作者版权所有
请勿转载

安全数字世界

预建未来
PLAN UP

作者版权所有
请勿转载

作者版权所有
请勿转载

工业互联网安全应急响应

李培信
北京天地和兴科技有限公司 技术工程总监

作者版权所有
请勿转载

工业安全应急响应

作者版权所有
请勿转载

- 应急响应

工业企业为了应对突发或重大信息安全事件的发生所做的准备，以及在事件发生后所采取的措施。

- “事件”触发

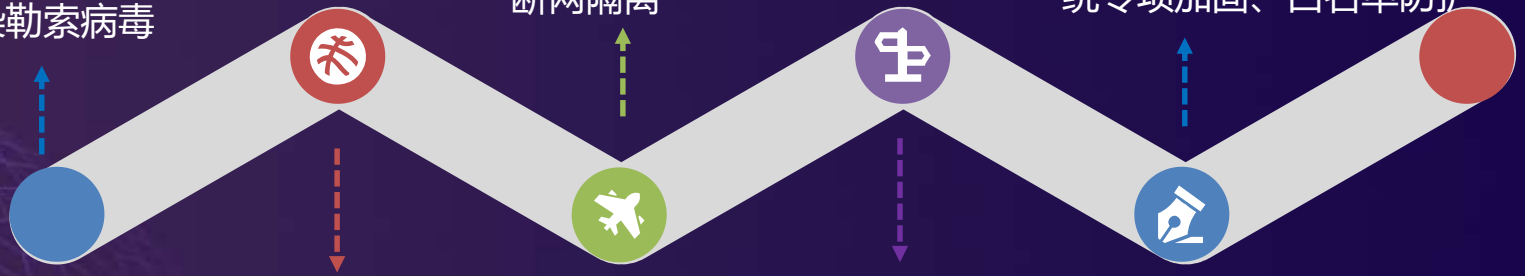
应急响应是一种被动性的安全体系，它是持续运行并由“事件”触发的体系。

作者版权所有
请勿转载

勒索病毒事件应急响应案例

C3安全峰会
CYBER · CLOUD · COMMUNICATION

作者版权所有
请勿转载



安全事件

感染勒索病毒

影响范围

短时间内大面积感染，部分生产管理系统瘫痪

临时处理措施

断网隔离

影响范围

远程暴力破解并植入病毒

处置方案

病毒清除、数据恢复、系统专项加固、白名单防护

作者版权所有
请勿转载

应急响应方法论（PDCERF）

作者版权所有
请勿转载

01 准备 Preparation

02 检测 Detection

03 抑制（封锁） Containment

04 根除 Eradication

05 恢复 Recovery

06 跟踪 Follow-up

作者版权所有
请勿转载

准备（Preparation）

作者版权所有
请勿转载

建立应急预案

明确事件处理流程
明确事件发布和汇报流程
制定定期演练机制

建立应急组织

明确第一责任人
明确组织结构、人员、职权

增强原有系统安全性

风险评估
问题整改

建立全局监控系统

态势感知
事件预警

作者版权所有
请勿转载

检测（Detection）

作者版权所有
请勿转载

确定事件性质

明确事件范围

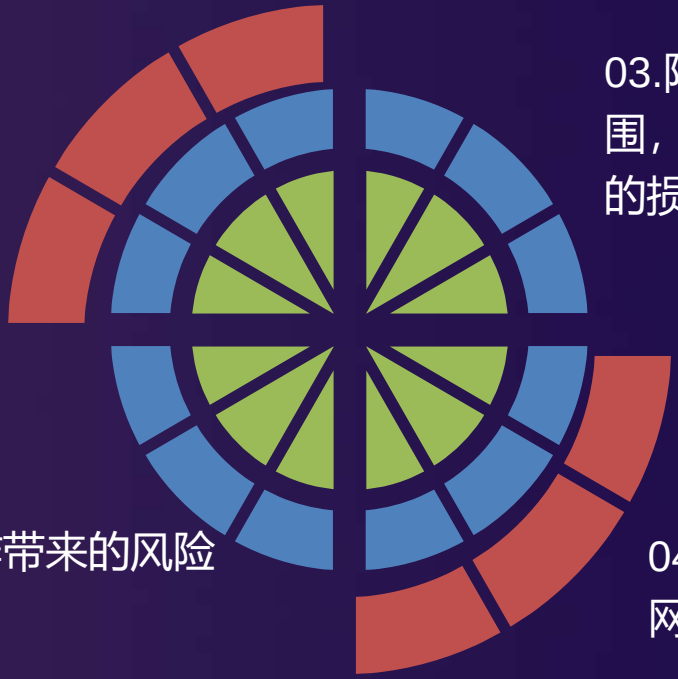
确定应急等级

作者版权所有
请勿转载

抑制或封锁（Containment）

作者版权所有
请勿转载

01.初步分析，确定适当的封锁方法



03.限制攻击的范围，同时限制潜在的损失和破坏

02.确定封锁操作带来的风险

04.确保封锁方法对各网业务影响最小

作者版权所有
请勿转载

根除（Eradication）

作者版权所有
请勿转载

01.详细分析，
确定原因

02.分析漏洞，
并修补漏洞

03.重新审视安
全保障策略

04.找出事件根源并
彻底根除

作者版权所有
请勿转载

恢复（Recovery）

把所有受侵害或被破坏的系统、应用、数据库等彻底地还原到它们正常的任务状态

安全措施实施后，重新数据备份

服务重新上线

持续监控

作者版权所有
请勿转载

作者版权所有
请勿转载

跟踪（Follow-up）

作者版权所有
请勿转载

作者版权所有
请勿转载

工控系统应急响应的特殊性

作者版权所有
请勿转载

安全事件可以直接波及生产控制设备，造成物理或人员伤害

操作指令、业务逻辑合理性风险难以判断

优先保证系统可用性、业务连续性

作者版权所有
请勿转载

应急工作服务体系

作者版权所有
请勿转载

应急技术支撑

威胁情报分析

安全事件应急响应

安全事件应急处置

安全风险持续监控

作者版权所有
请勿转载

工业互联网的新变化

作者版权所有
请勿转载

新技术、新标准带来新风险

工业系统连网带来安全风险提高

工控安全标准与政策落地需要时间

安全事件的不可预测性

作者版权所有
请勿转载

作者版权所有
请勿转载

Thank You

作者版权所有
请勿转载