白皮书

OT 环境也需要集成安全的原因

什么是OT安全?

正在被广泛使用的“OT”一词，其定义是什么？OT（Operation Technology）即工业运营技术，除了工业控制系统（Industrial Control System: ICS），还指与IT连接或一起使用的广泛领域。而OT安全是指保护上述OT环境的行为或体系。

由此又衍生出了一个问题——“IT安全和OT安全有何不同？”而这个问题还包含了另一个疑问，即OT环境是否无法用IT安全体系来保护。探究这个问题的答案，需要先了解IT和OT的本质和区别。

其基本的答案就在词语本身的含义当中。IT（Information Technology）安全着重于“信息”，而OT（Operation Technology）安全则着重于“运营”。尽管看起来并没有太大的差异，但这种本质的差异导致了方法上的根本差异。

首先，我们从安全的三个属性层面了解一下IT和OT安全。安全的三个属性分别为保密性（Confidentiality）、完整性（Integrity）和可用性（Availability）。这三个属性都是安全的基本要素，但其中存在优先级。通常，在IT安全中，保密性为最高优先级，其后依次为完整性和可用性。其英文缩写为“C.I.A.”。

而OT安全的优先级则有所不同。确保可用性最为重要，其后依次为完整性和保密性。其英文缩写为“A.I.C”。那么为什么会有这样的差异呢？原因非常简单。因为电脑可以重新启动，但工厂设备是绝对不能停止的。

IT和OT环境在设备组成上也有所不同。众所周知，IT环境通常由计算机、笔记本电脑、移动设备、服务器等IT设备组成。而OT环境则在现有的IT设备上增加了工业控制系统（Industrial Control System: ICS）。工业控制设备的代表性设备有可编程逻辑控制器（PLC）。简单来说，PLC是一种向工厂内的设备（例如泵、阀门、机械臂等）设备发送控制命令的设备。总而言之，OT安全与IT安全存在根本性区别，除了对现有IT设备的威胁之外，还必须考虑ICS安全。

OT安全入侵案例

此前，OT领域的外部访问被严格限制，因其环境的封闭性，安全的重要性相对较弱。然而，随着数字化的快速发展，与IT领域的交集增多，针对OT环境的攻击也越来越多，其损失规模也越来越大。特别是OT环境中，设备往往都运行了10年以上，且操作系统陈旧，因补丁不完善而存在很多漏洞。这也是网络攻击造成的损失容易扩散的原因。

从近期发生的重大OT安全事件来看，攻击主要集中在制造业，也有针对发电、能源等社会基础设施的攻击。针对OT环境的攻击大致可分为两类。第一种是将IT环境攻击技术应用到OT环境中。和IT环境一样，勒索软件感染在OT环境中也呈上升趋势，并且存在许多恶意利用因内部系统安全补丁不完善所遗留漏洞的恶意代码感染案例。另一种是篡改控制命令，打击工艺本身，从而造成损失。让我们逐一分析每种攻击类型的代表性案例。

首先是2019年台湾半导体企业TSMC的WannaCry勒索软件感染案例。TSMC因此次事故停产约48小时，并遭受重大经济损失。TSMC的勒索软件感染始于在OT网络内部设备中使用受感染的USB，其后通过“永恒之蓝（Eternal Blue）”SMB漏洞迅速传播。并且勒索软件传播到了与该工厂连接的其他海外工厂，损失也随之扩大。

第二个案例是美国佛罗里达州奥兹马尔（Oldsmar）市一家水处理厂发生的入侵事件。攻击者通过漏洞，在该厂管理人员可能访问的网站植入恶意代码，并由此入侵业务网络系统，窃取了账户信息和控制设备连接信息。其后，攻击者试图通过远程访问程序TeamViewer来操纵水中氢氧化钠的浓度，幸好当时正在监控的管理人员捕捉到了鼠标的异常操作，阻止了攻击。但是，这一事件险些酿成将数万名市民的饮用水变成“碱水”的大型恐怖袭击。

了解OT安全威胁

就针对OT环境的恶意代码而言，蠕虫或勒索软件等具有自我传播功能的恶意代码，大多是因用户的疏忽而进入内部，或是通过连接到互联网的IT网络而感染的。不同于一般恶意代码，为攻击ICS相关系统而制作的恶意代码会造成泄露工业机密或设备中断等严重损失。

那么OT环境是如何遭到入侵的呢？一般通过下面两种方式：

1. 入侵

通常，OT网络中的系统是隔离的，无法从外部访问，但它与IT网络中的部分系统是连接的。由于系统是由远程控制程序管理的，因此必须注意防止泄露远程控制程序的帐户信息。另外还应注意具有恶意意图的内部员工带来的内部威胁（insider threat）。

2. 恶意代码——蠕虫、病毒、勒索软件等

因不遵守规定的安全流程，在OT网络中会经常发生恶意代码感染事件。一般恶意代码不具备OT环境攻击功能，因此虽然可能会导致流量产生或冲突等问题，但不会对系统运行造成明显影响。但是，针对特定OT/ICS环境的恶意代码，将有可能导致攻击者意图造成的数据篡改或损坏等。

另外，OT系统可以直接连接到U盘等存储介质。原则上，维护人员应使用防病毒程序扫描连接到生产线系统的存储介质后带入。然而，若未精密扫描存储介质便使用，则可能会感染蠕虫或病毒等恶意代码。并且存储介质可能会从内部易受攻击的系统受到感染，并在连接到其他系统时传播。严重情况下，如台湾TSMC的案例，即生产线因感染具有自我传播功能的勒索软件而被迫停止生产。

此外，从攻击路径来看，针对OT环境的攻击通常会通过▲IT网络、▲直接访问（合作公司）、▲供应链来进行。

1. IT网络

OT网络通常与外部和互联网断开连接，因此很难进行直接攻击。然而，与IT网络相连的OT网络内的系统也有可能会通过IT网络而导致恶意代码进入内部。攻击者不会直接攻击OT网络，而是试图通过IT网络来攻击OT网络。由于大多OT网络系统也使用IT网络中常见的Windows或Linux，因此恶意代码的作用方式会与IT环境相同。

2. 直接访问（合作公司）

执行维护等业务的合作公司通常会直接访问OT网络内的系统。如果攻击者在合作公司使用的存储介质中插入恶意代码，便可以直接渗透到内部系统。然而，由于攻击者无法与外界通信，因此会尽可能收集大量OT网络内使用的系统类型和版本等信息，并创建相应定制型恶意代码。

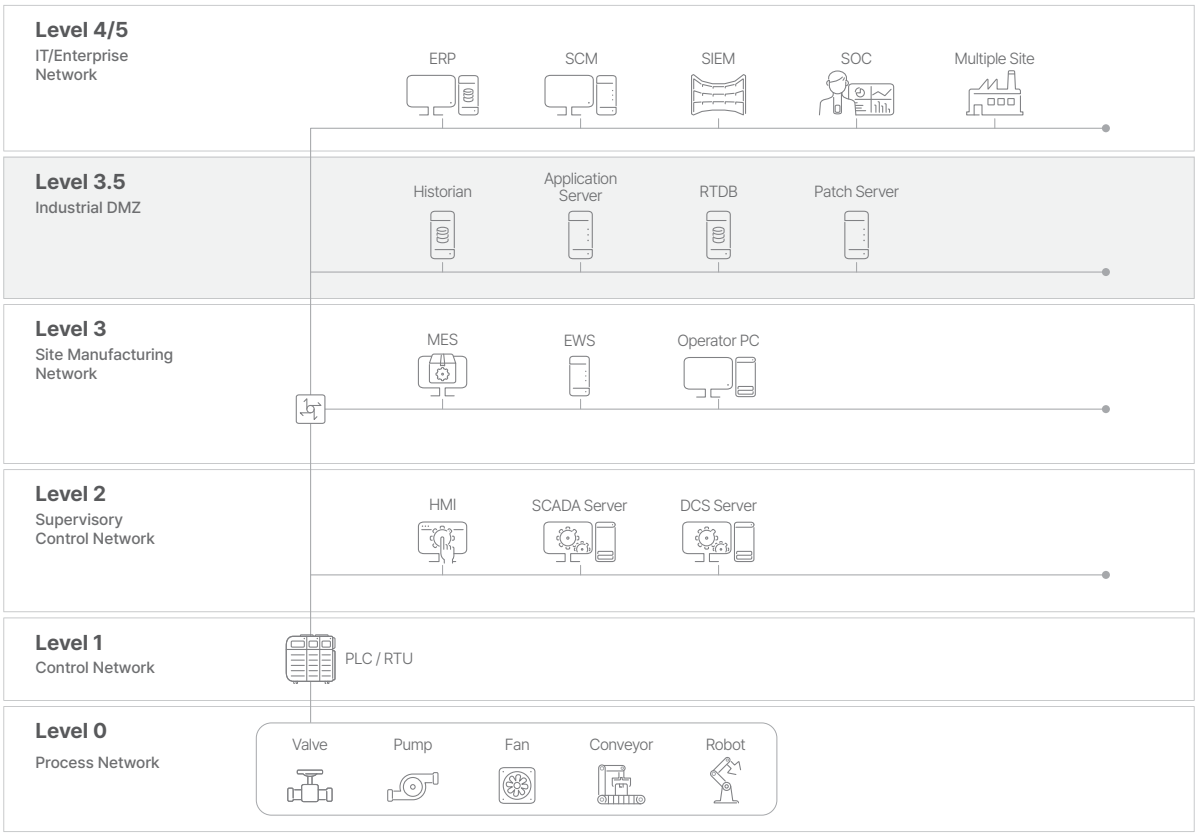
3. 供应链

在OT网络内运行的系统是由专业制造商提供的。攻击者通过攻击此类公司使其制作的程序中包含恶意代码，或者用包含恶意代码的安装文件进行替换。于2013年发现的“Havex恶意代码”，就是入侵在OT网络上运营的软件制造商的网站，并在安装文件中植入恶意代码的典型案例。因此，如果在供应链提供的软件中包含恶意代码的话，是很难获知感染事实的。

了解OT环境结构

此前由于种种原因，OT安全并没有得到重视，但如今已经成为了刻不容缓的课题。随着OT环境面临的威胁与日俱增，OT安全已成为实现真正制造创新的必要条件。那么，现阶段该如何具体建立OT安全体系呢?

要制定有效的OT安全策略，首先要了解OT环境结构。论及OT安全结构时，常会用到“普渡模型（Purdue Model）”。以该模型为准，OT环境从0级到5级分为总共6个层级。



[图1] 普渡模型

然而，考虑到第3级的特点，有时会将第3.5级作为额外的细分层。以下是对每个层级的说明:

Level 0：工序网络（Process Network） - 是现场运行的设备所在的层级。由阀门、泵、输送机和机器人等生产设备、从设备收集数据的传感器（sensor）、开闭装置等通过接收第1级命令进行操作的执行器（Actuator）组成。

Level 1：控制网络（Control Network） - 第1级处理第2级下达的命令并将其发送到第0层。此外，还会将从0级收集到的信息和数据发送到第1级。具代表性的设备有前文提及的对现场设备下达命令并进行控制的PLC（Programmable Logic Controller，可编程逻辑控制器）和RTU（Remote Terminal Unit，远程终端单元）等。

Level 2：监控网络（Supervisory Control Network） - 第2级由远程管理和运营现场设备的系统组成。主要系统有SCADA（Supervisory Control And Data Acquisition，数据采集与监视控制系统）和HMI（Human Machine Interface，人机界面）。SCADA通过第1级的PLC和RTU收集现场数据，并同时控制多个现场设备。HMI将现场收集的数据转换成类似银行ATM机的界面，从而实现高效运营。

Level 3：现场制造网络（Site Manufacturing Network） - 第3级管理整个生产系统并提高运营效率。该层级由优化生产活动全程的MES（Manufacturing Execution System，制造执行系统）、用于控制设备的EWS（Engineering Workstation，工程工作站）和管理产品生命周期的PLM（Product Lifecycle Management，产品生命周期管理）组成。

Level 3.5：Industrial DMZ - 亦称为工业DMZ，是OT环境和外部IT环境的连接点。存储传感器数据的RTDB（Real-time Database，实时数据库）、Historian、应用服务器和补丁服务器等均属于第3.5层。随着OT安全入侵事件频发，后文中将提及的IT-OT融合安全的重要性日益凸显，这一层也逐渐引起人们的关注。

Level 4~5：企业业务系统（Enterprise Biz System） – 由企业一般在IT环境中使用的资源组成，如资源管理（ERP）、供应链管理（SCM）、客户关系管理（CRM）等。管理与工艺相关的全公司业务。

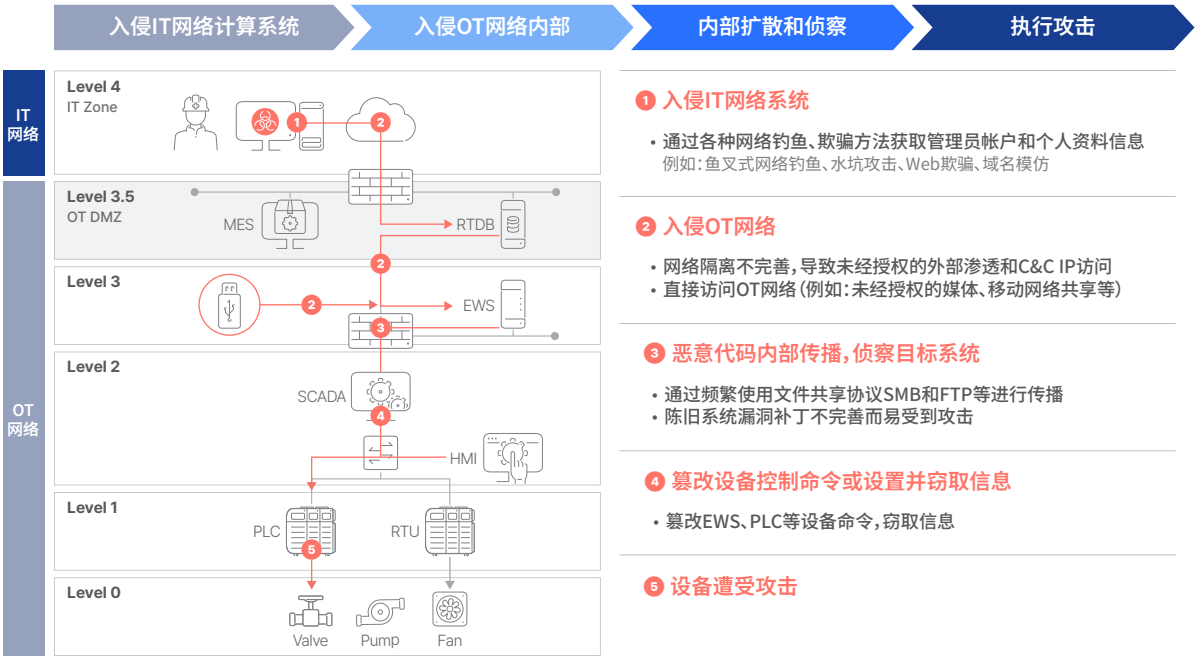
针对OT环境的攻击过程

从安全角度出发，以网络为准可对前文所述的第0~5级进行划分。大体上可以划分为IT网络（第4~5级）和OT网络（第0~3.5级），而OT网络又可以分为控制网络（第0~2级）和运营网络（第3~3.5级）。以下对OT环境各层级和网络的结构和构成要素进行了总结。

层级	区分	主要构成要素	说明
0	控制网络（OT）	• 传感器（Sensor） • 执行器（Actuator） • 生产设备	履行现场作业的设备
1		• PLC • RTU	对现场设备下达命令并进行控制
2		• SCADA • HMI • DCS	远程管理和运营现场设备的系统
3	运营网络（OT）	• MES • PLM	管理和运营整个生产系统
3.5		• RTBD • Historian • 应用服务器	OT和IT领域之间的交集或缓冲区
4~5	IT网络	• ERP • SCM • CRM	管理与工艺相关的全公司业务

[表1] OT环境各层级内容汇总

基于上述内容，我们来看一下入侵OT环境的最新攻击流程图。



[图2] 针对OT环境的攻击过程

OT环境中的安全威胁通常源自IT环境。虽存在未经授权的媒体直接连接到OT网络的情况，但大多数都是IT网络系统被入侵后连接到OT网络的。OT环境通常是一个封闭的网络，由基于气隙（Air-Gap）的网络隔离和网络分段（Segmentation）组成，因此攻击面（Attack Surface）有限。但OT环境与IT网络管理系统连接，因此如果IT网络系统首先受到安全威胁，则OT网络系统的网络连接信息和账户信息也可能被攻击者窃取。

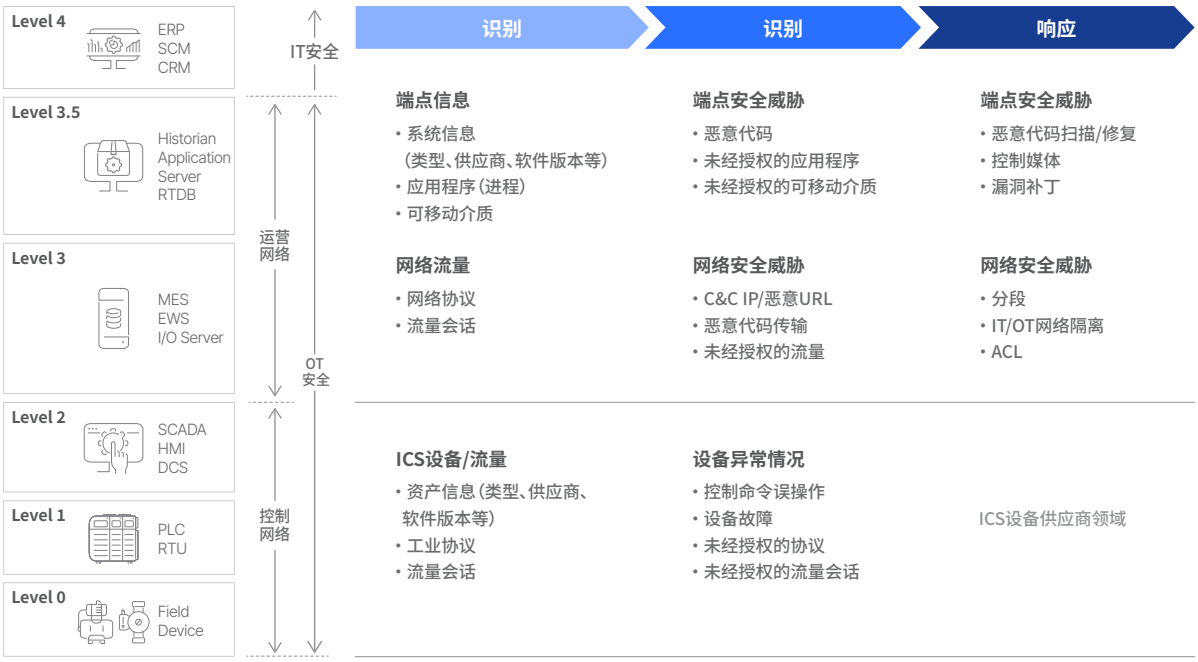
从过程来看，攻击者使用网络钓鱼或高级持续性威胁（Advanced Persistent Threat: APT）等各种技术入侵管理OT网络的IT网络系统。其后会窃取用于访问OT网络系统的管理员帐户、IP、URL等各种个人资料信息。之后便会捕捉网络隔离策略未落实或管理不善的部分，由此入侵OT网络。此外，恶意代码还会通过未经安全管理的USB传播到OT网络，甚至当未经授权的笔记本电脑通过移动网络共享直接连接到设备时，也有可能会被绕过OT网络边界安全的恶意代码入侵。

对于攻击者来说，后续的攻击过程就较为容易。它会检测攻击目标系统并传播恶意代码，而由于OT环境的工作特性，会频繁使用SMB端口、远程文件传输、远程访问，并且存在很多补丁不完善的老化系统，因此传播速度非常快。接下来，它会连接到SCADA或HMI等操作系统，并通过PLC下达异常控制命令或操作设备设置等，对运营造成直接影响。

而这将会是OT网络攻击的起点。需要再次强调的是，不应该将OT安全看作一个单独的问题，而应该与IT安全联系起来考量。

OT安全的要求事项和方法

OT安全基本遵循“识别>检测>响应”这一流程，这一点与IT安全别无二致。不过为了有效应对最新的OT安全威胁，需要构建覆盖OT领域、IT与OT的交集乃至IT领域的“IT & OT融合安全”体系。IT & OT融合安全必须根据“识别>检测>响应”流程涵盖端点、网络和ICS安全。以下对整体流程与各安全领域要求事项进行了总结。



[图3] OT安全流程与各安全领域要求事项

A. 识别

在IT & OT融合安全中，“识别”指的是确保运营中的资产和相关信息的透明“可见性”。在OT环境中，可见性是必要的一项，因为它是高效OT安全的基础。 由于OT网络中资产种类繁多，且使用寿命较长，因此对资产的位置、状态、网络通信等进行综合管理并不容易。因此，如果不能准确识别每项资产，就很难检测和响应安全威胁或影响可用性的设备误动作。

可从资产和网络的角度对可见性进行划分。从资产角度，可以分为控制网络中的各种设备和运营网络中的各种服务器或工作站；从网络角度，可以根据列举各资产间的网络会话与其使用的各种IT/ICS应用协议进行划分。

由于OT网络的环境特点，资产或网络的变化没有IT环境那么频繁，因此可以将已识别的因素作为基线，检测未识别的安全威胁和异常行为。

以OT网络为准观察控制网络的话，需要监控的是资产类型、供应商、软件版本等资产信息和设备的工业协议和流量会话。尤其必须具备将混杂在一起的不同工业协议按照标准进行整合并分析的能力。

再来看运营网络，各端点和网络区域都存在相应的安全要求事项。首先，在端点区域中必须确保系统信息的可见性。系统信息包括系统类型、供应商、软件版本等多种信息。此外，有必要了解整个工艺中使用的应用程序、进程和可移动介质。在网络区域则需要监控网络协议和流量会话。

B. 检测

通过识别确保可见性后，就需要检测OT环境中存在的威胁和异常情况。

首先，在控制网络需要掌握ICS设备的异常情况。需要对是否存在控制命令误操作、设备故障和未经授权的协议和流量会话进行综合监控，始终确保设备的稳定性。

而在运营网络中，一定要对端点领域进行恶意代码检测。此外，还需要检查是否存在未经授权的应用程序和可移动介质。在网络领域，需要对攻击者服务器（C&C）IP、恶意URL、恶意代码传输、未经授权的流量等威胁进行持续检测。

C. 响应

最后，响应是指基于先前识别和检测的信息找到最佳响应计划，最大限度地减少对工艺的影响。首先，由于设备的特殊性，针对控制网络ICS设备的威胁响应必须得到设备制造商的支持。

但对于运营网络，可以主动进行威胁响应。如果检测到端点安全威胁，可以通过进行恶意代码扫描和修复，将损失降到最低。还可以通过媒体控制和漏洞补丁来加强整体安全性。针对网络安全威胁，可以通过“分段（segmentation）”对网络进行细分化，提高监控和威胁响应的效率。此外，通过IT和OT之间的网络隔离，可以有效保护OT环境并加强访问控制。

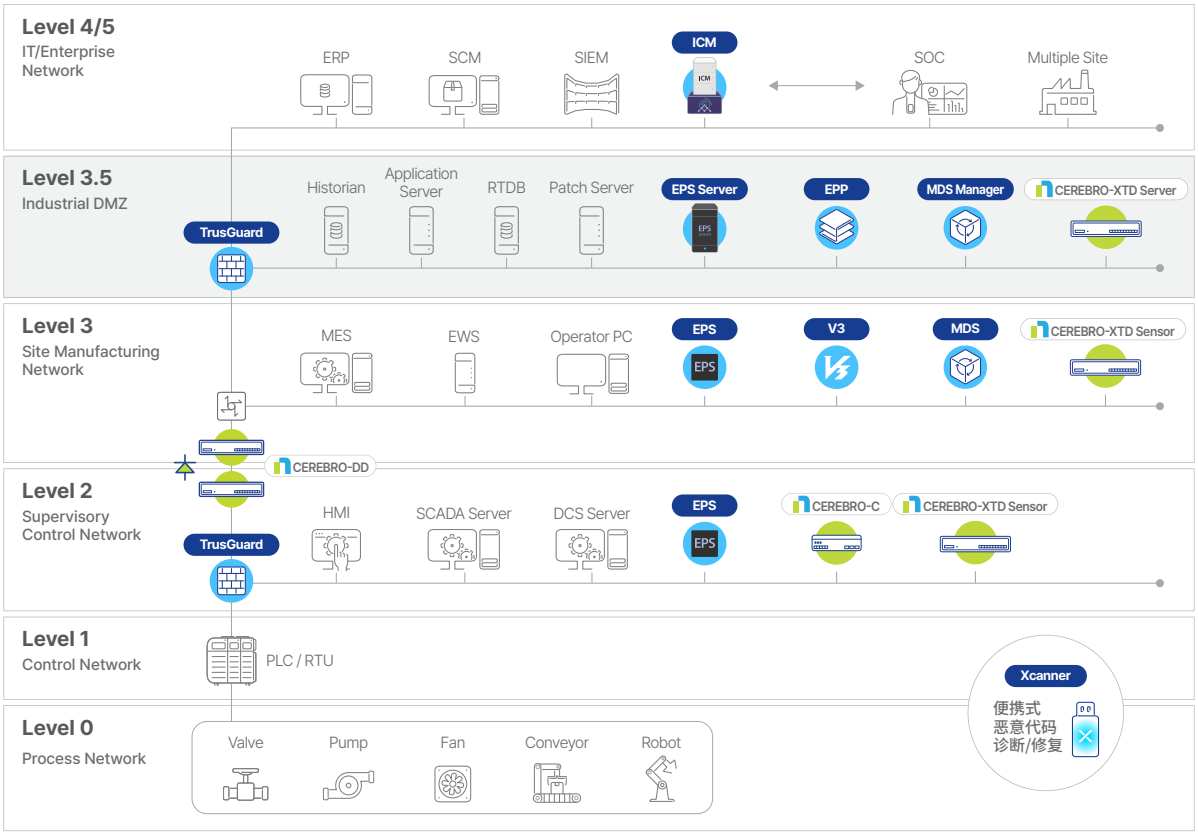
为具备上述各阶段安全能力而所需的安全解决方案可概括如下：首先，在端点领域，需要反恶意软件（Anti-Malware）、基于白名单的应用程序和媒体控制解决方案、补丁管理解决方案等。接下来在网络中，必须配备能够识别资产和检测威胁的入侵检测系统（IDS），并且为了响应需要配备单向数据传输、防火墙等解决方案。最后，针对ICS设备，需要能够基于DPI（Deep Packet Inspection，深度包检测）分析技术对各种工业协议进行异常情况分析的解决方案。

概括起来，为了有效运营由如此复杂的要素构成的IT & OT融合安全，需要基于集成安全框架的有机联动和安全体系，而不是单独的解决方案。

AhnLab集成OT安全框架的定义和引进效果

2021年7月，AhnLab收购了工业控制协议融合安全解决方案专业企业Naonworks，以应对日益增长的集成OT安全需求。Naonworks于2017年推出了OT协议标准化网关解决方案，此后相继推出了具有针对性的OT协议识别分析技术和安全平台，以基于开放架构的边缘计算平台为基础的OT和ICS环境专用安全解决方案“CEREBRO”。

已具备卓越IT安全能力的AhnLab，通过收购Naonworks，将自身的安全威胁检测响应分析技术与Naonworks的工业协议分析技术相结合，由此构建了集成OT安全框架。以下按OT环境层对AhnLab集成OT安全框架的结构进行了



[图4] AhnLab集成OT安全框架

从用户的角度，AhnLab集成OT安全框架的最大价值在于，它可以构建覆盖OT环境各层的“识别>检测>响应”集成安全流程。AhnLab和Naonworks的解决方案在安全框架下发挥必要的作用并产生协同效应。此外，从平台的角度，通过不断加强联动，从端点到网络安全全面提高用户管理效率。以下对构成AhnLab集成OT安全框架的解决方案在各安全阶段起到的作用进行了总结。

	第1阶段：监控&识别	第2阶段：检测威胁	第3阶段：响应	第4阶段：后续措施
AhnLab ICM	• 综合日志监控	• 日志分析 • 查询详细分析报告	• 更改安全模式例外处理项目 • 确认未应用扫描策略的Agent	• 确认是否修复 • 应用Rest API响应策略
AhnLab EPS	• 识别生产设备资产	• 检测已知恶意代码	• 恶意代码扫描 • 阻止未经授权的进程 • 阻止设备运行	• 转换为安全模式 • 请求AhnReport分析
AhnLab Xcanner			• 在被感染计算机上扫描和修复	
AhnLab MDS		• 检测已知/未知恶意代码 • 检测被感染设备的异常网络行为 • 检测绕过行为分析威胁	• 确认MDS误诊 • Pinpoint扫描	
AhnLab TrusGuard		• 检测网络安全威胁 • 检测未经授权的流量会话	• 基于ACL拦截未授权会话 • 拦截有害流量	• 设置防火墙策略 • 网络分段
CEREBRO-XTD	• 识别OT资产 • 识别各资产流量	• 检测恶意代码传播 • 检测C&C等有害流量	• 威胁检测响应警报	
CEREBRO-C	• 识别设备协议		• 转换设备协议	
CEREBRO-DD	• 识别设备协议		• 单向数据传输	

[图5] 各阶段安全解决方案的构成和作用

简单概括起来，AhnLab在端点和网络领域拥有多款保护OT环境的解决方案，而Naonworks拥有工业协议标准化和分析解决方案、物理单向数据传输解决方案，双方通过联合开发，将各解决方案的协同作用发挥至最大。

构成集成OT的安全解决方案的作用

构成AhnLab集成OT安全框架的解决方案发挥哪些具体作用？接下来将按各个解决方案仔细了解[图5]的内容。

AhnLab EPS

AhnLab EPS是AhnLab具代表性的OT端点安全解决方案，广泛应用于国内外半导体、显示器、汽车等制造生产工厂。AhnLab EPS可以通过基于Web的管理系统，有效识别分散在每个设备中的系统并进行高效集成管理。此外，还可以基于白名单，仅允许授权进程和媒体的使用，从而最大限度地降低对OT环境的威胁。由于无需创建单独的应用程序白名单，管理员可以灵活管理，并无需设置策略。

EPS 基于白名单的EPS Agent	VS.	基于黑名单的传统防病毒产品
主动预防	处理方式	事后处理
只使用授权的应用程序	应用程序运行范围	可使用所有应用程序
没有变化	引擎大小	不断发生变化
低	资源占有率	高
高	安全程度	一般
无需在Agent执行更新 更新和定期系统检查时，可在EPS服务器中调度）	引擎更新	需要定期更新引擎

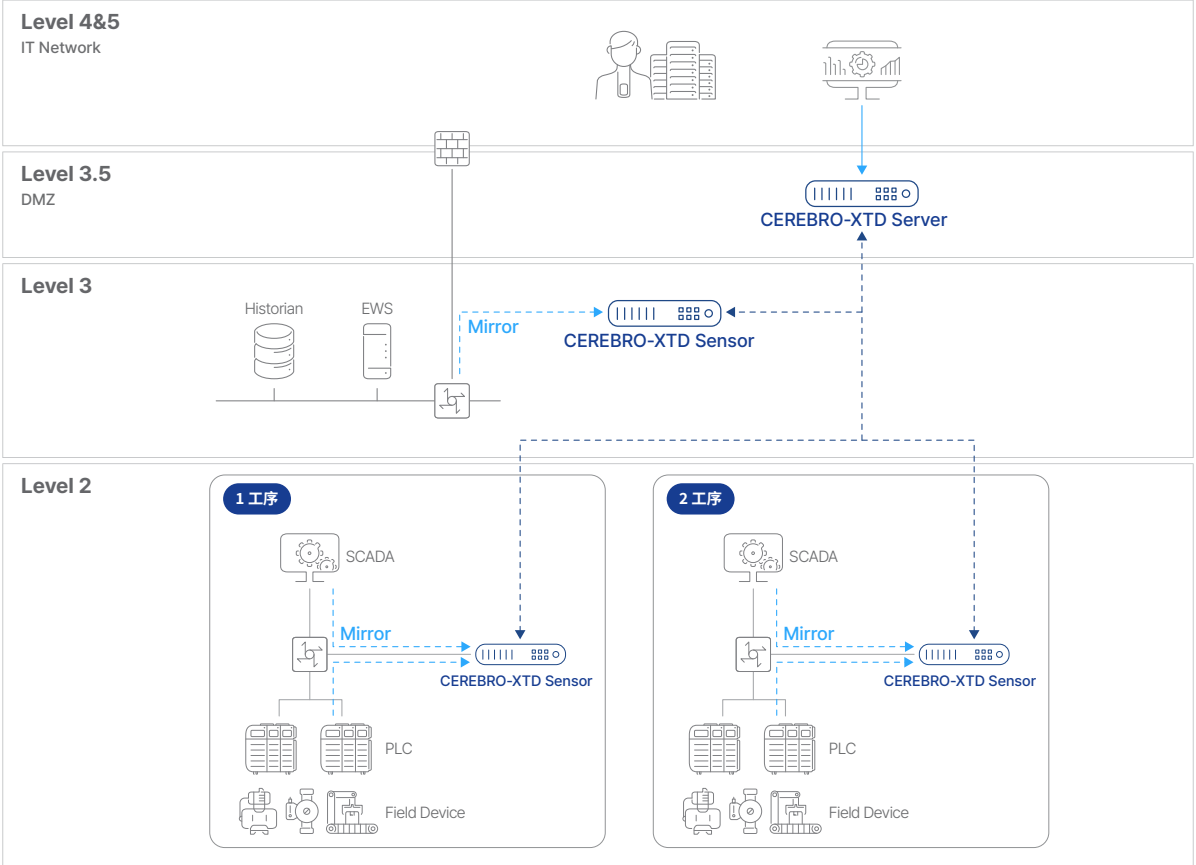
[图6] AhnLab EPS vs 传统防病毒产品

可在EPS中央管理服务器上进行恶意代码检测和分析，确保运营稳定性。其特点是由安装在终端系统中的超轻量Agent（EPS Agent）、中央监控和策略管理服务器（EPS Server）组成。并且在Windows XP等旧型操作系统、各种Linux发行版环境和嵌入式环境也支持Agent运营。

另外，AhnLab于2022年末推出了大型制造设备专用的安全解决方案“AhnLab EPS Relay”，它可针对OT环境中的资产提供可见性和安全管理功能。“AhnLab EPS Relay”提供可见性和安全管理功能，例如可▲识别位于封闭网络内的多个大型资产、▲并针对相应资产，统一应用拦截未经授权的应用程序、媒体控制、安全策略设置等“AhnLab EPS”的主要安全功能。通过使用“AhnLab EPS Relay”可以识别独立封闭网络中资产的数量和类型，安全情况等信息来确保可见性，而这些信息是很难通过以往基于网络数据包或协议识别资产的OT安全解决方案得到确认的。

CEREBRO-XTD

CEREBRO-XTD由AhnLab和Naonworks联合开发，可提供综合OT网络可见性，并实时检测安全威胁和异常行为。考虑到OT环境强调可用性的特点，能够以不影响设备运营的“被动监控”方式运行，增加了运营稳定性。



[图7] CEREBRO-XTD运营结构

CEREBRO-XTD的特点是能够与AhnLab的OT端点安全产品群联动，支持端点区域的可见性和恶意代码扫描和修复。此外，通过对多种OT协议的DPI（Deep Packet Inspection，深度包检测）分析技术，支持识别各类设备和针对异常控制逻辑的检测分析能力。

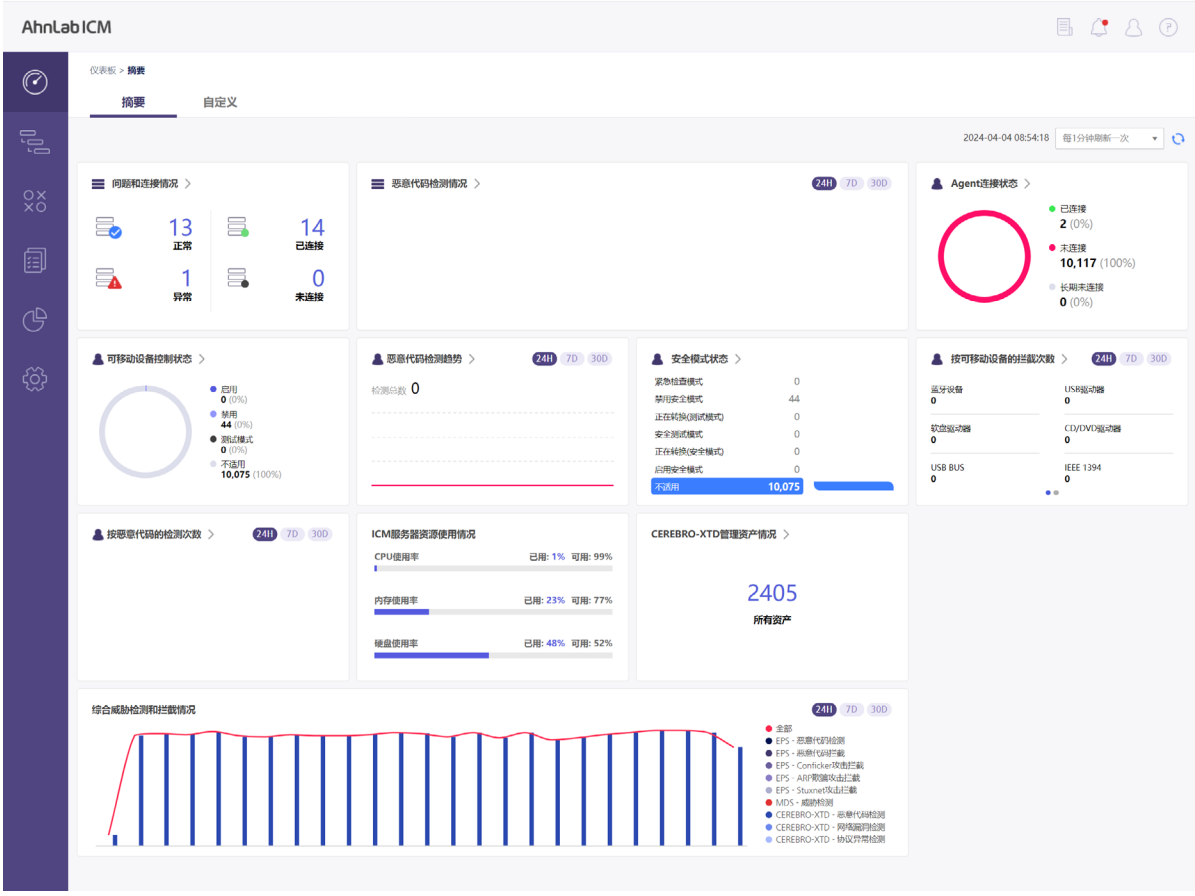
将CEREBRO-XTD与“AhnLab EPS”联动，可将可见性扩展到连接至OT网络的端点。一般的同类解决方案只提供至网络区域的资产状态。而CEREBRO-XTD通过与AhnLab EPS的联动，不仅可以提供网络区域数据，还可以提供连接到OT网络的服务器、工作站（Workstation）的操作系统补丁版本等详细的端点信息。

与AhnLab Xcanner联动时，还可以扩大恶意代码扫描区域。若初期在网络中检测到恶意代码传播或利用漏洞的恶意流量，则可以对位于端点区域的可疑系统再次执行恶意代码扫描。此外，不同于仅提供网络内安全威胁检测的大部分同类解决方案，还可以扫描恶意代码以查找威胁来源，从而实现更主动的威胁响应。

另外，还提供“威胁追溯（Threat Tracking）”功能，通过反向追踪检测到的威胁的传播路径，告知威胁信息。通过该功能，可以确定传播攻击的先前分发站点，从而识别攻击的传播和移动路径。由此用户可以确认检测到的威胁事件的传播路径和最初发生的资产等威胁之间的关联性，从而进行系统的威胁响应。

AhnLab ICM

在运行各种安全解决方案时，必须对解决方案检测到的信息和各种事件整合起来进行收集、监控和分析，从而缓解安全复杂性并提高效率。从这一点来看，AhnLab ICM能够支持OT环境的集成管理。



[图8] AhnLab ICM仪表板

用户可以通过直观的界面进行系统监控和日志分析。此外，通过各种报告和通知功能，用户可以采取适当的措施来更有效地管理系统，并降低管理过程中产生的总拥有成本（TCO）。目前，我们将端点解决方案AhnLab EPS、Xcanner、MDS与网络解决方案CEREBRO-XTD进行集成管理，并计划在日后持续扩大范围。此外，AhnLab ICM将通过与本公司威胁情报平台“AhnLab TIP”联动，针对从各安全解决方案收集的威胁信息，提供额外的内容分析等。

AhnLab Xcanner

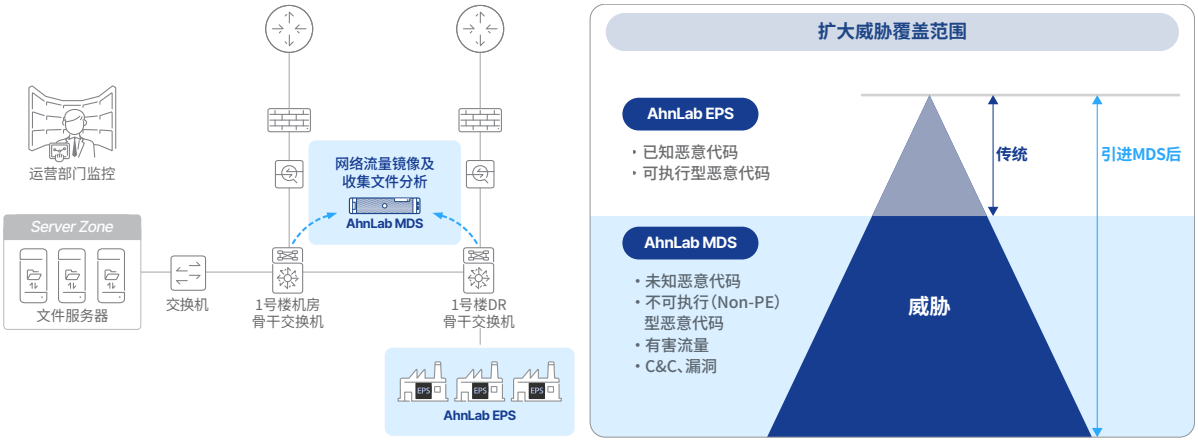
因OT环境的特点，存在一些无法安装Agent的系统。对于此类系统，可以通过非驻留型防病毒解决方案AhnLab Xcanner，以便携方式执行恶意代码扫描和修复。恶意代码感染系统很难进行实时响应，随着对此采取安全措施的必要性日益增加，还支持管理员对被感染系统进行有效的事后修复。此外，AhnLab Xcanner通过与Ahnlab EPS联动，EPS服务器管理员可以远程运行AhnLab Xcanner，执行进一步的恶性代码扫描和修复。

[图9] AhnLab Xcanner界面

在AhnLab Xcanner中可以设置扫描与修复选项，从而能够根据运营状况进行响应。并且可以对不需要扫描的文件夹或文件进行例外设置，用户可以更高效地运用。此外，无需删除先前安装的安全Agent，能够最大程度地减少冲突，因此不会对运营造成影响便可执行扫描和修复。

AhnLab MDS

近期，随着网络威胁持续升级，高级持续性威胁（Advanced Persistent Threat: APT）和新/变种恶意代码呈日益增加趋势。因此除了现有已知（Known）恶意代码，还需要对未知（Unknown）恶意代码进行分析和响应。



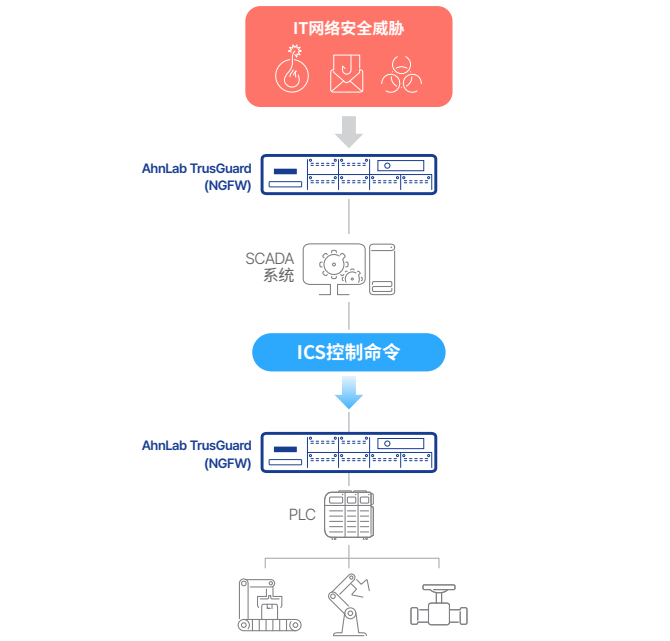
[图10] 通过AhnLab EPS与AhnLab MDS链接，扩大威胁覆盖范围

AhnLab MDS是AhnLab基于沙箱的APT响应解决方案，能够收集和分析生产网络流量中存在的文件，并对未知恶意代码进行动态分析。此外，还能够检测和分析攻击者的C&C IP连接，支持对OT网络恶意代码传播路径、C&C、漏洞等各种安全威胁的监控和对被感染设备的修复和响应。

与检测并响应已知恶意代码的AhnLab EPS链接时，便可防御已知和未知恶意代码，从而扩大综合威胁响应覆盖范围。

AhnLab TrusGuard

在网络领域，新一代防火墙AhnLab TrusGuard发挥着关键作用。首先，它能够检测OT网络边界的有害流量并拦截访问，同时还支持IPSec、SSL VPN等安全通信和网络分段等功能。

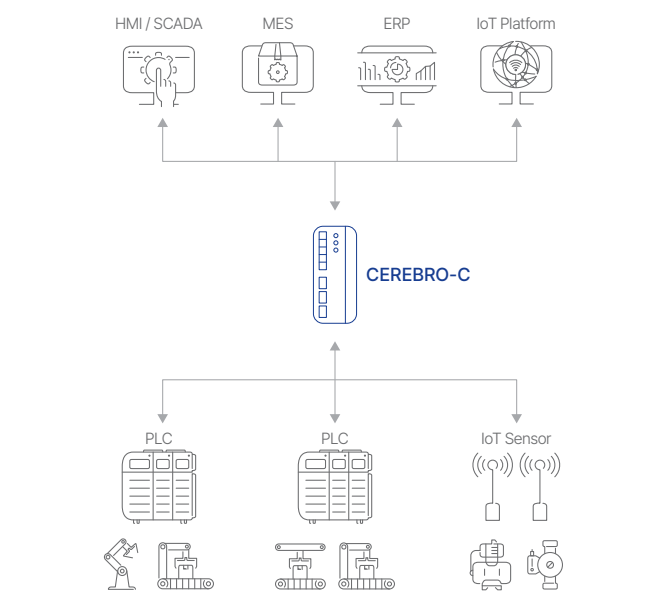


[图11] AhnLab TrusGuard OT安全威胁响应结构

此外，通过应用Naonworks的ICS协议分析技术，可以在OT网络内详细控制工业协议。具体来说，不仅可以控制Modbus、DNP3等各协议，还可以识别并控制功能代码（Function Code）。

CEREBRO-C

Naonworks的CEREBRO-C是用于集成管理OT和ICS网络的工业协议网关。通过将各种设备的协议转换为具有安全性的OPC-UA、MQTT等标准协议并进行传输，加强控制网络的安全性。



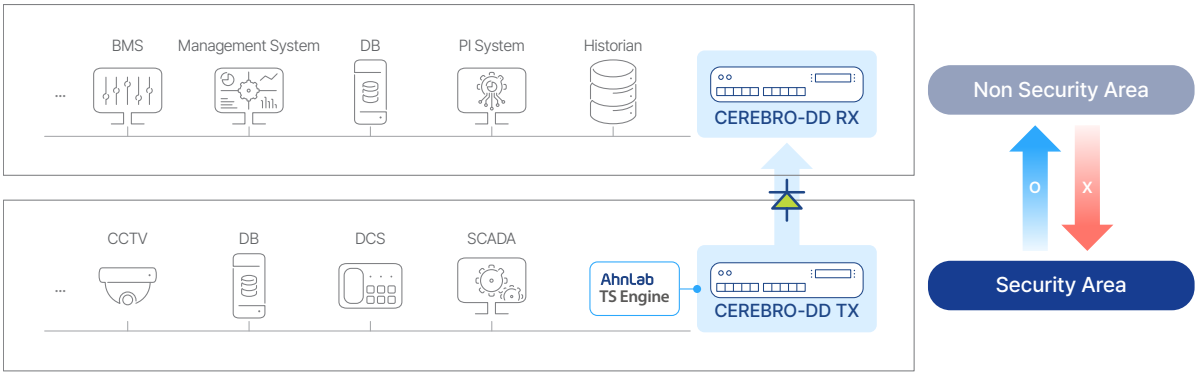
[图12] CEREBRO-C运行结构

CEREBRO-C具有良好的兼容性，可连接现场总线（Fieldbus）、以太网（Ethernet）等各种设备，与上层系统接口联动，支持Windows/Linux/容器多平台等。在构建以数据收集与链接和现场集成管理为目的的系统，或引进新设备时，无需改变现有网络配置便可解决不同通信协议带来的联动问题。

CEREBRO-DD

OT安全的重要要素之一就是网络隔离。这是为了防止安全级别较高的OT网络的数据被泄露，并拦截来自外部网络的恶意代码等威胁和访问。然而，最近随着OT和IT之间连接的重要性不断增加，对在相互隔离的网络之间进行安全数据传输的需求也越来越多。

“物理单向”能够实现不同安全级别网络之间的数据链接，从源头上阻止外部对OT等安全领域的安全威胁。CEREBRO-DD是物理单向安全解决方案，能构建从OT到IT的安全数据传输环境，全面保护OT网络。



[图13] CEREBRO-DD概念图（TX：发送服务器/RX：接收服务器）

为了加强安全性，CEREBRO-DD在单向通信区间使用未知协议。此外，还应用AhnLab的防病毒引擎进行多方位扫描。传输资料时会进行策略扫描、签名扫描、恶意代码扫描，以保证数据稳定性。

结论

OT环境的安全威胁正日益加剧。与IT环境相比，其造成的损害影响更为严重，甚至可能涉及到社会问题或给企业带来巨大损失。因此，人们对OT安全的关注每年都在增加。然而，由于OT环境具有与传统IT环境不同的特点，因此停止设备运行并引进安全解决方案并不容易，因此许多企业尚未采取积极措施。然而，由于每年OT安全事故发生率都在增加，因此认为现在是积极思考OT安全的时候，而不是坐视不管。

OT安全可能仍然在技术上感到陌生和困难。如果是这样的话，希望您记住以下三点：

#1. 为了保护OT环境，也必须考虑IT安全

OT环境的安全威胁也源自与OT环境相连的IT环境，一旦OT领域遭受入侵，损害可能会迅速扩散。这就是为什么需要IT和OT融合安全的原因。

#2. OT安全基本上需要“识别>检测>响应”流程

在OT环境中，资产或网络变化较少。因此，需要确保对资产的可见性，并通过识别基线来检测安全威胁，并采取适当的响应措施。

#3. 为了OT安全，需要能覆盖OT环境全层的集成OT安全框架

IT和OT融合安全根据网络划分为IT网络、OT运营网络和OT控制网络。根据每个层级的特点，需要采取适当的安全措施，并建立一个从何考虑管理和适当的安全解决方案的OT安全框架。

AhnLab与Naonworks合作，作为最佳OT安全合作伙伴，将继续推进集成OT安全框架走向尖端化。如今OT安全的重要性愈加突显，我们希望有更多的企业能够建立坚实的安全体系，创造安全的业务环境。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 (邮编: 100102) | 上海市闵行区万源路2158号 泓毅大厦1201室 (邮编: 201113)
https://www.ahnlab.com/cn
cn.sales@ahnlab.com
电话： +86 10 8260 0935/8（北京）| +86 21 6095 6780（上海）