1.行业背景

2017 年 5 月 12 日全球勒索病毒爆发，席卷了国内多个行业，其中包括政府、交通、金融、教育、医疗等行业，当然能源行业也在所难免。面对全球网络安全威胁的大环境下，能源行业需要加强网络安全建设，保障业务数据的安全性，使集团的生产系统可以抵御 APT、勒索病毒、恶意代码等新型未知威胁的攻击；从而增强集团公司网络安全防护、应急响应处置和指挥调度能力，提高网络安全综合防御水平。

2.痛点及需求

能源行业的痛点在于：

1. 提供服务的关键基础设施安全防护问题

能源行业有大量对外提供服务的关键基础设施，这类终端的操作系统比较老，被利用的漏洞多，而且终端使用者在安全意识方面较为薄弱，导致抵御勒索病毒、未知威胁攻击、恶意代码植入等高级威胁的防护能力较差，往往易被攻击者利用，通过这类终端为跳板做进一步信息收集或破坏。

2. 生产网内部之间防护隔离欠缺问题

能源行业网络架构复杂，涉及互联网、管理网、生产网等网络。互联网和管理网的网络边界间安全建设较为成熟，但生产网内部安全边界及区域划分较为模糊，例如：过程控制层与数据采集层之间；先进控制（APC）系统与过程控制网之间；控制器与操作员站（工程师站）之间，缺少网络安全防护。这类生产网内部区域一旦某节点出现未知威胁攻击，会迅速蔓延整个生产网络。

3. 传统安全领域与新安全技术相结合需求

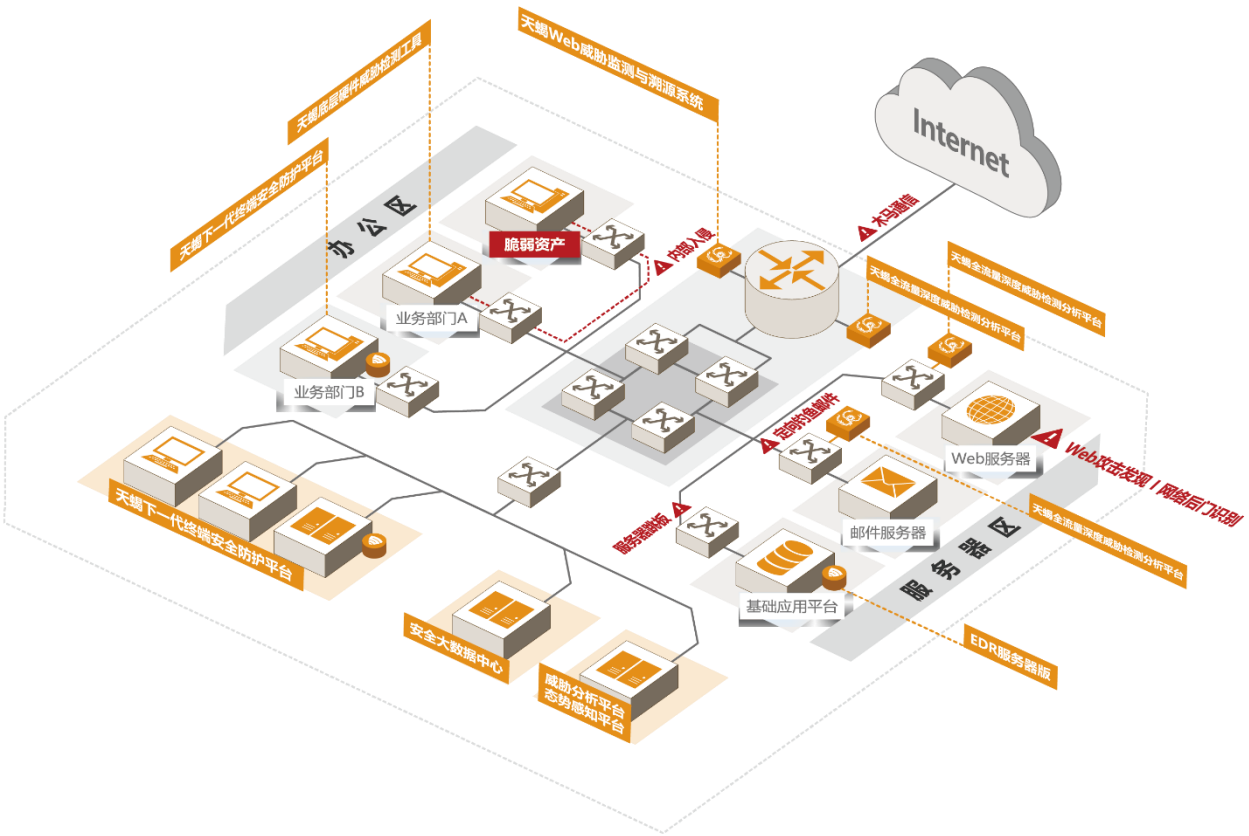
网络安全建设的重要性在互联网高速发展的时代日益凸显，各种网络攻击给用户带来了不可估量的损失。如果攻击者利用一个高危漏洞进行威胁攻击，就可能给集团内部的生产系统带来难以预估的安全风险。传统防御技术面对已知威胁，可以在短的时间内做出有效响应。但传统网络安全技术面对 0day、后门利用、钓鱼邮件等层出不穷的攻击方式下，传统防御技术就不能更快检测出威胁并做出

响应。传统防御技术与新安全技术的有效结合，可以对已知和未知领域的威胁进行有效的识别、侦测以及响应。

能源行业的需求主要在于：

1. 提升关键信息基础设施对高级持续性威胁的防御能力。
2. 提升核心资产生产区之间安全防护能力。
3. 提升内网、外网服务器端对勒索软件病毒的识别、分析、阻断能力。

3.解决方案



产品拓扑图

在操作系统层面，采用安全可控的 Windows10 神州网信政府版桌面操作系统，首先解决操作系统层面安全问题。

在内部核心服务器上可部署天蝎下一代终端安全防护平台，同时在对外提供的服务器的边界可部署天蝎 Web 威胁监测与溯源系统产品。

- 天蝎下一代终端安全防护平台负责监测、分析和识别集团核心服务器、生产机器的威胁行为动态。
- 天蝎 Web 威胁监测与溯源系统负责监测对外提供的应用服务器，向用户提供威胁事件的分析、回溯和响应功能。
- 为保障集团业务的连续性，我方人员在不影响业务正常通讯的情况下进行了网络渗透作业，主要包括：威胁情报、风险评估、信息安全应急响应、渗透测试、安全宣传培训。

4. 客户认可的价值

- 识别并消除对关键物理和网络基础设施的任何重大弱点，阻断变异型勒索病毒等高级未知威胁；
- 为在发生攻击或环境事件时，关键基础设施所支持的业务功能的连续性仍然可行提供了保证。
- 通过专业的渗透测试手段直接展示集团信息系统安全现状，全方位地搜集、检测、发现敏感信息、实验、攻击，尽可能地突破现有安全防范体系，获得对信息的越权操作。帮助安全人员直观地了解到目前业务系统的安全现状，为后续的安全工作提供支撑。
- 通过加强应急演练，提高集团人员的应急响应处置能力。
- 提高集团的网络安全防御体系的网络安全感知能力。