面向工业企业综合
安全的 XDR 平台

卡巴斯基工业网络安全

kaspersky 引领未来

ICS 和工业企业面临的网络威胁

被恶意软件攻击

自 2023 年初以来，约 35% 的与 ICS 相关的计算机受到恶意软件攻击，比上一年减少了近 5%。

卡巴斯基 ICS CERT，2023 年 10 月

了解更多

工业基础设施所有者和运营者面临的新现实是，黑客对自动化系统的兴趣日益浓厚、监管要求高、IT-OT 融合以及各种工业领域 网络攻击的兴起（根据卡巴斯基 ICS CERT 的统计数据，与 2022 年下半年相比，2023 年上半年的网络攻击数量增长了近 50%）。

数字技术的渗透通常被认为是 一件好事，它消除了 IT 和 OT 环境之间的差距，可以保护 OT 环境免受网络犯罪分子的侵害。将闪存驱动器带入 ICS 环境可能会严重影响公司的核心业务，同时有动机的黑客组织可以渗透到 OT 网络并造成相当大的破坏，和/或窃取有价值的信息。再加上自动化标准从共同建议发展到立法要求，以及分享最佳实践和管理风险的呼声越来越高，这使得工业企业的网络安全成为一项艰巨的挑战。

卡巴斯基 ICS CERT 预计，来自 以下行业 的组织将面临越来越频繁的网络攻击：

APT 攻击的主要目标包括：

关键基础设施所有者和运营者
具有重要战略意义的政府或公共组织面临运营干预带来的更大的潜在后果

高知名度的行业参与者
从单个工厂到全国性或国际规模的公司，它们从事的都是事件成本高昂的高风险业务

石油、天然气和化工

这些企业控制着高价值数据和系统，因此成为勒索软件和试图破坏运营或操纵价格的恶意行为者的诱人目标。

高端工业制造

这些企业扮演着重要的社会角色，并拥有可用于获取经济利益的宝贵数据，一旦泄露，将会导致巨大的经济和声誉损失。

矿产、金属与采矿业

矿产、金属和采矿业因其宝贵的资源、金融影响和相互关联的供应链而成为目标。

电力、电网和公用事业

电力、电网和公用事业在我们日常生活中具有举足轻重的作用，这也是犯罪分子发起意在制造混乱或施加影响的攻击的主要原因。

详细了解 针对工业组织的常见 TTP 攻击

了解更多

生产经营过程的稳定，以及宝贵资产的保护，直接关系到工业企业和关键基础设施的可持续发展。针对工业系统，特别是 ICS 和 SCADA 的攻击正在增加。与此同时，传统解决方案似乎无法防御针对工业环境的现代网络威胁。

选择一个值得信任、对工业与企业网络安全之间的重叠领域有深入的了解，并且有能力提供全方位尖端安全技术的合作伙伴变得前所未有地重要。

高级 ICS 安全技术

通过 KICS XDR 平台，用户可以看到更全面的情况，并获取更广泛的背景信息：网络和端点级别的事件链、精确的资产参数、网络通信以及拓扑图（甚至是来自尚无法提供流量镜像的分段）等。

卡巴斯基工业网络安全 (KICS) 是一个面向工业企业的本地扩展检测与响应 (XDR) 平台，经过专门设计和认证，用以保护关键的 OT 设备、资产和网络免受网络威胁。该平台包含集成技术，确保核心工业自动化和控制系统组件在各个层面上的安全。卡巴斯基工业网络安全解决方案 - 节点安全 (KICS for Nodes) 是一款提供合规审核和端点传感器功能的端点保护、检测和响应软件。卡巴斯基工业网络安全解决方案 – 网络安全 (KICS for Networks) 用于 OT 网络流量分析、检测和响应。该平台集成了站点级集中管理功能，这对于将 OT 安全运营扩展到大量大型、多样化和地理分布式工业基础设施至关重要。

平台组件无缝集成，帮助用户全面了解多个异地分布的 OT 网络和自动化系统，从而提升客户体验、情景感知能力和部署的灵活性。通过扩展检测和 响应，KICS 平台实现了 IT-OT 融合，并提供了许多单一供应商的优势。

端点传感器

- 保护状态
- 安全审核
- 网络通信
- 主机遥测传输
- 设备监控
- 事件响应

卡巴斯基工业网络安全解决方案-节点安全

增强了 EDR 的端点保护

- 服务器
- 工作站
- 便携扫描仪

卡巴斯基工业网络安全

统一控制台
本机集成
跨产品场景
常见攻击链
风险和资产管理

卡巴斯基工业网络安全解决方案-网络安全

保护工业设备免受网络威胁

- 服务器
- 传感器

响应措施

- 主机隔离
- 执行预防
- 隔离

平台应用程序点

融合
OT 和 IT 环境

IT 环境

DMZ / GTW

OT 环境

卡巴斯基工业网络安全解决方案-节点安全

操作员工作站

SCADA 服务器

工程师工作站

ICS 网关

网络设备

SPAN

卡巴斯基工业网络安全解决方案-网络安全

舱室控制单元 (BCU)

智能电子设备 (IED)

可编程逻辑控制器 (PLC)

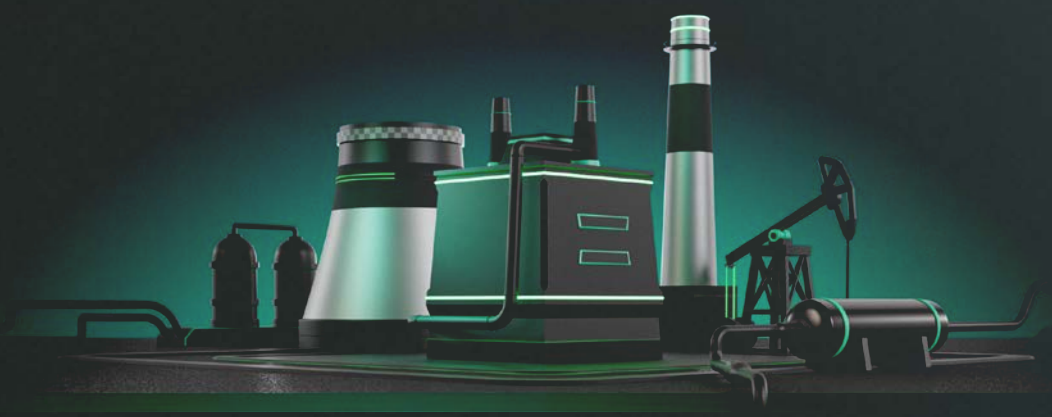
继电保护及安全仪表系统 (SIS)

独立节点
(使用 KICS 便携式扫描仪手动检查)

早期异常
检测和预测分析

卡巴斯基异常检测机器学习（卡巴斯基 MLAD）是一种创新的系统，使用神经网络同时监控各种遥测数据。它会检测设备故障和人为错误，帮助防止故障和事故，识别非典型的员工行为或 设备操作并据此预测专门攻击或 破坏，还会将异常检测与 设备状态和生命周期的预测分析相结合使用。

物理层



了解更多

由卡巴斯基产品提供安全防护

卡巴斯基工业网络安全解决方案-网络安全

卡巴斯基工业网络安全解决方案 – 网络安全 (KICS for Networks)

用于工业网络监控和 流量分析的专有协议级解决方案，作为软件或虚拟设备提供。

卡巴斯基工业网络安全解决方案 – 网络安全 (KICS for Networks) 在早期阶段识别 ICS 中的异常和入侵，显示攻击如何通过网络和节点 (EDR 攻击链和遥测) 发展，并确保采取必要措施防止对工业流程产生任何负面影响。

该解决方案有助于根据来自漏洞和网络连接的数据以及各种资产的角色来检测风险并进行排序，以防止事件发生。

优点

资产清查

自动资产清查和数据收集采用
被动和主动的数据收集方法

网络清查和可视化

- 网络通信地图
- 网络拓扑图

漏洞和风险评估

- 特定于 OT 的漏洞和 风险 管理
- 自动评分和设定优先级
- 风险补救建议

网络异常检测

网络完整性控制，
包含基准偏差监测和检测
恶意和可疑的网络活动

OT 过程控制和深度数据包检查 (DPI)

- 工业有效载荷数据提取
- 实时过程控制
- 工业命令控制
- 卡巴斯基 MLAD 提供的高级 OT 过程监控

集成和数据交换

- 集中式信息
- 与卡巴斯基和第三方或客户系统 (IEC 104、OPC、CEF、Syslog 和基于 API 的 连接器) 集成

集中合规工业网络节点审核

卡巴斯基工业网络安全解决方案 – 网络安全 (KICS for Networks) 提供集中的工业网络节点审核，包括基于代理的 (通过卡巴斯基工业网络安全解决方案 – 节点安全) 和无代理的网络硬件和端点漏洞审计，以及对 OVAL* 和 XCCDF** 行业标准的遵从性审计。

- 自动对 Windows、Linux 节点和网络设备执行集中安全审核
- 合规性审核。用于合规性检查和参数的全功能编辑器
- 所有报告和资产数据都在一个位置 – 卡巴斯基工业网络安全解决方案 – 网络安全 (KICS for Networks) 资产库
- 受保护的节点凭证库
- 支持任何第三方或自定义的 OVAL 数据库
- ICS CERT 提供的内置 SCADA 漏洞数据库

* 开放式漏洞评估语言 (OVAL)
** 可扩展配置清单描述格式 (XCCDF)

卡巴斯基工业网络安全解决方案 – 节点安全 (KICS for Networks)

卡巴斯基工业网络安全解决方案-节点安全

工业级、经过测试和认证的端点保护、检测和响应。适用于 Linux、Windows 和独立系统的影响小、兼容且稳定的解决方案。

卡巴斯基工业网络安全解决方案 – 节点安全 (KICS for Nodes) 为现代化、数字、托管式和分布式自动化系统的每个端点提供保护。该解决方案收集遥测数据，从而以清晰、详细且直观的方式显示安全事件在工作站、服务器、网关和其他端点上的进展情况，确保事件得到妥善处理且不会再次发生，令自动化系统管理员安心无忧。

卡巴斯基工业网络安全解决方案 – 节点安全 (KICS for Nodes) 便携扫描仪在无法安装安全软件的独立机器、自动化系统或设备上实施网络安全策略。它占用的空间非常小，不会干扰现有的安全解决方案。

- 无需安装的解决方案，即使是独立的基础设施，也能提供最终的情境感知和 OT 可见性。
- 允许您在维护窗口期间同时在多台机器上执行按需扫描，并提供便捷的报告。
- 对访问 OT 站点的设备（包括第三方承包商的计算机）进行反恶意软件合规性检查。

- 设备控制
- 文件完整性控制
- PLC 完整性控制
- 反勒索软件
- 漏洞入侵防护
- 网络威胁防护
- Windows 日志检查器
- Wi-Fi 控制
- 防火墙管理
- 注册表监控
- 安全审核
- EDR 代理
- 端点传感器（与卡巴斯基工业网络安全解决方案 – 网络安全集成）

- Windows 节点
- Linux 节点
- 便携扫描仪
- 审核代理

- 网关
- Historian 服务器
- SCADA 服务器
- 操作员工作站
- 工程工作站
- 系统管理工作站
- 嵌入式系统

优点

对受保护设备的影响小，

- 对受保护设备的影响较小，以获得最佳系统性能
- 安装、更新或升级无需重新启动
- 支持仅检测模式
- 可调的系统资源消耗

兼容性

- 支持从 Windows XP SP2 和 Windows Server 2003 SP1 开始的旧版操作系统
- 与工业自动化 供应商兼容
- 便携扫描仪作为免安装 选件提供

扩展保护

- 防御恶意软件、勒索软件和漏洞
- 日志分析
- 防火墙控制
- 内置的 ICS EDR 技术
- 安全隔离网闸数据库更新

模块化部署

- 灵活的选项和安全的非侵入式设置，专为 OT 设计
- 模块化结构允许只选择所需的保护组件

PLC 支持

- Siemens SIMATIC S7-300、S7-400、S7-400H、S7-1500、S7-1200、SIPROTEC 4
- Schneider Electric Modicon M340、M580
- 基于 CODESYS V3 的设备
- Fastwel CPM723-01

检查

- 基于 OVAL 开放式标准的全面安全性和合规性审核

卡巴斯基 XDR 有效性因素

根据上下文理解独特的特征、需求、专门的系统、协议和运营注意事项

与 ICS 集成可以实现工业网络流量和系统行为的全面可见性和分析

特定于 OT 的威胁情报，以利用卡巴斯基在工业环境威胁保护领域的专业知识

定制和配置使解决方案适合特定的风险承受能力、网络架构和法规遵从性需求

单个供应商可以最大限度地利用供应商的支持和协作，包括提供及时的更新和补丁

跨企业工业和公司层面的统一网络安全

针对工业系统，特别是 ICS 和 SCADA 的网络攻击正在增加。选择一个值得信任、对工业与企业网络安全之间的重叠领域有深入的了解，并且有能力提供全方位的尖端工业和企业网络安全技术的合作伙伴变得前所未有地重要。

卡巴斯基 XDR 是创造安全、无威胁的工作环境的完美工具。它与各种安全产品的兼容性有助于建立安全的网络空间，为您的业务提供特定行业的选择，并保护您免受任何威胁（无论大小）的危害。卡巴斯基 XDR 的集成选项允许它提供一个统一的全方位威胁视图，为您的安全团队提供为保护您的业务免受当前和潜在的威胁所需的所有工具和数据。

了解更多

26 年的世界级经验和 PB 级威胁数据

ICS CERT

ICS-CERT – 自有国际 OT/IoT 安全研究部

拥有 IT/OT 安全行业的久经验证的专业知识，获得众多奖项和成就

超过 100 个证书可与自动化供应商解决方案进行互操作

经过验证的技术有效性，符合标准和要求

全球客户

ROSATOM NORNICKEL EuroChem

NLMK TATNEFT ROSSETI Wintershine

alperia PacificLight КазМунайГаз AGC

卡巴斯基工业网络安全

卡巴斯基工业网络安全解决方案 – 节点安全

卡巴斯基工业网络安全解决方案 – 网络安全

了解更多

www.kaspersky.com.cn

#kaspersky
#bringonthefuture