paloalto NETWORKS | CORTEX XSIAM

XSIAM 买家指南：

如何面向 AI 时代改造 SOC

目录

弥合差距：
现代 SOC 的主动预防

网络安全形势正在迅速演变，给企业带来了前所未有的挑战。当今的威胁行为者更加诡计多端，使用先进的技术和 AI 绕过传统的安全措施。作为一名安全专业人士，您可能正在亲身经历安全运营中心 (SOC) 的需求发生了怎样翻天覆地的变化。在当今时代，数据泄露可能仅在数小时内发生（相比一年前需要 24 小时的攻击时长已大幅缩短[1]），同时监管要求也日益严苛，传统的威胁检测与响应方式已力不从心。

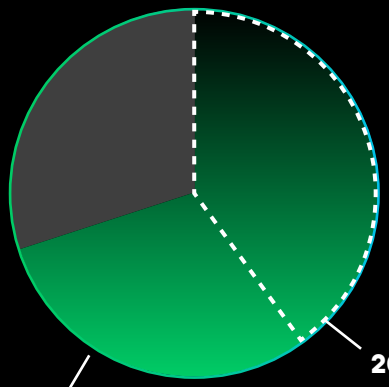
每当发生入侵时，安全团队都可能在事后拼凑出事情发生的经过 — 系统是如何被攻破的、涉及哪些系统以及哪些数据被外泄。这就引出了一个问题：如果掌握了信息，可以了解入侵发生后的事件，那为什么不能在事件发生前就预防或阻止呢？事后分析与主动预防之间的差距正是现代 SOC 不断向前发展的核心需求。

传统的安全信息和事件管理 (SIEM) 解决方案曾经是许多安全运营的基石，但现在却难以跟上时代的步伐。您可能会发现，自己正在艰难应对复杂的配置、耗时的集成、检测工程方面的巨额投资以及难以承受的警报量。

多重勒索战术继续抬头

近年来，勒索软件攻击的格局发生了显著变化，多重勒索战术日益盛行。

勒索软件案件中的数据盗窃：[2]



2022 年末：
约占 70% 的案件

2021 年中：
仅占约 40% 的案件

调查事件数量增长

在 18 个月的时间里，勒索软件攻击期间发生的数据失窃事件增加了 75%。

1. *2025 Unit 42 事件响应报告*，Palo Alto Networks，2025 年 2 月 25 日。
2. *2023 年 Unit 42 勒索软件和勒索报告*，Palo Alto Networks Unit 42，2025 年 9 月 28 日。

这些挑战会让团队感到力不从心，也会让企业变得脆弱不堪。许多安全工具各自为政，导致工作流程效率低下，增加了分析人员的认知负担，还有可能忽视关键的威胁。更严重的是，主动式安全功能（如漏洞管理）与被动式响应工具之间缺乏集成，不仅阻碍实时威胁检测，还会延迟事件响应，使企业暴露于风险之中。

此外，主要依赖静态关联规则和广泛的检测工程，再加上庞大的数据量，很难识别整个环境中安全事件之间的有意义关系，从而导致威胁防御不充分。这通常会导致警报显示为互不关联的数据点，使得 SOC 团队不得不进行手动关联，导致高误报率。这种脱节的流程会妨碍安全基础设施的效果，凸显出对更先进、适应性更强的威胁检测方法的需求。

量化成效：SOC 转型的真实投资回报

Palo Alto Networks 委托 Forrester® Consulting 开展的总体经济影响™研究表明，采用 Cortex XSIAM® 的典型企业实现了以下关键业务指标：[3]

257% | 560 万美元 | < 6 个月

三年投资回报率 | 净现值 | 投资回收期

85% | 70% | 310 万美元

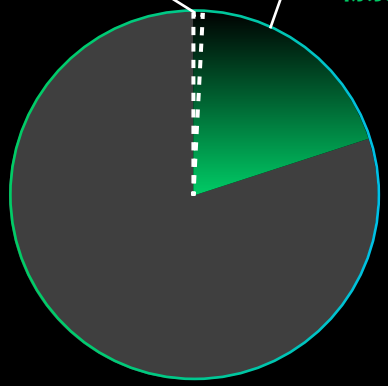
平均修复时间缩短 | 需 SOC 调查事件减少 | 工具整合节省成本

多重勒索战术继续抬头（续）

利用骚扰作为敲诈战术：[4]

2021 年中：
出现在不到 1% 的案件中

2022 年末：
出现在约 20% 的勒索软件案件中



1,900% 增长

同期，勒索软件团伙对骚扰战术的使用增加了 1900%。

这些统计数据凸显了勒索软件战略的重大转变，威胁行为者越来越多地利用多个施压点来敲诈受害者。数据窃取和骚扰战术都在急剧增加，凸显了企业面临的勒索软件威胁的复杂性和严重性正在不断演变。

3. *Palo Alto Networks Cortex XSIAM 的总体经济影响™*，Forrester Consulting，2025 年10 月 13 日。
4. Palo Alto Networks Unit 42，*2023 年 Unit 42 勒索软件和勒索报告*。

安全运营转型

SOC 转型始于 Cortex® 扩展数据湖 (XDL)——这一可扩展的、支持 AI 的平台化安全运维基础架构。作为安全运维中心的唯一可信数据源，Cortex XDL 能够集成、标准化并增强所有安全数据。

在此基础之上，Cortex XSIAM 将关键安全功能整合至统一的变革性平台，主要包括：

- 安全信息及事件管理 (SIEM)
- 端点检测和响应 (EDR)
- 扩展的检测和响应 (XDR)
- 安全编排、自动化和响应 (SOAR)
- 攻击面管理 (ASM)
- 用户和实体行为分析 (UEBA)
- 身份威胁检测和响应 (ITDR)
- 云检测与响应 (CDR)
- 威胁情报管理 (TIM)
- 威胁情报平台 (TIP)

> 通过 XSIAM，我们可以提高可视性并加快调查速度。无缝数据接入与自动化设置带来变革性突破。
>
> – Mike Dembek
> Boyne Resorts 网络架构师

图 1. XSIAM 指挥中心

Cortex XSIAM 将数据、AI 助力的防御和自动化集中在一个平台上，从而颠覆了安全运营。XSIAM 指挥中心可展示端点和网络、身份、云、应用程序遥测等一系列数据源，同时提供了对数据摄取的健康状况和总量的洞察。

这种整合使您不再需要在多个工具之间切换，从而降低了复杂性，提高了团队的工作效率。您可以通过一个专为满足现代 SOC 需求而设计的统一平台来管理整体安全运营，不必在各种控制台之间穿梭，也不必为集成问题而苦恼。

部署 Cortex XSIAM 的企业已获得显著成效。根据 Forrester 的总体经济影响™ 调研结果，一个典型企业在第三年实现了以下成果：**需一级 SOC 关注的告警量减少 85%**，在事件分级和一级运营方面节省超过 **93 万美元**成本；**需安全运维团队调查的事件量减少 70%，平均修复时间 (MTTR) 缩短 85%**，价值超 **120 万美元**。[5]

XSIAM 流线化的智能体 AI 和自动化功能从根本上改变了您处理安全事件的方式。平台实现了数据整合、分析和分流的自动化，大大减少了分析人员的手动工作量。这种自动化可以让团队专注于重要的事情——解决需要人类专业技能的高优先级事件。

XSIAM 开箱即用的 AI 模型超越了传统方法，可以连接各种数据源中的事件，在单一位置提供事件和风险的全面概览。通过利用警报分组和 AI 驱动的事件评分，XSIAM 可以无缝连接低置信度的事件，将其转化为高置信度的事件。这种优先级划分基于整体风险，使安全团队能够高效集中精力。

XSIAM 平台可以确保持续收集、拼接和规范化原始数据，而不局限于警报。这使 SOC 团队拥有卓越而简化的调查能力，使其能够更快、更有效地识别和补救威胁。

有了 Cortex XSIAM，您会发现分析人员的体验和工作效率都有了显著提高。平台的 AI 驱动方法有助于排除干扰，减少警报疲劳，使团队能够专注于关键的威胁。这种转变意味着分析师将更少的时间用于例行警报分流，而将更多的时间用于发展技能、进行深入调查和主动猎取威胁。

此外，XSIAM 自动化驱动的方法加快了事件补救的速度。凭借 Cortex Marketplace 中数百个经过验证的内容包，以及原生的 MCP 服务器与客户端支持，您可以轻松连接整个安全生态系统，实现威胁洞察集成与响应编排。通过将以前的手动任务自动化，嵌入式自动化可节省应对事件或管理风险（如攻击面暴露）所需的时间和精力。

您可以根据具体需求灵活添加、定制或修改自动化功能。剧本可定时执行、按需启动或由告警自动触发，确保响应及时并管控风险。

当需要调查威胁时，Cortex 智能体助手将为您调遣 AI 智能体团队应对各类安全挑战。该功能深度集成于 XSIAM 平台，通过 Cortex AgentiX™ 智能体规划执行高级工作流——将繁琐人工操作转化为即时专家级响应。您的团队将获得具备情境感知的分步指导与内置控制功能，加快响应速度，做出果断决策，确保业务安全。

Cortex AgentiX 提供基于真实专业知识的角色化 AI 智能体，成为团队成员的效能倍增器。这些智能体具有十余年安全自动化领先技术积累，全球威胁情报赋能，基于 12 亿次执行的剧本经验，发挥持续运作的安全专家级能力。分析师只需使用自然语言指令，智能体就能快速精准地规划和执行复杂的多阶段任务。

5. Forrester Consulting，*总体经济影响™*。

为自己的企业评估 CORTEX XSIAM

在为企业考虑 Cortex XSIAM 时，必须评估几个关键因素。首先，评估安全工具的现状及其复杂性。若您正疲于应对工具泛滥及主动防护与被动响应功能间的流程割裂问题，XSIAM 的整合方案将带来显著效益。考虑一下团队在不同工具之间切换和手动关联信息上浪费了多少时间。XSIAM 统一平台能大幅降低此类运维负荷，显著提升团队运营效率。

其次，考虑企业处理的数据总量和数据种类。XSIAM 擅长处理和分析大量多样化的数据，因此特别适合环境复杂、拥有丰富数据的企业。如果您正在面对内部数据与云数据混合的局面，苦于无法全面了解安全态势，那么 XSIAM 从各种来源摄取和分析数据的能力可能会改变游戏规则。

如果企业在云环境或混合环境中运营，XSIAM 的云原生架构以及跨内部部署和云资产的全面可视性可以显著增强您的安全运营。许多企业都发现，自己的传统安全工具难以在云环境中提供充足的可视性和保护。XSIAM 将 SOC 扩展到云，确保整个基础设施的统一可视性和安全运营。

第三，审查合规性要求——这也是关键考量因素之一。XSIAM 强大的报告功能和全面的数据分析可以帮助您更有效地满足各种监管标准。考虑一下团队目前在合规报告上花费了多少时间，以及 XSIAM 如何精简这个流程。

与传统的 SIEM 和其他安全平台相比，XSIAM 通过其 AI 驱动的方法提高了威胁检测能力。由于整合了工具并提高了效率，您可能会看到运营复杂性有所降低，而且有可能显著节约成本。在评估投资回报率时，不仅要考虑直接成本，还要考虑到分析人员腾出时间和改进安全态势带来的价值。试想一下，有了 XSIAM 的自动分流和响应功能，团队能够以多快的速度检测和应对威胁。

Forrester Consulting 的总体经济影响™ 研究记录了实际财务收益。研究发现，采用该解决方案的企业**在三年内实现了 257% 的投资回报率**，且**投资回收期不足六个月**。正如一位全球安全副总裁在研究中所言：“平均检测与修复时间缩短了 80% 以上。过去需要 4 小时检测加 2 小时修复的流程，现在总共只需 40-50 分钟。”[6]

> “Cortex XSIAM 颠覆了我们的安全运营方式，这是我们以前的 SIEM 无法做到的。XSIAM 为我们的检测、调查和响应工作流程开启了自动化和编排 — 这对 LOLC 的生产力和安全态势来说是一个巨大的改进。
>
> - Prasanna Siriwardena
> LOLC Holdings PLC 首席信息官

6. Forrester Consulting，*总体经济影响™*。

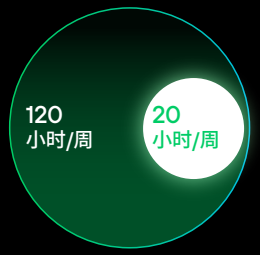
相比于仅凭 SIEM 解决方案，看看 XSIAM 带来的改进

节省时间：传统 SIEM 与 XSIAM

SIEM XSIAM

威胁检测开发

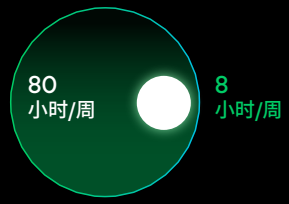
持续创建适应威胁态势变化的警报的流程。



100
小时/周（节省）
将大部分威胁检测开发外包给 XSIAM 研究团队。

警报调整

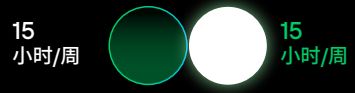
持续基于历史可信度优化警报的流程。



72
小时/周（节省）
将端点警报调整外包给 XSIAM 研究团队。

系统维护

日志解析、服务器补丁更新等



无更改

分析

通过复杂统计数据和机器学习创建高级警报。

SIEM

[功能漏洞]
需搭配附加组件包及 BYOML 模型使用。规范化十分艰难。

XSIAM

[新功能]
XSIAM 通过统计和机器学习实现自动基准和异常警报。

节省时间的结果：

4.5 FTE
减少总体工作量

图 2. XSIAM 相比于传统 SIEM 节省的时间

在采用 XSIAM 之前，需评估企业是否为 AI 驱动的安全运营做好了准备。考虑一下团队当前的技能和流程，为转变安全运营方式做好准备。

虽然 XSIAM 可以大大改善安全运营，但可能需要对团队的工作方式进行一些调整。在采用 AI 驱动的新平台时，考虑一下培训和变更管理方面的问题。

让安全运营永不过时

Cortex XSIAM 在零信任架构、安全访问服务边缘 (SASE) 以及安全服务边缘 (SSE) 等安全范式的演进中发挥着关键作用。其全面的可视性和高级分析功能与这些现代安全方法相得益彰，让安全运营面向未来，永不过时。在企业向零信任架构迈进的过程中，XSIAM 能够深入洞察用户和实体的行为，帮助实施和维护稳健的零信任模型。

该平台实现了主动式安全态势管理与被动事件响应的有机统一，通过以下核心能力应对企业最关键的两大风险领域：

- **Cortex 风险暴露管理：**借助 AI 驱动的优先级评估及覆盖企业本地与云环境的自动化修复，将漏洞噪声降低高达 99%。这一突破性方案专门针对那些存在现成武器化漏洞利用且缺乏补偿控制措施的高危漏洞，使企业能够精准锁定真正关键的 0.01% 威胁。
- **Cortex 电子邮件分析：**结合大语言模型分析与行业顶尖的检测响应技术，有效拦截高级钓鱼攻击和邮件渗透。考虑到邮件作为主要通信工具（预计 2030 年用户将达 50 亿[7]）且长期位居网络攻击首要目标，该功能可实时清除恶意邮件、禁用沦陷账户并隔离受影响终端。

随着企业的发展和威胁的演变，XSIAM 的可扩展性确保其能够应对不断增加的数据量并适应新型威胁。平台的 AI 模型和检测器不断更新，可提供最新的威胁情报和检测能力，无需团队进行手动更新。这意味着您始终可以防范最新的威胁，无需不断手动调整和更新自己的安全工具。

XSIAM 还能从分析师的手动操作中学习，并为未来的自动化操作提供建议。这显著增强了平台自动处置安全事件的能力，并持续优化响应效率与精准度，从而推动企业的安全防护水平实现日臻完善的良性演进。

XSIAM 利用成熟的安全专用 ML 数据模型，自动规范和拼接各种来源的海量数据，从而检测安全威胁。这些模型基于从数以万计的环境中学习到的行为而建立，有助于区分异常行为和恶意行为。这大大降低了误报率，提高了检测和预防能力，在攻击演变成安全事件之前就会将其阻止。

此外，XSIAM 的自带机器学习 (BYOML) 功能允许将自己的机器学习工具集成到平台中。这样，您就可以凭借 ML 的强大力量，使用 XSIAM 中的集中化和规范化数据来捕猎威胁，从而进一步提高检测和应对复杂威胁的能力。

整合的经济效益

根据 Forrester Consulting 的 Palo Alto Networks *Cortex XSIAM 总体经济影响™* 研究报告：[8]

310 万美元
通过淘汰 20+ 个传统工具，企业在三年间累计节省了 310 万美元

220 万美元
安全态势 60% 的改善带来了 220 万美元的价值

560 万美元
三年净现值达到 560 万美元

通过采用 XSIAM，您即能解决当前的安全挑战，又能使企业满足未来的网络安全需求。面对不断演变的威胁形势，这种高瞻远瞩的方法可以让您对自己保护企业的能力充满信心。随着新型威胁的涌现，企业的 IT 基础设施需要不断成熟才能满足需求，而 XSIAM 灵活的 AI 驱动方法可以确保企业的安全运营能够适应并有效应对。

XSIAM 使 SOC 团队和企业的安全态势日臻完善。

也许最重要的是，XSIAM 通过 AI 和机器学习提供持续改进。平台根据新数据和新兴的攻击技术定期精进其检测和响应能力。这意味着，随着时间的推移，安全运营会变得更加行之有效，能够适应新的威胁和模式，无需不断进行手动调整。

7. *2025-2030 年电子邮件统计报告*，cloudHQ，2025 年 4 月 24 日
8. Forrester Consulting，*总体经济影响™*。

改善关键的 SOC 指标

Cortex XSIAM 提供了一种革命性的方法，可以缩短平均检测时间 (MTTD) 和平均响应时间 (MTTR)，显著增强您的安全运营。通过利用先进的 AI 和机器学习，XSIAM 可以自动完成单调乏味的数据整合和分析任务，使团队能够近乎实时地识别威胁。这意味着您可以比以往任何时候都更快地发现潜在的漏洞，往往能在攻击者对企业造成重大损害之前就将其抓获。

但是，检测只是成功的一半。XSIAM 以自动化优先的方法加快了事件响应速度，将数小时人工调查压缩为分钟级自动化响应。想象一下，SOC 团队不再受困于人工分流活动，也不再浪费宝贵的时间来关联来自不同来源的数据。借助 XSIAM 平台 AI 驱动的事件评分与警报分组能力，赋能分析师聚焦高价值威胁处置。

我们通过将被动式与主动式安全能力深度融合，不仅实现更快速的事件处置，更能从源头预防大量潜在攻击。XSIAM 将风险暴露管理与电子邮件分析直接集成至 SOC 平台，运用统一的数据模型、AI 与自动化技术，精准打击企业面临的两大最常见攻击途径。

随着团队利用高级剧本和 Cortex AgentiX 智能体对威胁实施快速精准打击，您会发现 MTTR 显著降低了。也许最重要的是，XSIAM 能够不断学习并适应环境，确保安全态势随着时间的推移不断改善。当您面临着不断涌现的新威胁时，XSIAM 尖端的 AI 模型会不断发展，使您领先潜在对手一步。

这意味着，您的安全运营不仅能够有效降低 MTTD 和 MTTR，更能为应对未来的安全挑战做好充分准备。有了 Cortex XSIAM，您就可以自信驾驭复杂的网络安全环境，因为您知道，自己的关键 SOC 指标正在不断优化，保护着企业最宝贵的资产。

研究数据印证了这些改进成效。某专业零售企业的安全运维总监表示，其季度告警量**从 25,000 条锐减至 4,500 条**。该研究基于客户访谈构建的典型企业案例显示，部署阶段**需 3 名全职人员在两个月内完成，后续年度维护仅需 0.5 名全职人员配置**。[9]

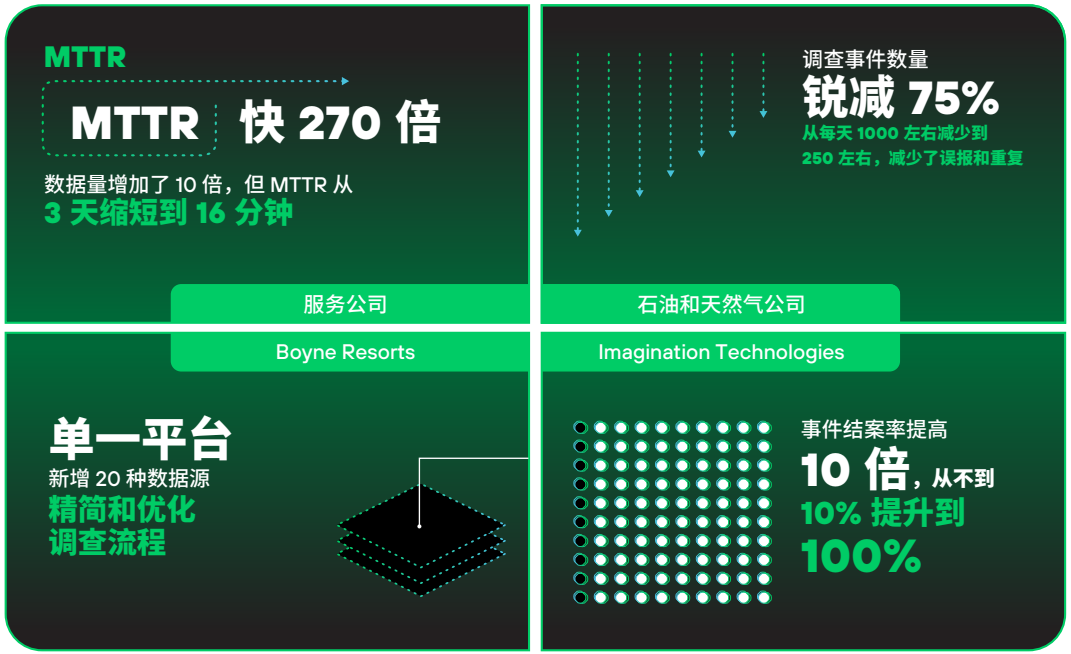


图 3. 客户借助 XSIAM 实现可量化改进的典型案例

> “我们将 XSIAM 视为迈向新一代 SOC 的下一个前沿，因为它将各种功能集成到了一个统一的平台中。有了 XSIAM，我们的网络运营团队有望获得更高的自动化程度，被赋予更强大的能力。
>
> - Rob Jillson
> Resolution Life Australasia 网络安全主管

9. Forrester Consulting，*总体经济影响*™。

CORTEX XSIAM 是适合您的解决方案吗?

1. 当前的 SOC 挑战

- ☐ 您是否正在为当前 SIEM 的复杂配置而苦恼?
- ☐ 您是否面临着安全工具之间耗时的集成?
- ☐ 大量的警报是否让您的团队不堪重负?
- ☐ 您的工作流程是否由于安全工具各自为政而效率低下?
- ☐ 您的主动防护机制与被动响应措施是否存在协同断层?

2. 威胁检测和响应

- ☐ 您是否严重依赖静态关联规则?
- ☐ 您是否需要改进实时威胁检测?
- ☐ 您的事件响应流程是否因缺乏集成而频频延迟?
- ☐ 您是否在为高误报率而苦恼?

3. 数据管理

- ☐ 您是否要处理大量多样化的安全数据?
- ☐ 您是否正在面对内部数据与云数据混合的局面?
- ☐ 您是否需要更好的数据规范化和关联能力?

4. AI 和自动化需求

- ☐ 您是否希望利用 AI 改进威胁检测?
- ☐ 您是否希望实现例行安全任务的自动化?
- ☐ 减少事件分流中的人工操作是否是当务之急?
- ☐ 您是否需要 AI 驱动的漏洞优先级研判来穿透警报噪音?

5. 统一平台需求

- ☐ 您是否需要整合多种安全能力，例如 SIEM、EDR、XDR、SOAR、漏洞管理与邮件安全?
- ☐ 您是否希望从单一平台管理安全运营?
- ☐ 您是否希望弥合主动防御与被动响应之间的协同断层?

6. 云和混合环境

- ☐ 企业是否在云或混合环境中运营?
- ☐ 您是否需要更好地了解内部资产和云资产?

7. 合规与报告

- ☐ 您是否需要精简合规报告流程?
- ☐ 您是否正在为监管标准寻找更全面的数据分析?

8. 可扩展性

- ☐ 企业是否正在成长，需要处理日益增长的数据量?
- ☐ 您是否需要一个能够适应威胁不断演变的解决方案?

9. 高级分析

- ☐ 您是否对 AI 驱动的事件评分和警报分组感兴趣?
- ☐ 您是否需要更好地关联各种数据源中的事件?
- ☐ 您是否希望借助 AI 精准研判关键漏洞优先级?

10. 团队准备

- ☐ 您的团队是否准备好适应 AI 驱动的安全运营?
- ☐ 您是否愿意为新的高级平台的培训投资?

11. 面向未来

- ☐ 您是否正在向零信任、SASE 或 SSE 安全模型迈进?
- ☐ 您是否需要一种通过 AI 和 ML 不断改进的解决方案?

12. 自定义 ML 集成

- ☐ 您是否有兴趣集成自己的机器学习工具?

13. 电子邮件和漏洞管理

- ☐ 您是否需要增强防护以应对高级电子邮件威胁?
- ☐ 您是否疲于应对漏洞积压和优先级排序?
- ☐ 您是否希望通过自动化修复关键漏洞来提升安全防护效率?

如果您对其中大部分的问题回答“**是**”，特别是在与企业的特定安全挑战和目标相一致的领域，那么 Cortex XSIAM 将是适合您的 SOC 的解决方案。

立即开始使用

了解 Cortex XSIAM 如何帮助企业简化安全运维、整合主动与被动式防御、实现大规模威胁拦截，并加速事件响应处置——从当下到未来持续提升安全运营效能。

联系我们 →

关于 Cortex XSIAM

Cortex XSIAM 是面向现代 SOC 的人工智能驱动型安全运营平台，利用人工智能的力量简化安全运营，大规模阻止威胁，并加快事件修复。通过将多种产品集中到专为安全运营而设计的一款高度整合平台中，降低风险和操作复杂性。

Cortex XSIAM 统一了行业最佳安全运营功能，包括 EDR、XDR、SOAR、ASM、UEBA、TIP 和 SIEM。XSIAM 集中所有安全数据，并使用专为安全设计的机器学习数据模型。借助 XSIAM，自动化数据集成、分析和响应操作，使分析师能够专注于重要的事件。要详细了解 Cortex XSIAM，请访问 www.paloaltonetworks.com/cortex/cortex-xsiam。

paloalto NETWORKS

联系我们：
请拨打咨询热线 400-9911-194
邮件：Contact_SalesChina@paloaltonetworks.com
www.paloaltonetworks.cn

关注派拓网络
官方微信公众号

cortex_ebook_cortex-xsiam-buyers-guide_102125