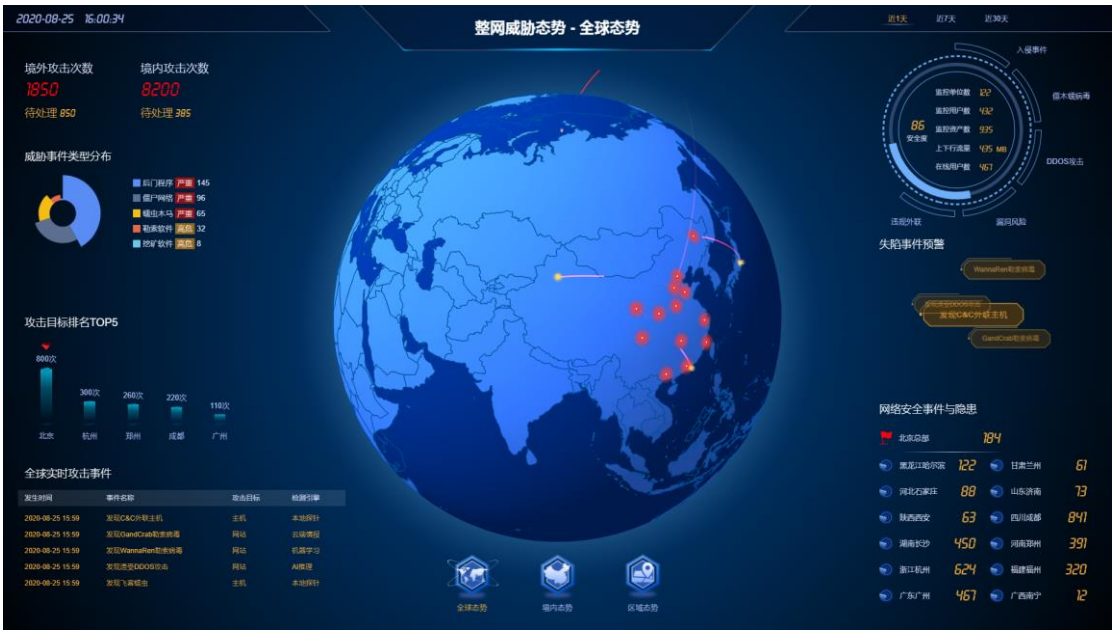
紫光安全分析与管理平台（UNIS SDOP）

产品概述

近年来，国内外网络攻击频繁，业务系统遭受攻击、勒索病毒爆发、大规模用户信息泄漏等问题，不断给我们敲响警钟。面对日益严峻的安全形势，紫光恒越顺势而为，推出紫光安全分析与管理平台（UNIS SDOP）。

紫光安全分析与管理平台是以安全大数据为基础，对能够引起网络态势发生变化的要素进行获取、理解、评估、呈现以及对未来发展趋势预测的一个过程；是从全局视角提升对安全威胁的发现识别、理解分析、响应处置的一种能力；是通过智能分析和联动响应，结合机器学习和人工智能，实现“安全大脑”的闭环决策，实现安全能力的落地实践，真正做到对安全风险威胁的“主动发现、预知未来、协同防御、智能进化”。

紫光安全分析与管理平台贯穿安全风险监控、分析、响应和预测的全过程，以威胁、风险、资产、业务、用户等为对象，基于安全日志、网络流量、用户行为、终端日志、业务数据、资产状态等多源数据，结合外部情报，通对全局状态评价、外部攻击评级等手段，实现“事态可评估”；通过对攻击趋势分析、异常流量判断和终端行为检测，实现“趋势可预测”；通过对未知威胁的智能检测识别、流量/行为/资产的状态监控和多维度风险分析，实现“风险可感知”；通过对攻击溯源取证、云网端协同联动、工单流程闭环处理和设备策略自适应调整，实现“知行可管控”。



紫光分析与管理平台效果图

产品特点

◆ 多样化数据采集

- 支持各种网络设备、安全设备、主机及应用日志采集。
- 采用主动、被动技术实时采集网络中的异构海量日志；支持 SYSLOG 协议、HTTP/HTTPS 被动采集，FTP、数据库主动采集，部署代理等多样化日志接入。
- 支持海量日志集中存储或分布式存储，满足快速查询的海量日志的要求。
- 通过日志范式化和日志分类支持不同厂家日志与系统的快速适配。

◆ 基于 AI 的智能化威胁分析

- 内置多个 AI 分析场景，单独分析场景化威胁展示。
- 基于现有安全事件，依托攻防专家经验，关联资产、情报等多维信息，提供“专家级”推理分析。
- 引入监督学习、强化学习等 AI 人工智能算法，利用“知识大脑”推理检测已知及未知类型的复杂攻击，全面掌握规模群体性事件的感染路径。
- 建立行为基线，通过资产/用户的流量、动作等行为的偏离情况，判断各类异常行为。

◆ 全过程溯源取证

- 针对攻击全过程进行多维度分析，可视化绘制出完整的攻击链条。
- 对安全事件进行回溯和调查，主动对攻击过程进行抓包取证，提供完整攻击证据。
- 针对 NAT 应用场景，基于 IP 和时间段信息，追溯地址转换关系，并呈现对应的安全事件。
- 利用云端丰富的实时威胁情报和本地的网络行为、终端行为、文件信息，覆盖攻击的源头、手段、目标、范围等相关信息，对发现的未知威胁进行快速溯源和定性。

◆ 自动化编排与响应

- 根据发现的安全事件，自定义安全响应剧本，根据防护需要调整处置步骤。
- 响应处置动作类型多样，包括黑名单阻断、访问控制、告警、工单处置、用户下线、主机病毒查杀及隔离等操作。
- 不仅可以针对 FW、IPS、WAF、ACG 等常见安全设备进行调度，更可以对交换机、路由、无线 AP 等网络设备进行调度。

- 规范处置流程，提升安全管理水平。

◆ 漏洞全生命周期管理

- 主动扫描网络安全漏洞，支持第三方漏扫结果导入。
- 通过工单任务实现了漏洞加固任务的下发、审核、复验等功能。
- 支持漏洞加固任务处置状态跟踪，对超期未处理任务可进行短信提醒。
- 支持人工或工具的方式对漏洞进行复验，并根据验证结果自动同步漏洞当前状态。

产品功能

紫光安全分析与管理平台产品通过采集全网安全事件数据，结合云端威胁情报，对海量安全数据进行挖掘和关联分析，生成全方位的安全全景视图，使用户能够快速准确地掌握网络当前的安全态势，并以此为依据进行联动响应，形成闭环处理。

项目	功能
安全态势展示	整网威胁态势：支持全网威胁态势呈现，从全球、境内、区域多维度分析呈现
	外网攻击态势：支持实时监测外网对内网资产的攻击威胁态势
	资产态势：支持全网资产梳理，进行资产相关态势分析呈现
关联规则	实时关联分析：在一定时间窗口内对日志进行关联，实时的给出相关告警
	支持自定义关联规则
威胁告警	受到网络攻击后，可以通过短信和邮件等形式向用户进行告警
日志审计	对收到的各类日志进行审计
资产管理	支持资产、资产组：资产包括主机设备、网络设备、安全设备、中间件、数据库、应用系统
	资产管理：支持手工添加、导入，支持资产自动发现
安全编排及响应	支持安全处置编排，可自动下发并执行响应动作
报表	支持日报、周报、月报和自定义周期报告，支持基于区域、资产、资源事件类型、等级，自定义报告输出
权限管理	支持三权分立，用户登录时可以对用户进行本地和外部认证。
系统管理	支持系统状态监控包括服务节点监控和服务进程状态监控
	支持系统日志、操作日志管理

订购信息

紫光安全分析与管理平台可以根据实际需求按照平台授权、功能特性授权两部分进行选购。

◆ UNIS SDOP 紫光安全分析与管理平台标准版配置

- 选择平台授权

描述	备注
UNIS 紫光安全威胁分析平台软件授权函	必配

- 根据需求选择功能特性授权

描述	备注
UNIS 紫光安全威胁分析平台软件威胁情报一年更新升级授权函	选配
UNIS 紫光安全威胁分析平台软件威胁情报三年更新升级授权函	选配
UNIS 紫光安全威胁分析平台软件定制化开发授权函	选配

◆ UNIS SDOP 紫光安全分析与管理平台增强版配置

- 选择平台授权

描述	备注
UNIS 紫光安全威胁分析平台增强版软件授权函	必配
UNIS 紫光安全威胁分析平台增强版分布式日志采集器授权函	必配

- 根据需求选择功能特性授权

描述	备注
UNIS 紫光安全威胁分析平台增强版流量及行为组件授权函	选配
UNIS 紫光安全威胁分析平台威胁情报一年更新升级授权函	选配
UNIS 紫光安全威胁分析平台威胁情报三年更新升级授权函	选配
UNIS 紫光安全威胁分析平台增强版定制化开发授权函	选配

紫光恒越技术有限公司

北京基地
北京市海淀区中关村东路 1 号院 2 号楼 402 室
邮编：100084
电话：010-82054431
传真：010-82054401

www.unisyue.com

客户服务热线
400-910-9998