卡巴斯基 OT 网络安全

用于工业企业的网络物理安全生态系统

kaspersky 引领未来

卡巴斯基
OT 网络安全

统一工业安全概念

技术
一系列经过测试、符合要求、经过批准的工业安全解决方案

知识
可靠的威胁分析和全面的工业网络安全培训

专业知识
为综合工业网络安全提供全方位专业服务

IT-OT 融合

卡巴斯基扩展检测与响应

技术

专业解决方案

- 卡巴斯基反无人机系统
- 卡巴斯基异常检测机器学习
- 卡巴斯基软件定义广域网

卡巴斯基工业网络安全

KICS XDR

节点安全
端点保护、检测与响应

网络安全
网络流量分析、检测与响应

卡巴斯基操作系统解决方案

- 卡巴斯基物联网安全网关
- 卡巴斯基安全远程工作区
- 卡巴斯基汽车安全网关

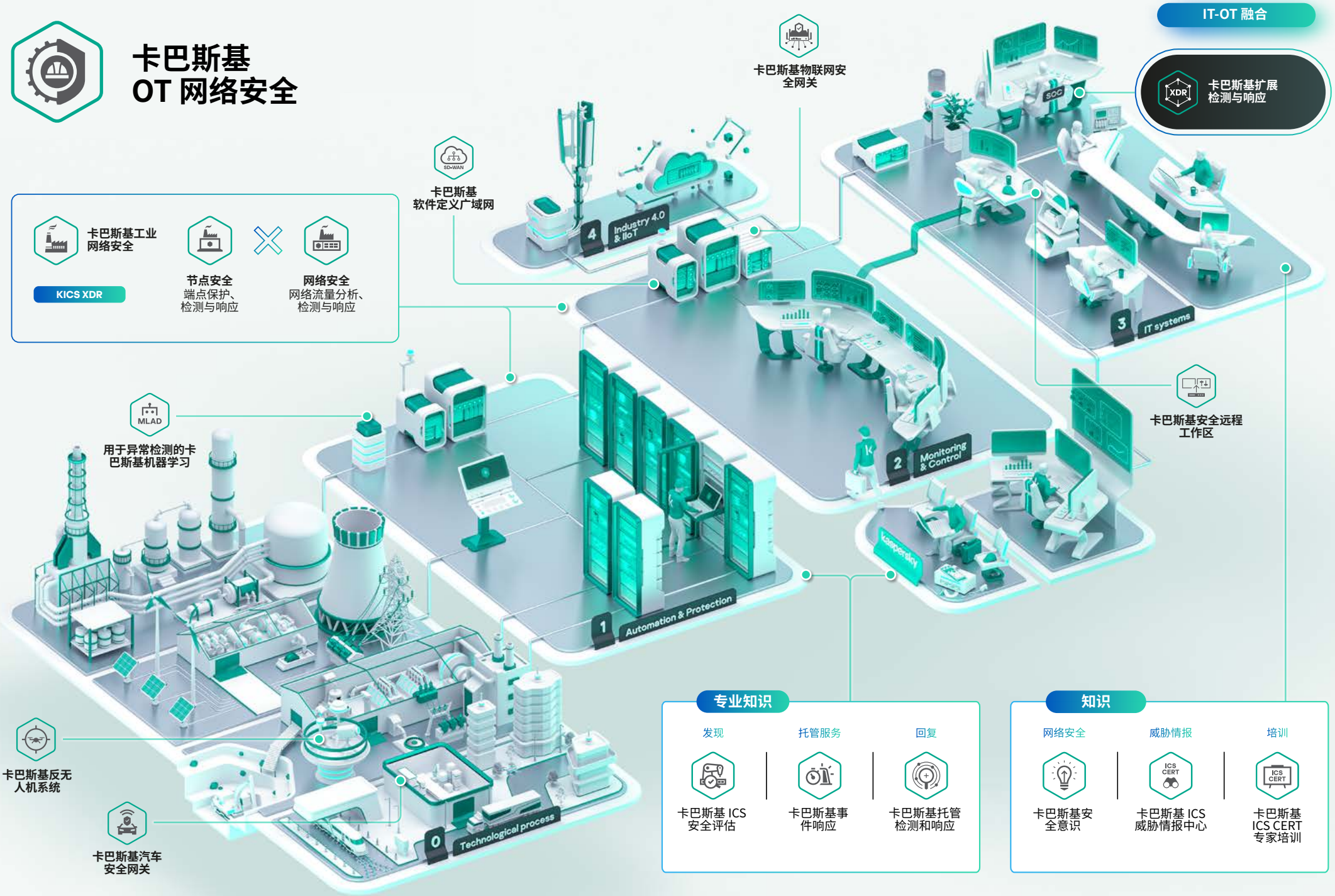
知识

网络安全	威胁情报	培训
卡巴斯基安全意识	卡巴斯基 ICS 威胁情报中心	卡巴斯基 ICS CERT 专家培训

专业知识

发现	托管服务	回复
卡巴斯基 ICS 安全评估	卡巴斯基事件响应	卡巴斯基托管检测和响应

卡巴斯基
OT 网络安全


IT-OT 融合
卡巴斯基扩展
检测与响应
XDR
卡巴斯基物联网安
全网关
卡巴斯基
软件定义广域网
SD-WAN
卡巴斯基工业
网络安全
KICS XDR
节点安全
端点保护、
检测与响应
网络安全
网络流量分析、
检测与响应
MLAD
用于异常检测的卡
巴斯基机器学习
卡巴斯基安全远程
工作区
卡巴斯基反无
人机系统
卡巴斯基汽车
安全网关
4 Industry 4.0 & IIoT
3 IT systems
SOC
2 Monitoring & Control
Kaspersky
1 Automation & Protection
0 Technological process
专业知识
发现
卡巴斯基 ICS
安全评估
托管服务
卡巴斯基事
件响应
回复
卡巴斯基托管
检测和响应
知识
网络安全
卡巴斯基安
全意识
威胁情报
卡巴斯基 ICS
威胁情报中心
培训
卡巴斯基
ICS CERT
专家培训
ICS CERT

访问网站

卡巴斯基工业网络安全

扩展检测与响应

技术

用于保护自动化系统的本机 XDR 平台

- 在潜在的威胁、异常、漏洞和入侵企图对您的操作造成危害之前及时发现它们
- 由自动化供应商和监管机构认证
- 对技术过程没有不利影响。防止严重损害
- 便于管理复杂的分布式自动化基础设施和事件响应
- 帮助降低风险并维护违规记录

XDR 平台的优势

工业自动化和控制系统 (IACS) 的端到端覆盖。保护 Linux、Windows、隔离或第三方计算机，检测网络异常和威胁。

端点和网络的主动和/或被动安全审计。将风险、安全政策和资产管理集中在 IACS 的各个层面。

出色的系统和网络可见性。调查和重建整个攻击链。跨工业网络和不同节点的事件进展可视化。

从合作伙伴处购买　申请获取演示文件　产品介绍

ics.kaspersky.com

访问网站

卡巴斯基扩展检测与响应

技术

跨企业工业和公司层面的统一网络安全

通过与卡巴斯基扩展检测与响应的紧密集成，卡巴斯基工业网络安全平台支持新的场景，包括与第三方解决方案的交互，并具有增强的调查和响应能力。该平台不仅可以在工业环境中保护您的业务，还可以在工业和企业环境重叠的领域保护您的业务。这得益于卡巴斯基一流的 IT 网络安全产品组合的紧密配合。

通过这种方式，安全团队可以形成事件发展的整体图景，并确定其根本原因，以防止将来发生类似事件。

KICS 的响应示例：

- ✔ AV 扫描和 AV 数据库更新
- ✔ 启动任务
- ✔ 更改节点授权
- ✔ 节点和过程隔离

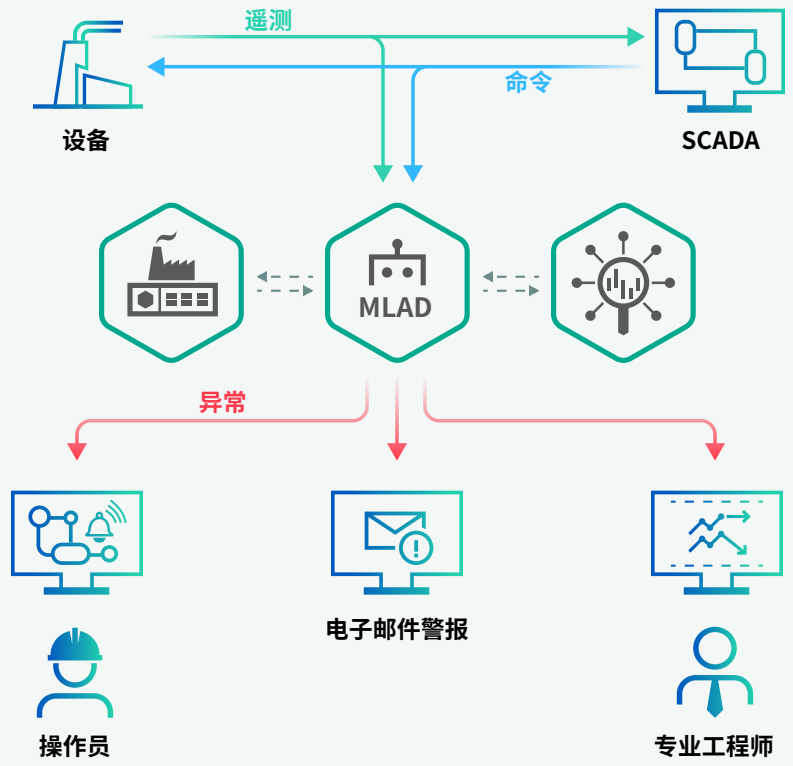
联系我们　　产品介绍

访问网站

MLAD

用于异常检测的卡巴斯基机器学习

技术



早期异常检测和预测分析

- 在设备故障和人为错误变得严重之前就检测到它们，有助于防止发生故障和事故
- 识别非典型的员工行为或设备操作，避免其被作为专门攻击或破坏的迹象
- 将异常检测与设备状态和生命周期的预测分析相结合

生态系统与人工智能

与卡巴斯基工业网络安全解决方案 – 网络安全 (KICS for Networks) 和 KUMA 集成：接收来自这些系统的遥测数据和事件，并发送有关检测到的异常的警报

将诊断规则应用于问题的预定义症状，并应用机器学习以检测与正常设备行为的任何偏差

使用人工智能分析过程遥测及与员工行为相关的事件

访问网站

SD-WAN

卡巴斯基
软件定义广域网

技术

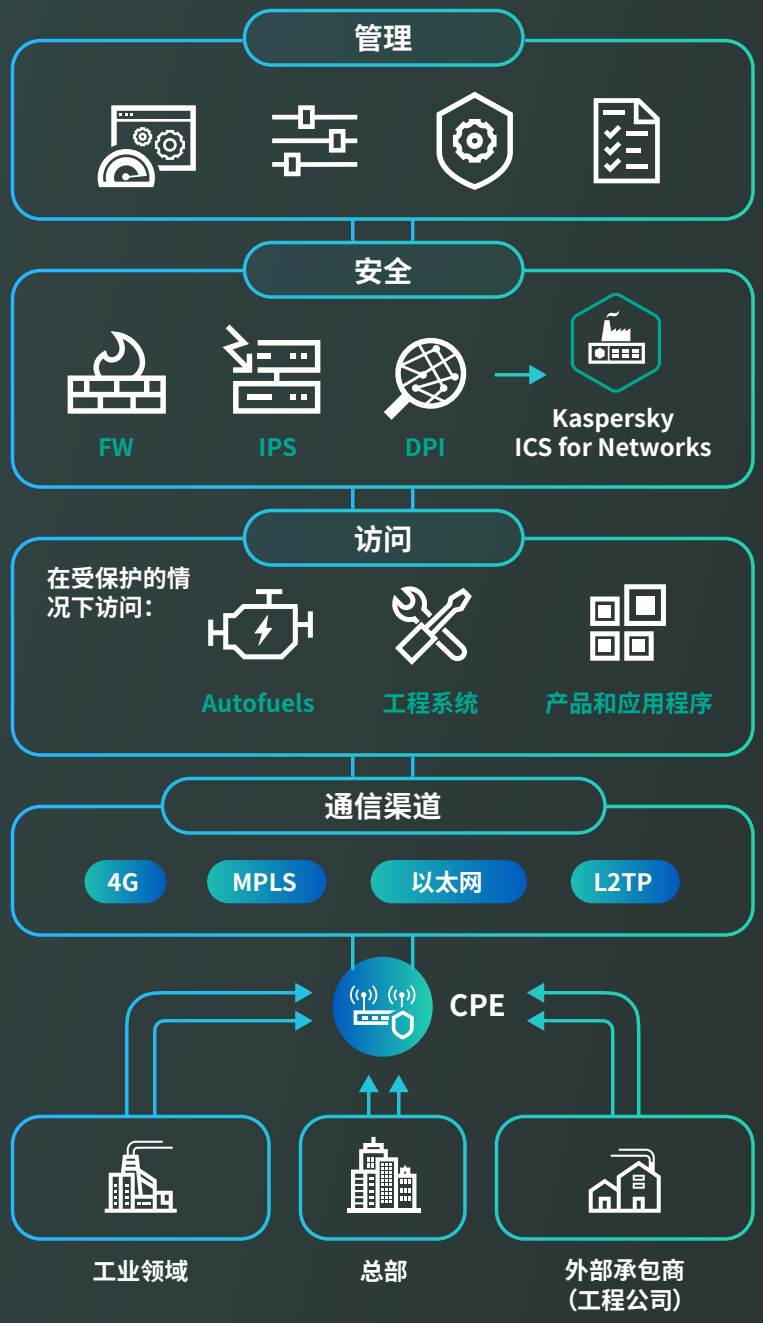
卡巴斯基软件定义广域网 功能：

- 便捷的可扩展性
- 便捷管理
- 成本优化
- 集中安全

一个解决方案即可构建可靠的工业网络

卡巴斯基软件定义广域网 允许企业建立一个容错的、地理分布式网络，可实现集中管理，同时确保生产过程的连续性。卡巴斯基软件定义广域网 架构允许您通过虚拟网络功能 (VNF) 管理器轻松集成卡巴斯基和第三方安全工具。

使用 软件定义广域网 基础设施和 Kaspersky ICS for Networks，您可以为众多分布式工业站点组织集中监控和保护系统。



联系我们

访问网站

卡巴斯基反无人机系统

技术

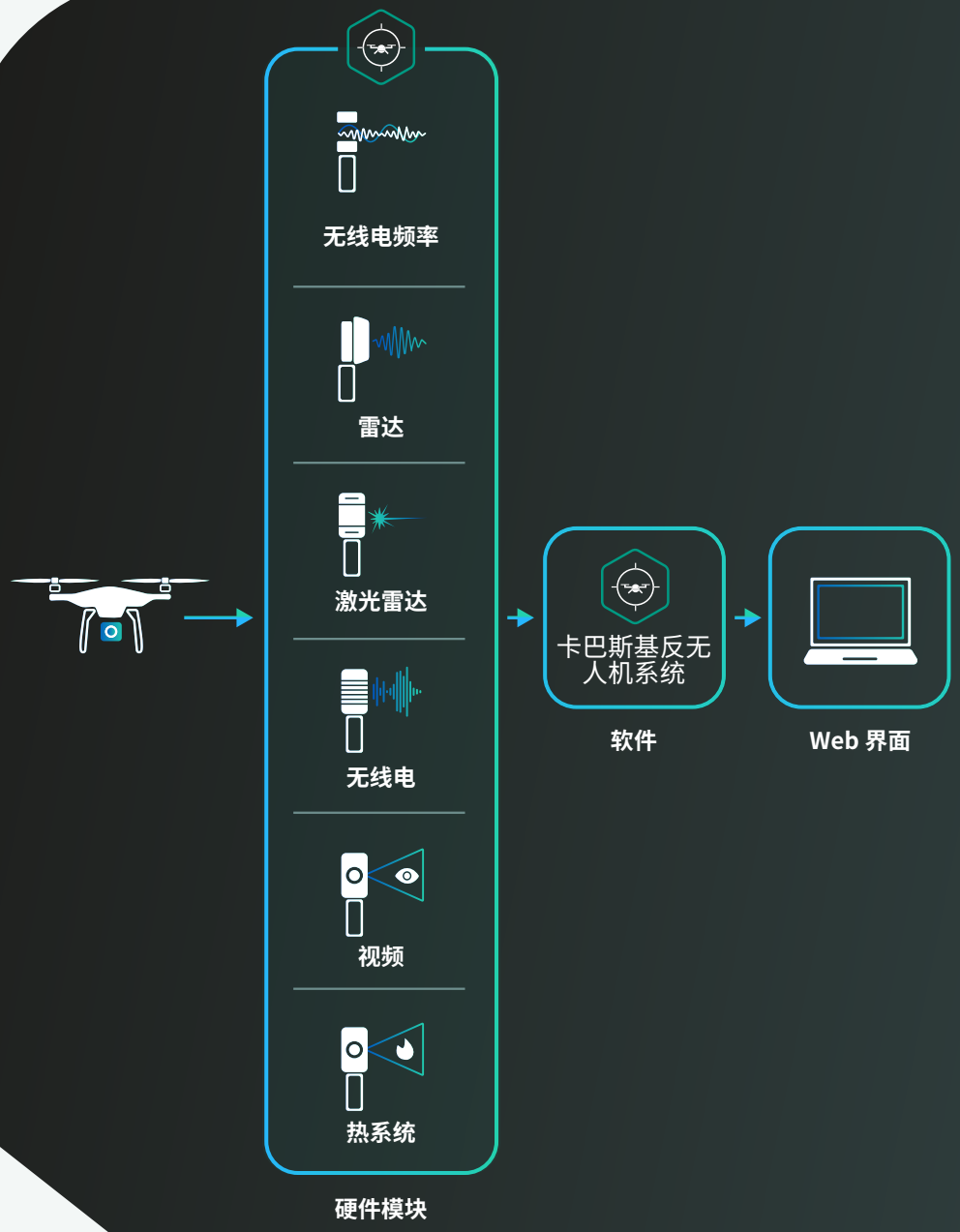
关键功能

- 无人机探测与跟踪
- 利用神经网络对无人机进行分类
- 定向和全向干扰

无人机监控和防御解决方案

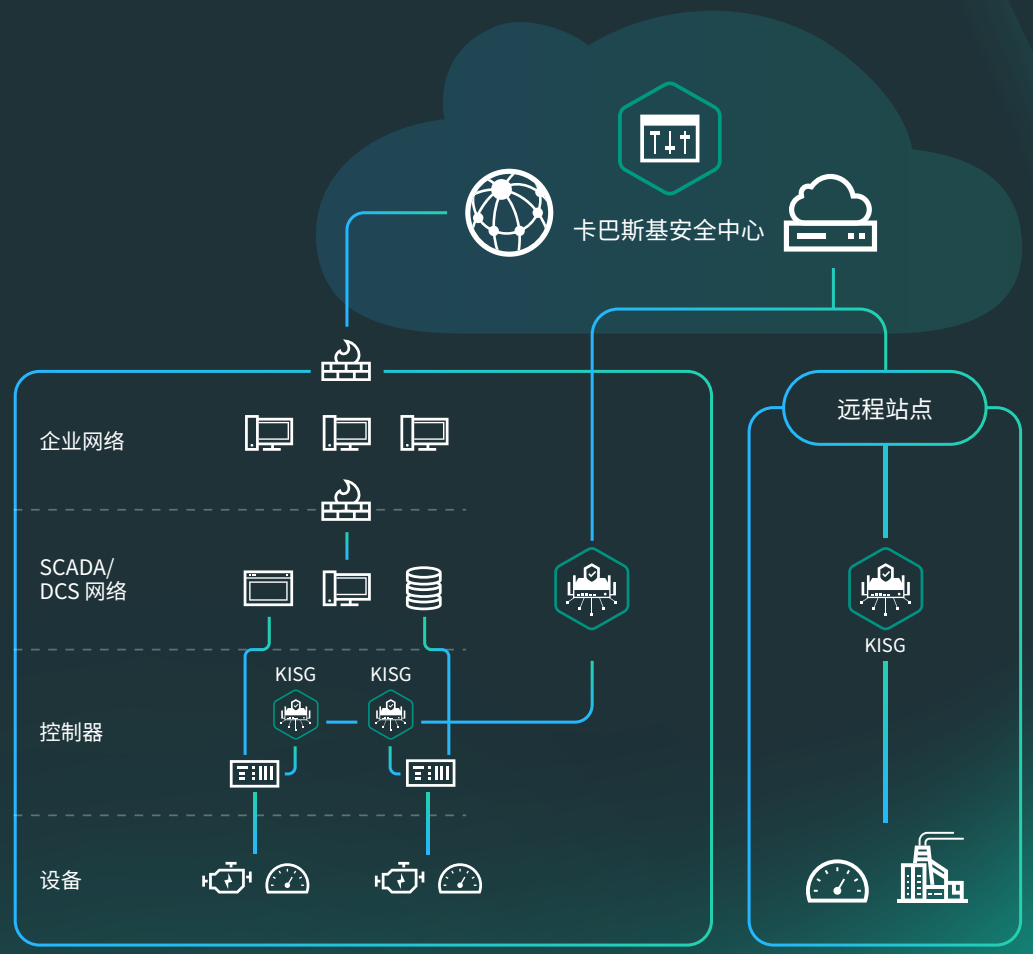
卡巴斯基反无人机系统通过防止未经授权的无人机进入工业企业的空域，降低被攻击的可能性。该系统自动扫描空域，探测无人机并进行分类。Web 界面中将显示与实时相关的信息。在遇到威胁的情况下，在适当的许可下，操作员可以使无人机失效。

卡巴斯基反无人机解决方案采用模块化设计，可以应用于任何规模的工业场所。该解决方案还支持“敌我”操作模式，允许客户使用自己的无人机，避免非法无人机器的干预。



申请获取演示文件　　产品介绍

antidrone.kaspersky.com



aprotech

该解决方案的技术和商业开发由 Adaptive Production Technologies LLC（Aprotech，卡巴斯基的子公司）负责

联系我们 **申请获取演示文件** **产品介绍**

访问网站

卡巴斯基物联网安全网关

技术

关键功能

- 确保从物联网设备到数字和云平台的数据收集和传输安全
- 基于 KasperskyOS 的卡巴斯基网络安全方法能自动防御绝大多数类型的网络攻击，无需额外的安全工具
- 基础设施透明、集中事件管理和生产优化

工业 4.0 下用于业务发展的可信数据

该解决方案由基于 KasperskyOS 的卡巴斯基物联网安全网关和卡巴斯基安全中心 管理控制台组成。这些网关可以安全地收集设备数据并将其传输到数字和云平台，提供高质量的商业智能，以优化生产并防止事故发生。该控制台支持映射来自不同来源的事件，并管理多达 100,000 个物理、虚拟和云工作站。

访问网站

卡巴斯基安全远程工作区

技术

产品应用程序

风险

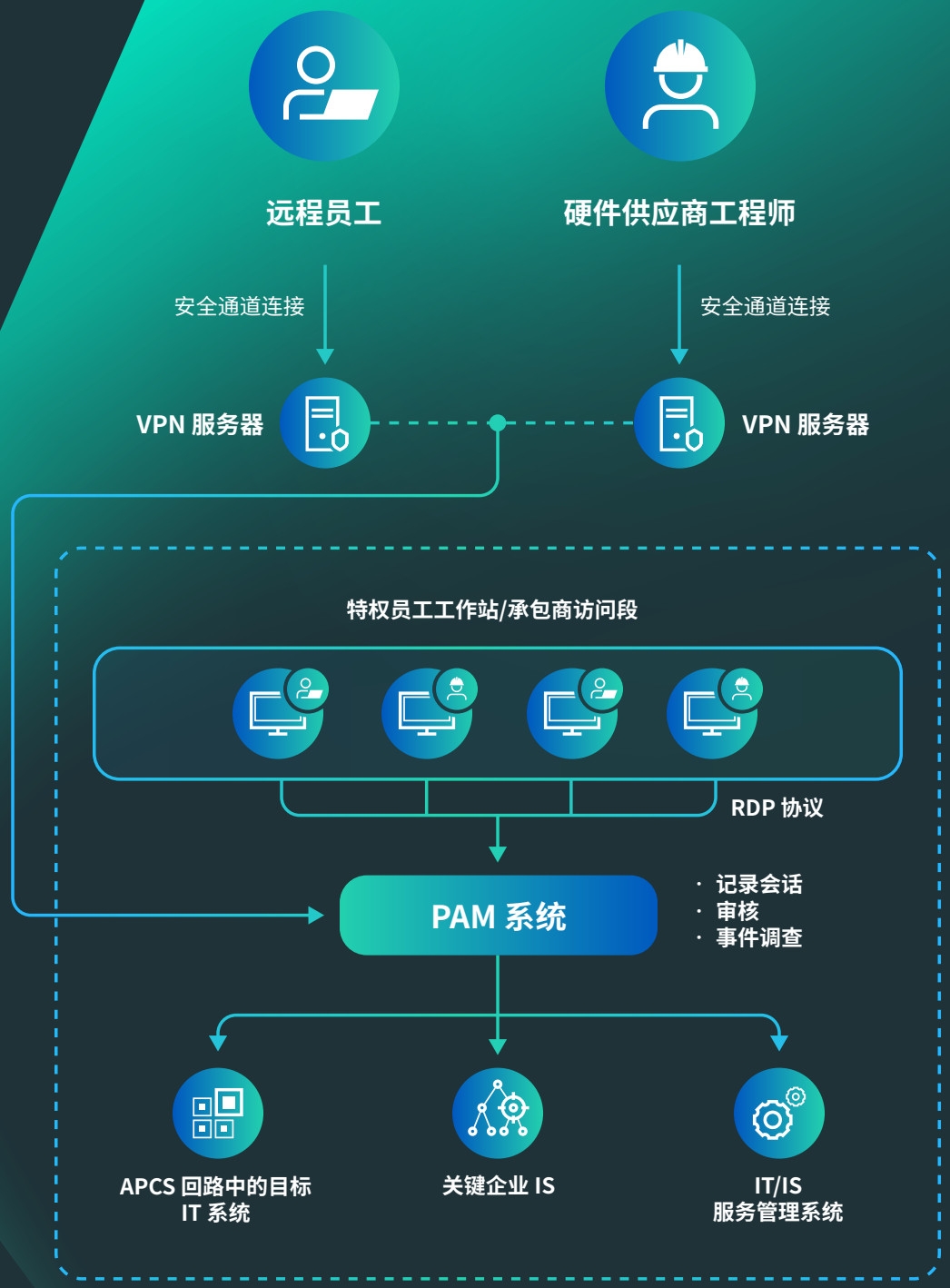
用户工作站是最常见的网络攻击目标之一

解决方案

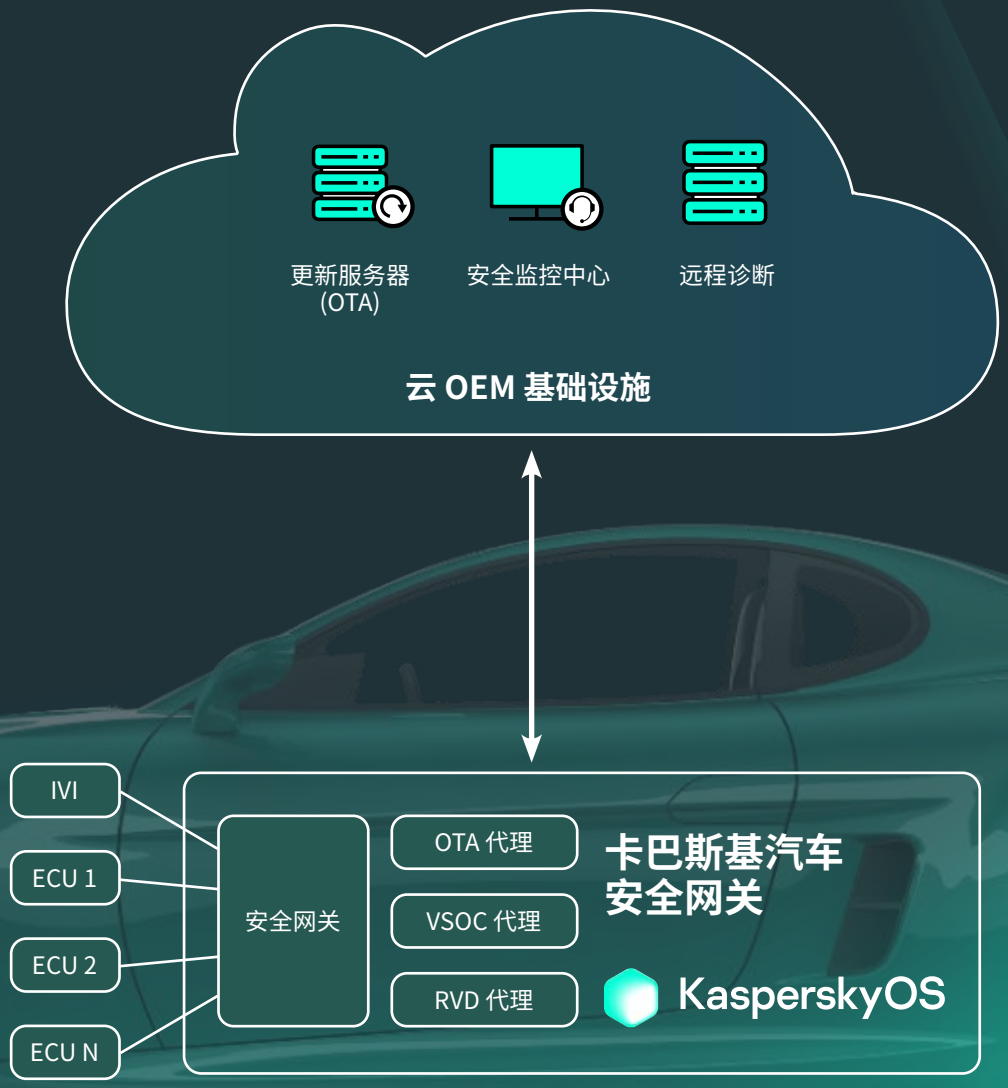
卡巴斯基安全远程工作区 (KSRW) 是一种基于卡巴斯基自己的微内核 KasperskyOS 操作系统为瘦客户端构建受管和功能基础设施的解决方案

网络免疫瘦客户端基础设施

网络免疫瘦客户端作为卡巴斯基安全远程工作区的一部分，提供到虚拟桌面的安全连接，包括一个将用户连接到工业基础设施的可信区域。



解决方案概述　申请获取演示文件　产品介绍



访问网站

卡巴斯基汽车安全网关

技术

车辆保护

- 未经授权的访问
- ECU 定向攻击
- 通过车辆信息系统 (IVI) 进行的攻击
- 恶意诊断
- 更新系统的危害
- 不受控制的连接和数据流，通信中断

主要优点

- 基于安全设计的解决方案
- 帮助遵守网络安全法规
- 4 合 1：连接网关、安全网关、OTA-master 和 VSOC 代理
- 遵守 ISO21434、ISO26262、AUTOSAR Adaptive、Uptane

AUTOSAR

联系我们　　产品介绍

访问网站

ICS CERT

卡巴斯基 ICS 威胁情报中心

知识

全面了解工业网络安全威胁和漏洞，以进行有效的风险评估、准确的攻击检测、事件调查以及响应。

由卡巴斯基 ICS CERT（工业网络安全领域的首个私营 CERT）深厚的专业知识和经验提供支持。

关键功能

- 快速威胁检测和广泛的分析能力
- 提高调查和主动搜索威胁的有效性
- 全面的威胁和漏洞信息，用于做出明智的决策

深入了解针对贵组织的网络威胁，确保领先于对手

卡巴斯基 ICS 威胁数据源

一套针对工业网络安全的特定需求量身定制的定期更新的威胁情报数据源

威胁情报

自动数据流

卡巴斯基 ICS 威胁情报报告

就针对工业组织的恶意活动加强人们的认知，同时还提供在最热门的工业控制系统发现的漏洞的相关信息

卡巴斯基咨询分析师

客户可以通过该服务针对其面临或感兴趣的特定威胁请求专家指导和见解。

申请获取演示文件　解决方案概述　联系我们

访问网站

卡巴斯基 ICS 威胁数据源

知识

卡巴斯基威胁数据源服务提供实时威胁情报信息，帮助工业组织保护其网络和系统免受网络威胁。数据源包括有关已知恶意软件、网络钓鱼网站、最新漏洞和利用以及其他类型的网络威胁的信息。根据事件背景，可以更容易地使用数据来构建“更大的图景”并回答与“人物、事件、地点、时间”有关的问题，以确定攻击者，并帮助您做出快速决策和采取行动。

您将获得：

卡巴斯基 ICS Hashes 数据源

最新的威胁情报，用于 ICS（以及 OT 中使用的其他系统）简化和自动执行及时的攻击检测和调查

#防御

#检测

#调查

卡巴斯基 ICS 漏洞数据源

以机器可读的格式提供关于工业环境中使用的 ICS 系统和其他系统的软件和硬件漏洞的经核实和精炼的数据

#防御

#检测

#调查

OVAL 格式的 ICS 漏洞数据源

定期更新的包含 OVAL 定义的数据源，用于自动检测 SCADA 系统和其他工业软件中的已知漏洞

#检测

联系我们　有关服务的更多信息

访问网站

卡巴斯基 ICS 威胁情报报告

知识

卡巴斯基 ICS 威胁情报报告对针对工业组织的恶意活动提供了深入的情报和更出色的认知，同时提供了在最热门的工业控制系统和基础技术中发现的漏洞的相关信息。为工业组织量身定制的详细信息可帮助客户保护关键资产（包括软件和硬件组件），并确保技术过程的安全性和连续性。

报告通过**卡巴斯基威胁情报门户网站**提供，也可以通过 API 访问。

您将获得：

APT 报告

关于针对工业组织的全新 APT 和大规模攻击活动的报告，以及关于活跃威胁的最新动态。

威胁环境

关于工业控制系统威胁形势的重大变化、新发现的影响 ICS 安全等级的关键因素以及 ICS 面临的威胁的报告，包括地区、国家和行业特定的信息。

发现的漏洞

关于卡巴斯基在工业控制系统、工业物联网和各行业基础架构中使用的热门产品中发现的漏洞的报告。

漏洞分析和解决

我们的顾问服务提供了卡巴斯基专家给予的可行建议，以帮助识别和抵御威胁。

联系我们　　有关服务的更多信息

*** 有关已发布的报告的补充信息：**

- 有关 ICS 漏洞的信息
- 按地区和行业分类的过程控制系统威胁统计信息及新趋势
- 针对 ICS 的恶意软件的分析
- 有关法规要求和标准的信息

访问网站

卡巴斯基咨询分析师

知识

您将获得：

卡巴斯基分析师咨询服务是对卡巴斯基威胁情报产品组合的补充。通过这项服务，您可以联系专家获取有关您面临或感兴趣的特定威胁和漏洞的支持和有用信息。利用这些数据，您可以提高防御能力，抵御针对整个组织和工业基础设施的威胁。

主要优点

联系领先的威胁情报专家，包括卡巴斯基 ICS CERT 的工业安全专家

个性化的详细背景信息，有助于有效调查

我们的专家会详细说明如何对威胁和漏洞做出快速响应

联系我们　　有关服务的更多信息

访问网站

卡巴斯基安全意识

知识

提高员工的网络素养

- 培训材料，帮助员工掌握工业网络安全领域各个最重要方面的必要知识，提高组织各个层面的意识水平
- 卡巴斯基交互保护模拟 – 通过商业模拟提供的基于游戏的培训，包含不同行业的多种场景：火力发电、水力发电、石油和天然气、石化、石油控股等。
- 卡巴斯基自动化安全意识平台 (ASAP) – 交互式学习模块和模拟的网络钓鱼攻击，旨在培养网络安全行为

涵盖的主要内容

- 电子邮箱
- 网站和互联网
- 密码和帐户
- 社交媒体和即时消息
- 工业网络安全
- PC 安全
- 移动设备
- 机密数据
- 银行卡安全和 PCI DSS
- GDPR

联系我们　立即试用　培训目录

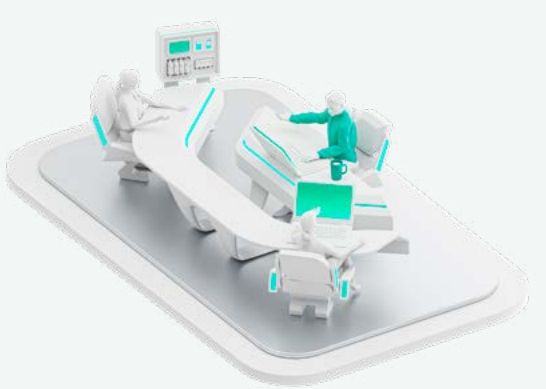
访问网站

卡巴斯基 ICS CERT 专家培训

知识

运用学到的知识

我们的 ICS 培训课程经过专门设计，以确保信息技术 (IT)、运营技术 (OT) 和信息安全 (IS) 专业人员以及管理人员和其他员工可以丰富他们的工业网络安全知识并获得专业的实践技能。



卡巴斯基专家传授的实用技巧

- 数字取证和事故响应
- 探索 OT/IoT 设备和工业软件中的漏洞
- 针对 IT、OT 和 IS 专家的跨职能培训课程

联系我们　培训目录

访问网站

卡巴斯基 ICS 安全评估

专业知识

您的工业基础设施的安全性分析

一种识别工业基础设施安全漏洞和弱点的综合方法，包括：

- 攻击面
- 工业网络基础设施、DCS、工业设备的安全级别
- 关键系统被破坏的风险

检查关键组件

- 网络流量，包括工业协议
- 过程控制组件：SCADA、PLC、智能电表等
- 自动化过程控制系统的物理元素
- 网络架构，包括 ACS 网络

有关服务的更多信息　　联系我们

访问网站

卡巴斯基托管检测与响应

专业知识

关键功能

- 主动威胁检测：获得专利的攻击指标可帮助跟踪控制系统内未被发现的威胁
- 自动和引导式响应
（可应需求提供完整的取证调查和恶意软件分析）
- ICS 网络安全专业知识：由业界最成功的经验丰富的主动威胁检测团队之一提供支持

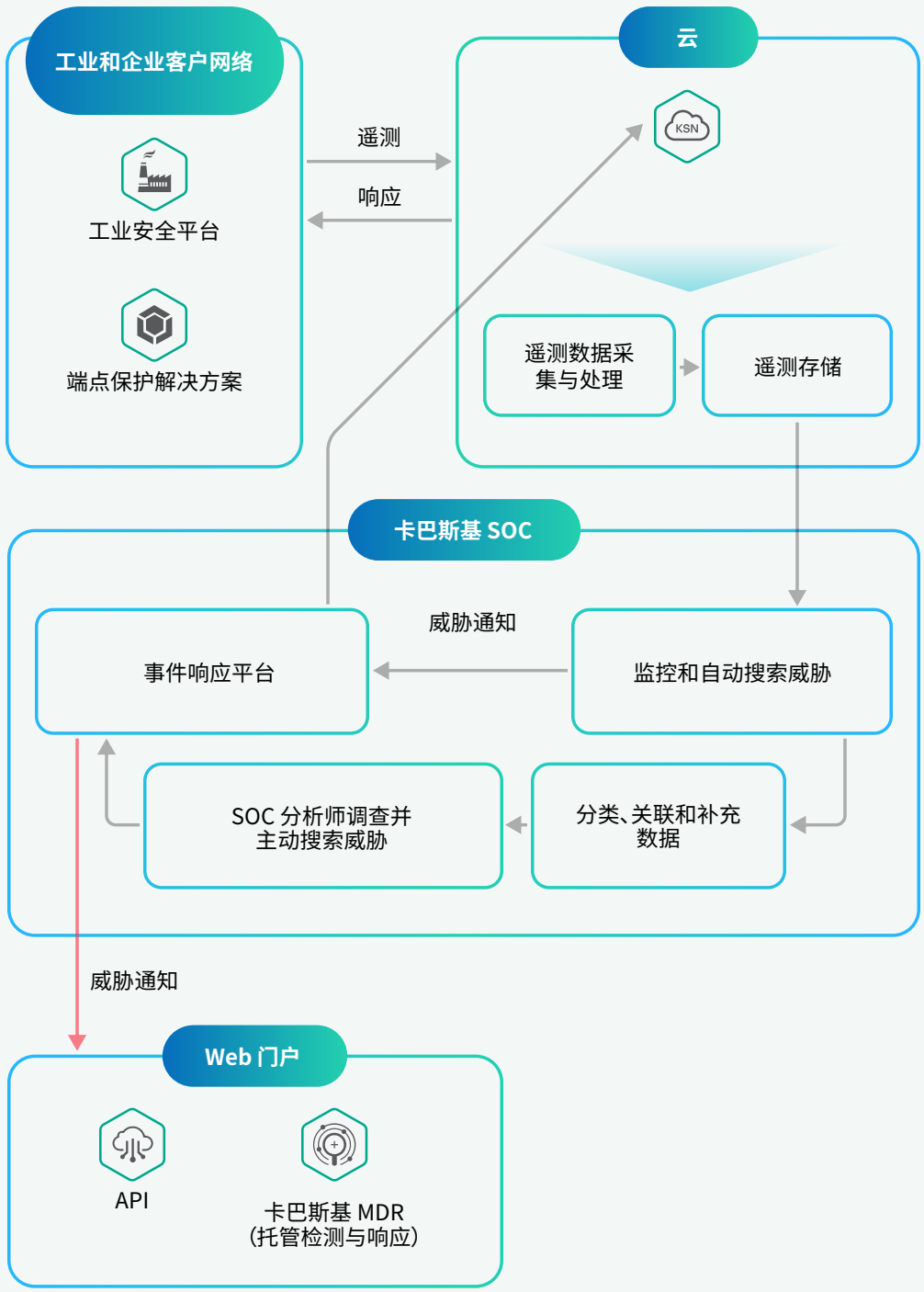
您将获得：

- 持续搜寻、检测和消除您的工业企业面临的威胁
- 无需雇用新的网络安全专家，降低了安全成本
- 无需在内部建立 SOC，即可拥有 SOC 的所有主要优点

我们保护的客户中有 25% 来自工业领域

请查看 MDR 报告以了解更多信息

联系我们 **有关服务的更多信息**



访问网站

卡巴斯基事件响应

专业知识

对事件做出响应

风险

一个漏洞就足以让网络犯罪分子控制整个工业系统

解决方案

- 卡巴斯基全球应急响应团队快速消除事件后果
- 分析事件发生的原因、来源和后果
- 所使用恶意软件的详细视图
- 卡巴斯基 ICS-CERT 的额外支持

服务组合

事件响应：
调查和消除威胁

数字取证：
数字证据的分析

恶意软件分析：
获取攻击中使用的文件的详细视图

在卡巴斯基全球应急响应团队 (GERT) 的研究中发现 IR 趋势。

在卡巴斯基 ICS-CERT 订购 IR 手册

了解更多

联系我们

您可以信任的合作伙伴

26 年的世界级经验和 PB 级威胁数据

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

[有关 OT 生态系统的更多信息]

[有关 IT 生态系统的更多信息]

[联系我们]