **threat-detection-wksp-guardduty-finding-maliciousip**

   Logs: **/aws/lambda/threat-detection-wksp-inspector-role-creation.**

   重复：
   /aws/lambda/threat-detection-wksp-remediation-inspector
   /aws/lambda/threat-detection-wksp-remediation-nacl
   /threat-detection-wksp/var/log/secure
8. 删除订阅 SNS 主题时创建的 SNS 订阅：threat-detection-wksp。

完成了！恭喜您完成本次研讨会！