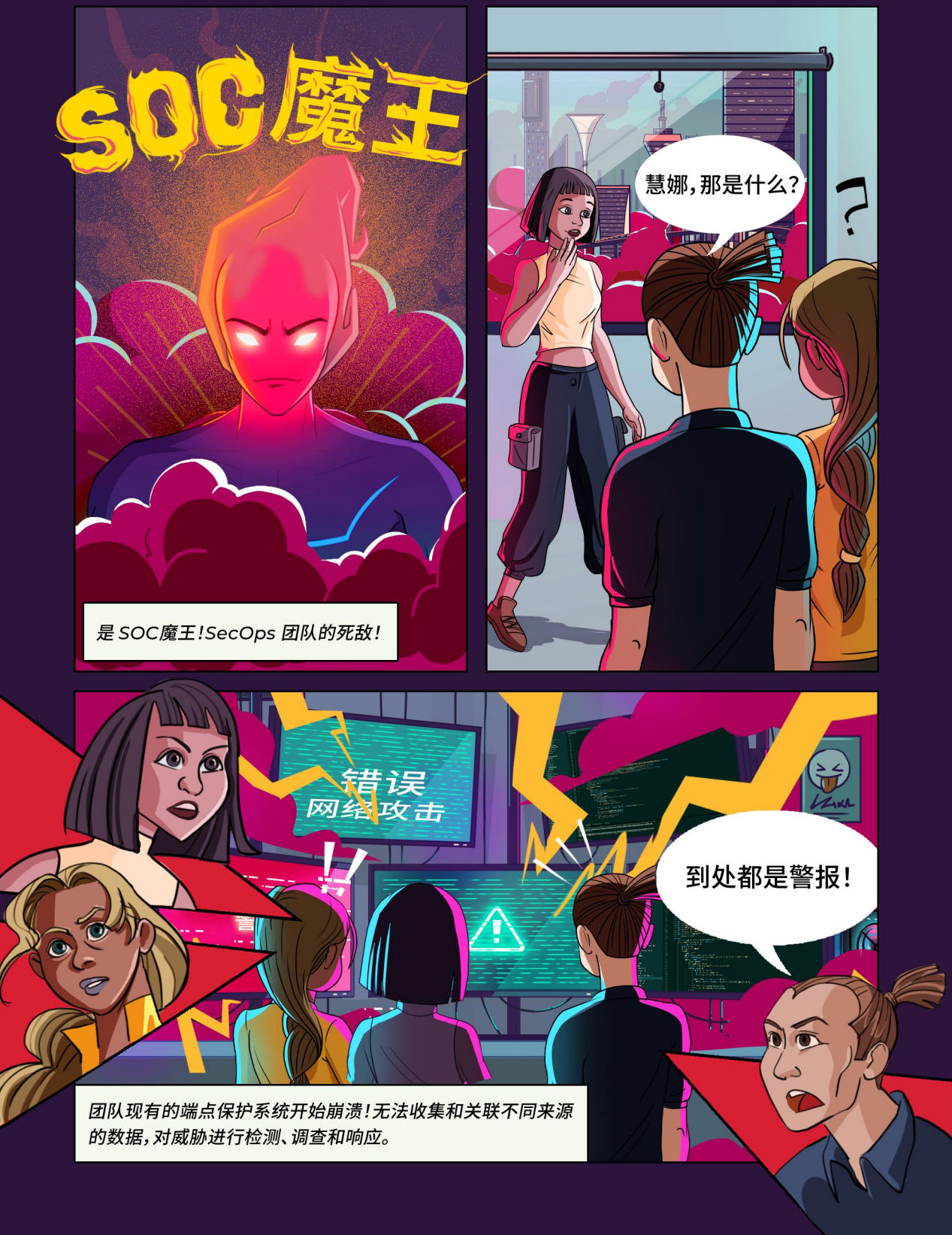
paloalto NETWORKS | CORTEX BY PALO ALTO NETWORKS

CORTEX CITY

SOC魔王 VS FUTURESOC的较量

第 1 期

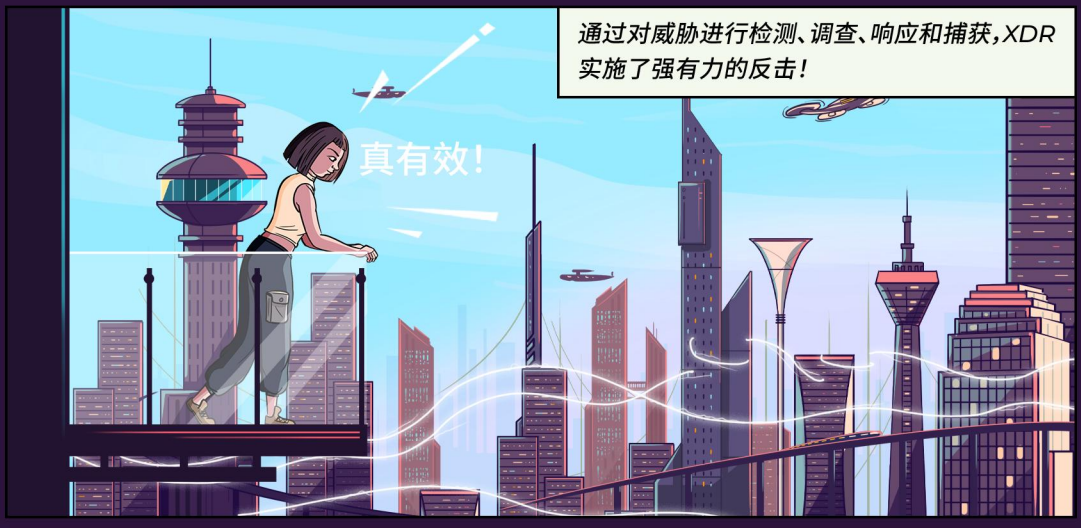

在一个清新、明朗的早晨，Cortex City熙熙攘攘，大家又开始了新的一天。
突然，不知从何而来的浓雾笼罩了整座城市，并遮盖了攻击面。这只能是…
!!


SOC魔王
是 SOC魔王!SecOps 团队的死敌!
慧娜，那是什么?
?
错误
网络攻击
到处都是警报!
团队现有的端点保护系统开始崩溃!无法收集和关联不同来源的数据，对威胁进行检测、调查和响应。

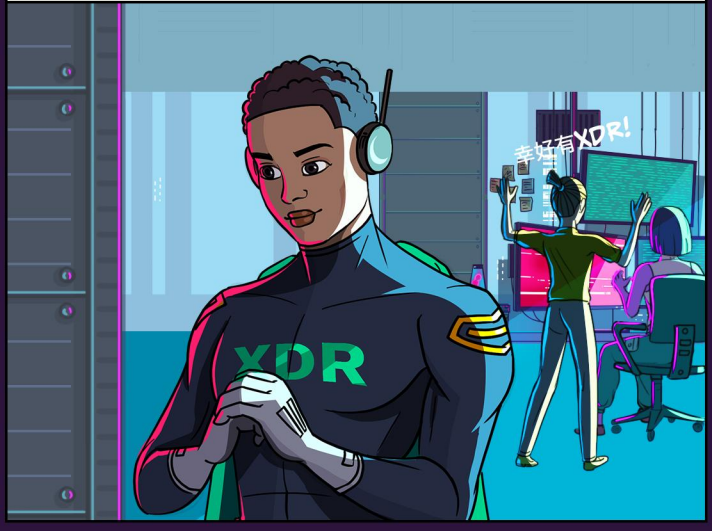

于是，慧娜快速呼叫最精锐的团队！求助帮忙抵御这次网络攻击…
FUTURESOC，
我们急需你们的帮助！
在FutureSOC总部…
XDR
该你出场了！
XDR
XDR立即采取行动，监控网络是否有任何入侵迹象并且迅速确定攻击源。
XDR

他对端点进行了分析，找到攻击点。然后给出了整座城市的攻击点视图。之后，他将相关的端点遥测和事件数据发送给 BigTech Inc.。

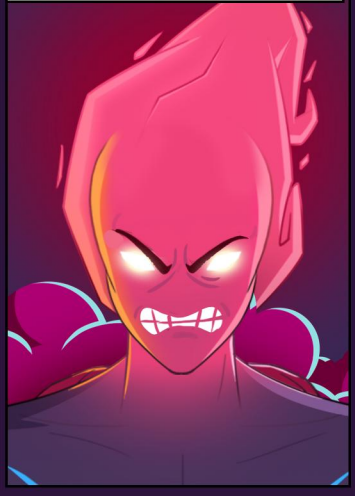
通过对威胁进行检测、调查、响应和捕获，XDR 实施了强有力的反击！



他在检测、响应和扩展到云环境方面实力超群，为慧娜的团队提供了抵御攻击所需的信息。

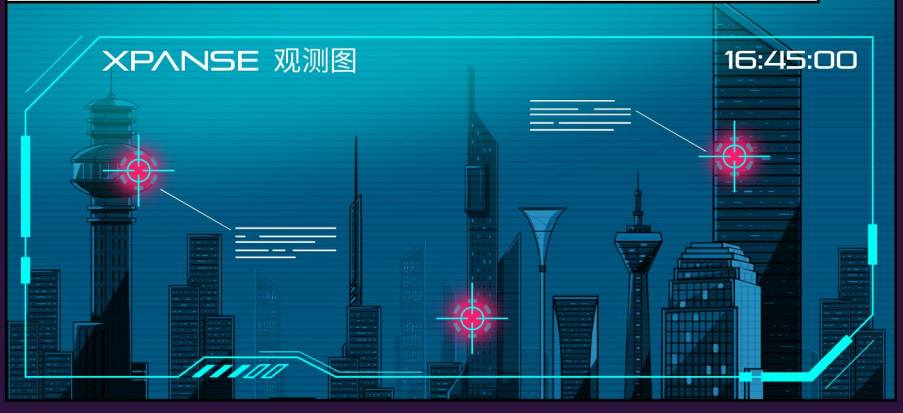


可别小看SOC魔王，他并没那么好对付！城里很多地方仍弥漫着危险之雾…



慧娜和 XDR 呼叫 FutureSOC 团队，寻求进一步保护。

Xpanse 抢在 SOC魔王之前找到了漏洞，并不断寻找资产，进行持续监控，主动降低风险。同时，将资产情况与由外而内的映射交联，然后…




她把所有信息汇集在一起，了解漏洞暴露和遭受新攻击的原因，及攻击的展开过程。此时，危险之雾已几乎驱散殆尽！
Xpanse
XSOAR 也前来协助 Xpanse 一臂之力，将危险彻底清除！
XSOAR
Xpanse
XSOAR

强力调查与响应

自动响应未来事件

跨部门协调行动

人工任务自动

与所有SOC工具兼

XSOAR 可立即从慧娜的工具中提取警报，获取有关端点、用户、主机、漏洞、恶意软件和攻击者情报的信息，进行即时遏制。

激活

XSOAR

XSOAR 成功驱散了危险之雾！整个攻击面逐步减少，并最终清除。这让慧娜及其团队得以重新监控全局！

呼哗！

击退 SOC魔王的攻击后，一切恢复如初。XSOAR 向慧娜和她的团队说明了如何增加自动化武器，抵御供应链攻击、国家级攻击和零日攻击。

FutureSOC团队则帮助BigTech Inc. 确定传入警报的优先级，并简化其工作流程，通过人工智能和机器学习加快修复速度。

他们之所以能取得成功，秘诀在于 Cortex 的全套组合产品。慧娜及团队借助端点安全、检测、响应、自动化和攻击面管理，不仅繁忙的工作减少了，甚至可以悠闲享受晚间和周末时光！

最终

利用网络、云和身份数据以及互联网暴露资产风险的单一数据源来准确检测威胁，慧娜及其团队甚至可以发现最隐秘的 SOC魔王攻击，并借助 SOC 的全部力量进行响应。

FutureSOC 团队证明，只要采用恰当的安全技术，即使是SOC魔王最新的威胁也能成功的抵御。

使安全事件具有全面可见性，并采取协调一致的响应，你也可以主动防御和保护网络和资产，打造美好未来。

我们欢迎你现在开始未来 SOC之旅！和 Cortex 一起应对云原生世界不断变化的需求。

请点击链接请求演示：
www.paloaltonetworks.cn/cortex/request-demo