一个为工业企业提供全面安全防护的扩展检测与响应 (XDR) 平台。

卡巴斯基工业网络安全

kaspersky 引领未来

被恶意软件攻击

2024 年第一季度，总共 30 起网络安全事件被受影响的组织或相关责任官员公开确认，其中涉及制造业的事件占 64.5%。

卡巴斯基 ICS CERT，
2024 年 6 月

了解更多

工业威胁态势

工业基础设施所有者和运营者面临的新现实受到多种因素的影响，包括黑客活动人士对自动化系统的兴趣日益增长、高监管要求、IT-OT 融合以及工业领域网络攻击种类的增多（2024 年第一季度，卡巴斯基的解决方案阻止了来自 10,865 个不同家族的恶意软件对工业自动化系统的攻击）。

数字技术的普及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。将单个闪存驱动器带入 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：

石油、天然气和化工

勘探、开采、运输和精炼的数字化是这些公司的一个关键竞争因素，这意味着整合工业物联网、无人机和机器人以及部署 5G、区块链和虚拟现实解决方案，因而扩大了恶意行为的范围。

关键制造

为了提高成本效益，这些企业部署尖端技术、扩大连接性、利用云技术并探索 IT-OT 融合场景，所有这些举措都增加了面临全新和不断变化的威胁的风险。

矿产、金属和采矿

该行业是关键且具有国家重要性的制造业的基石，必须在引入自动化和数字技术的同时平衡开支。作为黑客活动人士和高潜力攻击者的目标，不能在网络安全方面有任何妥协。

电力、电网和公用事业

数字技术和新兴技术对于推动能源转型并同时维持传统基础设施至关重要，这些基础设施仍然是大多数能源设施的支柱。然而，它们是最大的风险，需要额外的网络安全工作。

APT 攻击的主要目标包括：

关键基础设施所有者和运营者

石油和天然气、化工、能源和公用事业等具有重要战略地位的组织面临着运营干扰带来的更大潜在后果

关键制造

从单个工厂到全国乃至国际范围，这些公司（包括来自金属和采矿业、农业和全球制造业的公司）从事着涉及重大事故成本的高风险运营

针对工业系统，特别是 ICS 和 SCADA 的攻击正在增加。与此同时，当今针对工业环境的网络威胁似乎对传统解决方案产生了抵抗力。在此背景下，卡巴斯基为这些行业提供了全面的防护措施。在我们的网站上探索我们的客户成功案例、威胁态势洞察以及专门针对特定场景的产品。

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。

详细了解 2024 年初针对工业企业的 APT 和金融攻击

了解更多

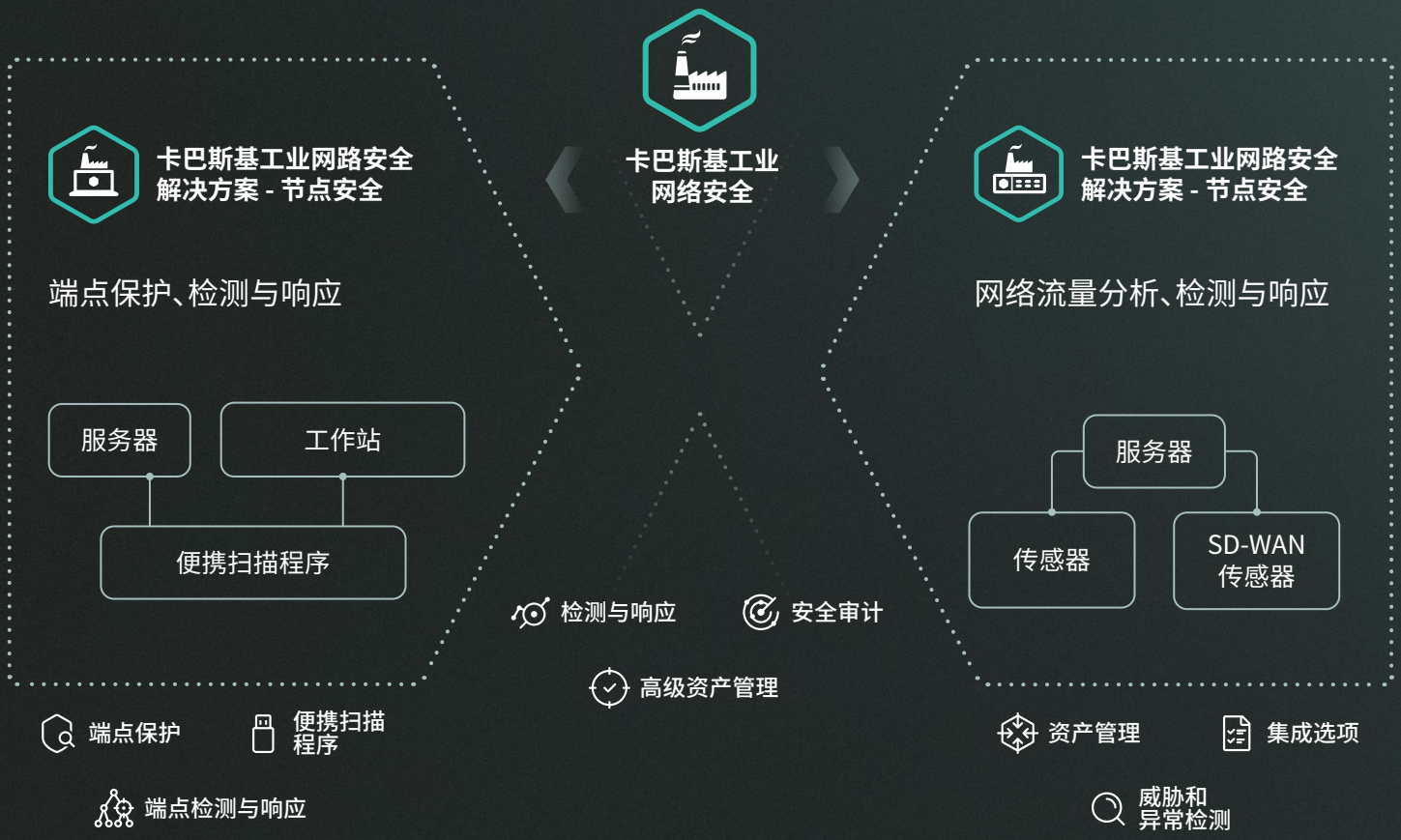
高级 ICS 安全技术

IT 和 OT 环境之间的间隔过去保护了后者免受网络犯罪分子的侵害，但这个间隔正变得越来越小，因此，对于网络物理系统的所有者和运营者来说，采用一套综合性的企业级单一供应商安全解决方案来保护关键基础设施已成为必然。**卡巴斯基工业网络安全 (KICS)** 原生 XDR 平台由 KICS for Networks 和 KICS for Nodes 组件组成，用于保护工业自动化系统和网络。

卡巴斯基工业网络安全解决方案 – 网络安全(KICS for Networks) 是一个流量分析、检测和响应产品，提供工业网络监控、入侵检测和风险管理，同时提供对工业网络节点的集中审查，以发现漏洞并使其符合工业标准。
卡巴斯基工业网络安全解决方案 – 节点安全 (KICS for Nodes) 提供工业级端点保护、检测和响应，以及基于 OVAL* 的合规性审查。这个模块化、低影响的解决方案与 Linux、Windows、旧系统、独立系统和 PLC 兼容。便携扫描程序版本无需安装即可保护独立机器和承包商设备。

这些组件结合在一起构成了 KICS XDR 平台，提供集中式资产清查、风险管理和审计，通过具有全面事件图、分析等功能的单一平台，在多种分布式基础设施上实现安全可扩展性。

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。



* 开放式漏洞评估语言 (OVAL)

平台应用程序点

融合 OT 和 IT 环境

IT 环境

DMZ / GTW

OT 环境

卡巴斯基工业网路安全解决方案 - 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

卡巴斯基工业网路安全解决方案 - 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)

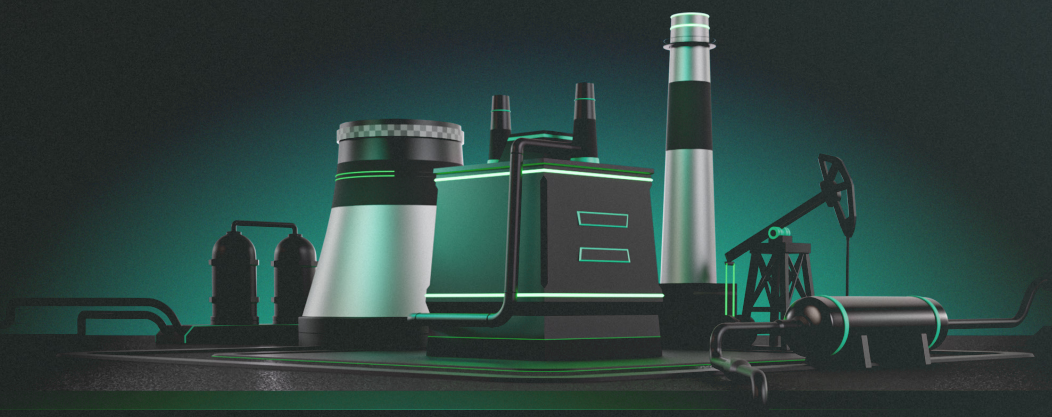
继电保护及安全仪表系统 (SIS)

孤立节点
(使用 KICS 便携式扫描仪手动检查)

物理层

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。



了解更多

由卡巴斯基产品提供安全防护

卡巴斯基工业网路安全解决方案 - 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)

工业网络监控和流量分析解决方案。实现对专有工业协议的深度数据包检查 (DPI)。以软件或虚拟设备的形式提供。

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。

资产管理

资产发现
通过漏洞数据库、风险优先级排序和安全主动轮询，深入了解您的资产

网络可见性
监控流量，形成拓扑图，并随着时间的推移跟踪网络态势，以实现终极可见性

流量分析工具集
跟踪和分析网络会话，实现详细的流量数据导出和存储

优势

- 专为工业应用和协议设计。对各种 OT 协议、设备和网络攻击的开箱即用支持 + 允许从外部项目导入
- 预设的安全审计配置规则
- 用户友好的界面和可定制的报告
- 全面的跨分布式基础设施的风险意识
- 从多个来源获取流量样本：自有网络传感器、SD-WAN 传感器、端点传感器和便携式探测器

生态系统和整合

生态系统
通过与以下解决方案和我们统一的跨产品网络安全方案集成，解锁卡巴斯基生态系统的广泛功能：

- 卡巴斯基新一代安全 - XDR 专家版
了解更多
- 卡巴斯基物联网安全网关 (KISG)
了解更多
- 卡巴斯基异常检测机器学习 (MLAD)
了解更多
- 卡巴斯基软件定义的广域网 (SD-WAN)
了解更多

通过单一控制台管理生态系统的所有元素

第三方集成
与众多外部安全工具和平台无缝兼容

威胁和异常检测

入侵检测
基于签名的检测和统计引擎，可检测暴力破解或扫描尝试

网络完整性控制
系统会学习正常的网络交互并对每个偏差发出警报

异常检测
检测基本数据包和协议级异常。可以通过 MLAD 进行增强

工业协议 DPI
维护进程和命令控制，并高效跟踪遥测数据

事件关联
将安全事件与 MITRE 分类和单一杀伤链相关联

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

卡巴斯基工业网路安全解决方案 - 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) 为当今的数字、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。

端点保护

实时威胁防御
对可移动驱动器和关键区域进行自定义和按需扫描，防止漏洞利用并保护文件

本地活动控制
设备和 Wi-Fi 控制功能。确保 PLC 项目完整性，实现全面的本地活动感知

网络活动控制
管理主机防火墙并阻止网络会话，确保免受网络威胁

系统监控
验证文件完整性、跟踪注册表访问、检测系统日志中的威胁，以确保操作系统的安全

端点检测和响应

检测
入侵指标 (IoC) 扫描、全面的监控和报告功能

响应
防止执行、隔离/删除文件、启动/终止进程、隔离网络等

Windows 节点
便携扫描程序
Linux 节点
审核代理

便携扫描程序

恶意软件扫描程序
对带入工业现场的独立设备和所有计算机进行反恶意软件扫描

OVAL 扫描
通过手动进行漏洞和合规扫描，但单机上实施网络安全策略

数据包捕获
捕获并分析网络流量，即使对于隔离的基础设施，也能实现终极感知

使用零占用解决方案收集有关硬件和软件的全面数据

优势

- 对受保护设备影响低，资源消耗可调
- 与旧的操作系统和工业自动化供应商兼容
- 基本安全配置以及高级选项，保护您的主机免受任何类型的威胁
- 模块化部署和非侵入式设置
- PLC 支持：Siemens SIMATIC S7-300、S7-400、S7-400H、S7-1500、S7-1200、SIPROTEC 4；Schneider Electric Modicon M340、M580；CODESYS V3 设备；Fastwel CPM723-01
- 灵活的授权许可选项，从 1 个月到 5 年
- 经过验证且高效的配置预设，适用于最流行的 ICS

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

KICS 平台及其他产品

跨企业工业和公司层面的统一网络安全

原生 OT XDR

卡巴斯基工业网络安全的核心组件 KICS for Networks 和 KICS for Nodes 专为在我们的生态系统内无缝协作而打造，实现统一且连贯的体验。如果一起购买，它们将构成一个原生 XDR 平台，提供额外的有价值的跨产品功能。

高级资产管理

端点硬件清查
全面了解基础设施中的所有连接设备，确保资产跟踪准确并增强安全管理

应用程序、用户和补丁清查
详细了解环境中的软件部署、用户访问和补丁状态。充实数据以进行适当管理并减少潜在漏洞

端点流量监控
持续监控每个端点的数据流，以快速检测异常模式或潜在威胁，确保对可疑活动做出迅速响应

安全审计

漏洞扫描
彻底扫描您的资产以评估安全漏洞、增强风险意识、实现及时响应并加强您的整体安全态势

合规性审计
基于代理和无代理的审计，以符合 OVAL 和 XCCDF* 行业标准。功能齐全的编辑器、集中式报告数据库、受保护的节点凭据保管库等

配置控制
确保安全资产配置，跟踪安全风险变化，并维护硬件和软件资产的基线完整性

检测与响应

检测
通过主机网络事件与单一杀伤链视图的关联，增强并简化了威胁识别。充实网络警报数据，以深入洞察事件

响应
通过执行预防、主机隔离和文件隔离，实现强大的威胁响应。无缝防火墙集成进一步增强您快速有效地响应安全事件的能力

开放式 OT XDR

通过关联引擎、自动化响应和第三方连接器扩展 EDR 解决方案的功能 — 利用卡巴斯基 XDR 优选版解决方案增强您的 KICS 平台，以解锁：

- 全面监控和关联信息安全事件 (SIEM)，与各种系统集成
- 威胁情报充实和管理

单一 IT-OT XDR

超越界限，实现终极 IT-OT 融合。将您的 KICS 平台与卡巴斯基 Next XDR 专家版相结合 — 利用卡巴斯基一流的端点保护功能，并从以下功能获益：

- 卡巴斯基单一管理平台提供单一调查图、行动手册和事件管理
- IT 基础设施的综合保护 (IT XDR)

XDR 工业

卡巴斯基工业网络安全

了解更多

卡巴斯基单一管理平台

XDR 企业

卡巴斯基新一代安全 - XDR 专家版

了解更多

* 可扩展配置清单描述格式 (XCCDF)

27 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

200 多个与自动化供应商解决方案兼容的证书

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

卡巴斯基工业网路安全解决方案 - 节点安全

卡巴斯基工业网路安全解决方案 - 网络安全

了解更多

ww.kaspersky.com.cn

#kaspersky
#bringonthefuture