Graylog Security

利用先进的 SIEM 技术增强您的网络安全

Graylog Security, 以自管理或SaaS体验的形式提供，是一个可扩展的网络安全解决方案，结合了安全信息和事件管理 (SIEM)，、威胁检测和事件响应（TDIR）、威胁情报、事件调查和异常检测功能，帮助安全专业人员简化对网络威胁的识别、研究和响应。

正确的SIEM

资源受限的组织需要经济实惠且主动的威胁检测、事件分析和响应以及合规性报告来加强其安全态势。Graylog Security基于Graylog平台构建，结合了企业日志管理、威胁检测、推荐补救步骤以及易于部署、管理和使用的报告。我们的安全平台旨在提供您所需的功能，同时又无需传统SIEM解决方案的复杂性和成本。

Graylog Security概览

以安全为中心的用户界面

Graylog Security独特的以安全为中心的用户界面可提高您的生产力和效率，该用户界面专为分析师量身定制，可快速访问调查、警报和报告工作流程。

Graylog Security 优势

- 利用闪电般的搜索能力在几秒钟内搜索大量数据
- 轻松追踪资产并快速识别问题或日志的来源
- 过滤警报噪音，将安全工作集中在重要的事情上
- 利用可靠的自动化技术提高重复性、安全性要求高的任务的生产力
- 利用随时间推移不断学习安全行为的异常检测机器学习引擎

基于风险的评分

通过基于风险的自动化评分关注“当前”风险。Graylog Security为单个警报分配风险评分，分析师可以轻松地确定安全事件的优先级。

用于取证分析和故障排除的闪电般快速搜索

当您试图保护您的环境免受网络威胁时，每一秒都至关重要。Graylog Security旨在在几秒钟内解析数太字节级的数据，让您实时找到重要的日志数据。通过简单的下拉菜单快速访问之前的查询历史。

有意义的异常检测

将不良行为者拒之门外，保持领先。Graylog Security异常检测功能采用强大的机器学习（ML）异常检测引擎，可以自动了解您的环境，提醒用户和实体的非正常行为（用户和实体行为分析）。

在大量警报中识别优先安全事件

排除干扰，快速获取所需数据并不困难。Graylog安全警报引擎可以轻松过滤噪音，让您可以专注于真正重要的安全事件，减少警报疲劳并最大限度地提高生产力。

事件调查专用工作区

使用Graylog Security中的一体化工作区从头到尾轻松管理事件调查，在调查潜在事件或问题时收集和组织数据集、报告、证据和其他背景信息，在整个调查过程中跨团队协作，并使用以前调查保存的数据快速识别趋势。

快速查找行为不当的资产

Graylog Security的资产模块允许您跟踪整个环境中的不同类型的资产，并使用其信息丰富日志消息。您可以通过Graylog UI轻松添加资产信息，或者通过LDAP或AD轻松同步。

精心组织的威胁覆盖

Graylog Security利用异常检测、西格玛规则、威胁情报和MITRE ATT&CK®框架等先进的网络技术帮助您检测整个环境中的威胁。

您降低风险的成效如何?

使用Graylog Security，通过衡量表示您降低风险的成效如何的关键安全KPI来了解您的网络弹性，让您知道改进措施的重点在哪里。

降低TCO并增强安全性

Graylog Security的云原生功能、直观的用户界面和开箱即用的内容意味着，与传统SIEM相比，您可以更快地从日志中获取有价值的数据。通过旨在显著减少警报疲劳、快速获得答案和增强安全专业人员能力的功能来降低您的劳动力成本。利用可以放置数据的“热”层，实现更便宜的远程或内部存储选项，同时提供同样快如闪电的强大搜索体验。

强大、闪电般的功能

异常检测/UEBA
能够快速学习“正常”行为并自动大规模识别用户和实体的偏差，并随时间推移不断进行微调和改进。

资产充丰富
通过跟踪不同的资产并使用附加信息丰富日志消息的能力，深入了解您的环境。

合规报告
利用Graylog的仪表板功能轻松构建和配置计划报告。

关联和警报
通过电子邮件、短信、Slack等接收警报。根据查找表中的动态列表更新警报标准。

数据规范化和丰富
通过添加WHOIS、IP地理位置、威胁情报或其他结构化数据来执行更快的研究。

Graylog用户日志
跟踪谁访问了哪些日志数据以及他们对其采取了哪些行动，以确保合规性和安全性。

事件调查
在调查潜在事件时用于收集和组织数据集、报告、证据和其他背景信息的一体化工作区。

预建仪表板、警报
使用针对安全用例的预构建内容快速开始 — 搜索模板、仪表板、相关警报、动态查找表等。

搜索查询生成器
构建任何分析类型的多个搜索并将其合并为一个操作，将结果导出到仪表板。

安全分析仪表板
组合小部件来构建定制数据显示并自动将报告发送到您的收件箱。

SOAR集成
轻松与其他业务关键系统共享数据，实现完全的透明度和协作。

威胁情报源
使用现有的威胁情报源为事件日志数据添加背景信息并查明潜在的安全问题。

graylog SECURITY

咨询我们的专家并了解Graylog Security的运行

眼见为实。在Graylog，我们希望您在购买之前就能得到所有问题的答案。我们提供定期产品演示，以展示产品功能并留出时间进行问答。立即安排您的Graylog Security演示，亲眼见证我们的强大网络安全平台的运行。

Graylog Security 可让您深入了解数万个网络组件之间的事件关联，以识别威胁或可疑活动。

关于Graylog

Graylog是日志管理和安全信息事件管理（SIEM）领域的领导者，致力于让世界及其数据更加高效和安全。Graylog由从业者构建，切实为从业者考虑，为每天解决安全、合规、运营和DevOps问题的数千名IT和安全专业人员从数据中获取答案。Graylog是一个屡获殊荣的平台，已在全球超过50,000个设备中部署，旨在快速、大规模地捕获、存储和实时分析太字节级的机器数据。Graylog 通过使用更具成本效益和灵活性的架构快速高效地进行数据分析、威胁搜寻、检测和事件调查，消除了噪音并提供卓越的用户体验。

www.graylog.org
info@graylog.com | 1301 Fannin Street, Suite 2000, Houston, TX 77002

graylog