

安世加

"Face the challenge, Embrace the best practice"

EISS-2020 企业信息安全峰会 之上海站

2020年11月27日



安全事件管理自动化之路

——坑与梯

沈勇

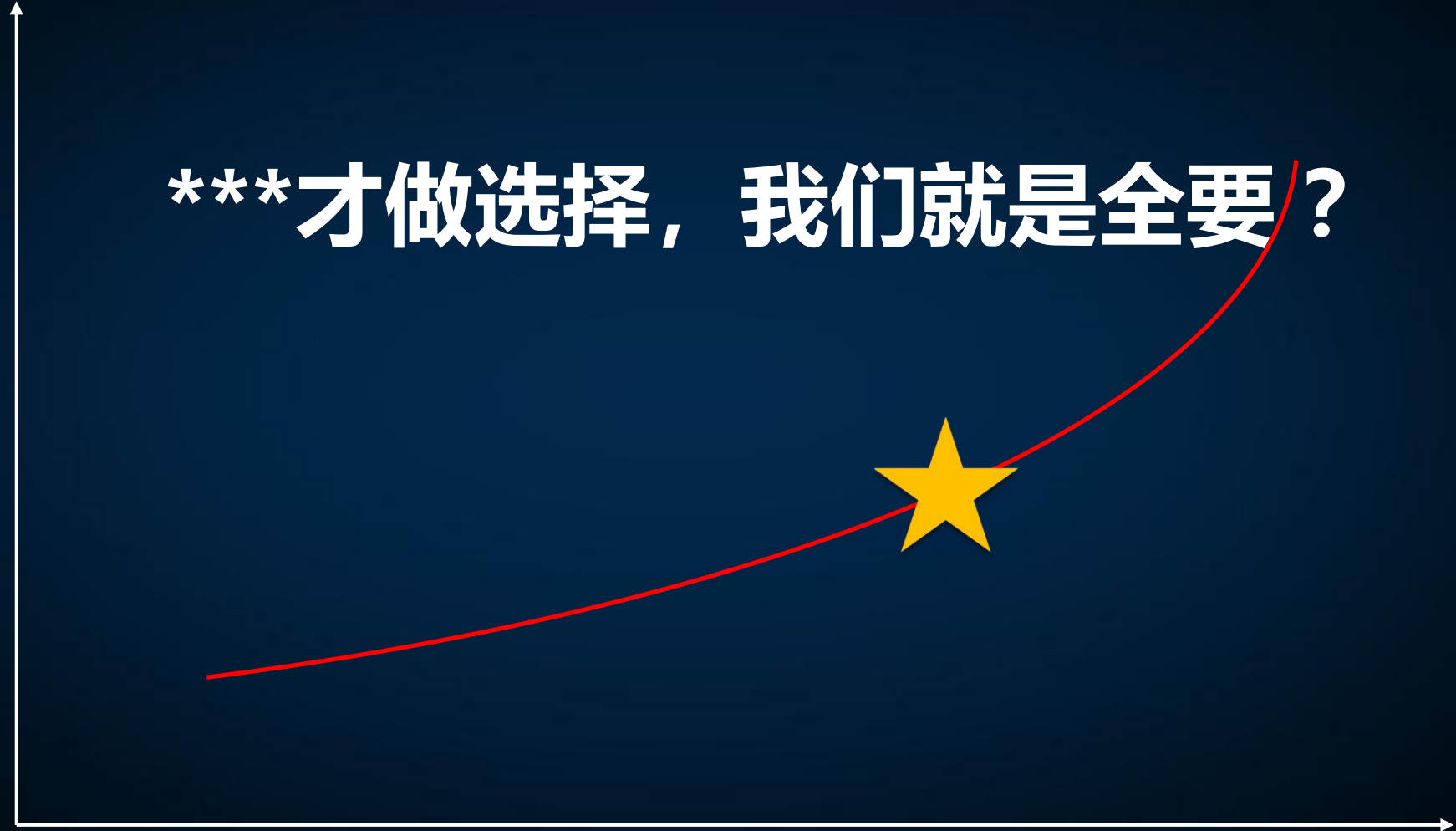
2020-11-27

安世加



1. 准备

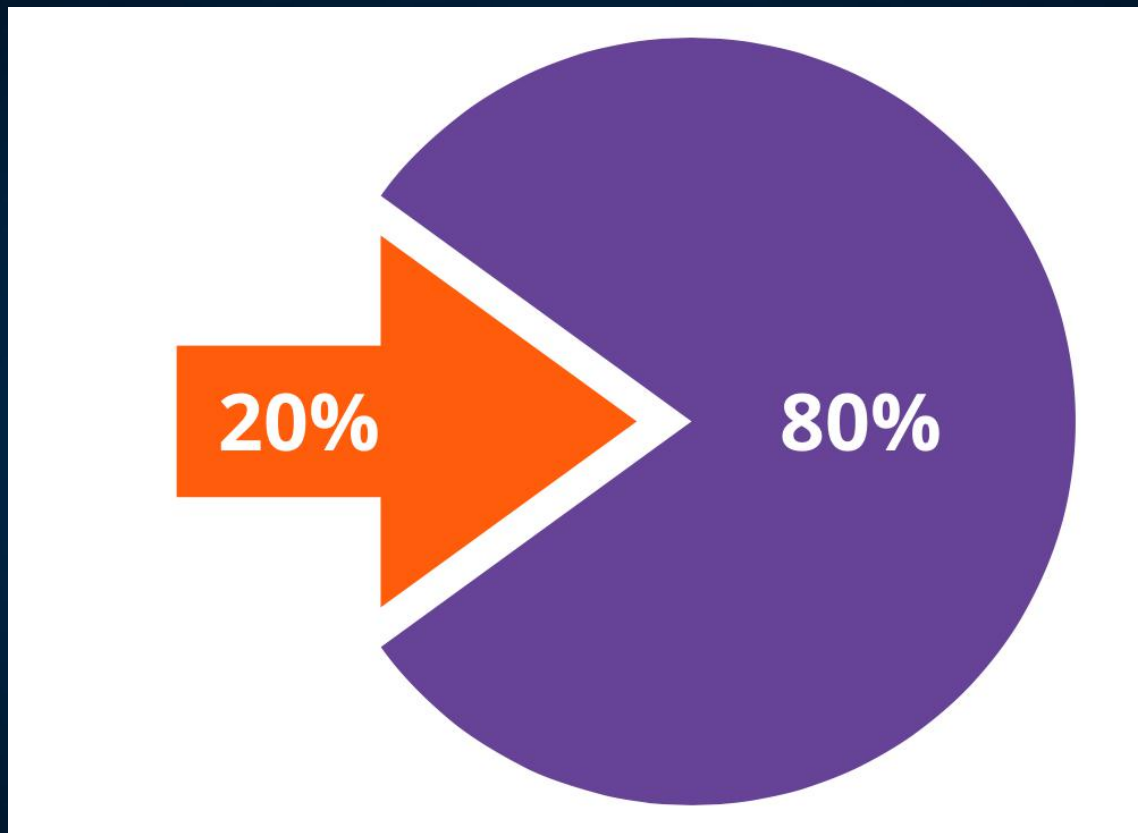
***才做选择，我们就是全要？



A graph with a red curve and a yellow star. The curve starts at a low point on the left and rises steeply towards the right. A yellow star is placed on the curve, marking a specific point. The graph is set against a dark blue background with white axes.

数据源、工具、预置规则数量

1. 准备



慎重选择

深广兼顾

突出重点

不断评价

随时调整



2. 检测|分析



不准、误报

换源
多源关联
SOAR自动交叉验证*



告警太多

规则引擎压缩*
多源关联
AI模型*

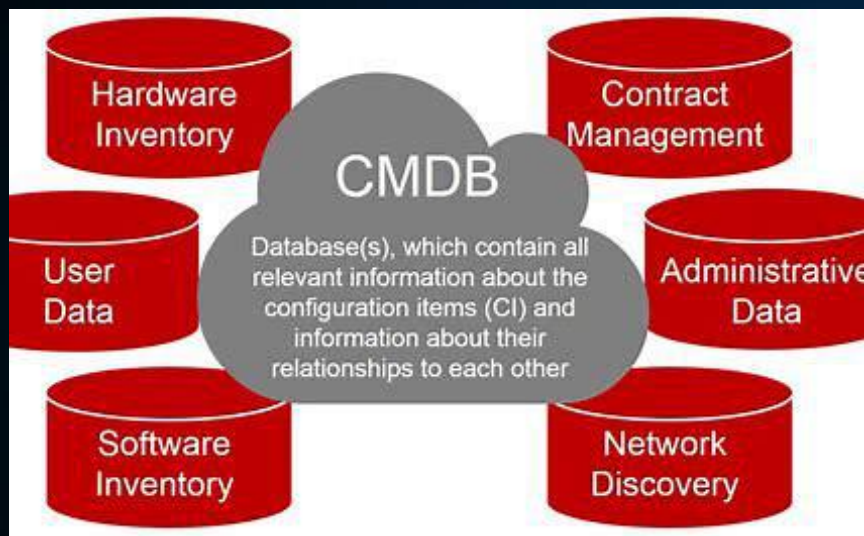


漏报

人工发现转规则
ATT&CK覆盖率*
威胁狩猎



3. 遏制|根除|恢复



**CMDB信息不准/缺失;
人、资产找不到**

**推动改进
自己动手***



**缺少工具API:
WAF/FW/EDR...**

**找工具厂商
换工具厂商
求助兄弟团队、自己动手**



缺编排调度

**SOAR
剧本积累/优化**



4. 事后活动



评价响应速度

MTTD (分段) *
MTTR (分段) *



评价工具能力、数据质量

数据源对有效告警的贡献率*
各情报源的价值贡献*
安全工具的调用量、成功率



评价积累的数据

规则/模型准确率
剧本调用量、成功率

欢迎联系

沈勇

- 平安科技 安全产品专家
- 云安全联盟（CSA）上海分会联席主席
- 云安全联盟（CSA）CSA认证讲师
- CCSK 4.0认证中文教材、CCSSP认证教材编组成员
- 世界经济论坛金融科技网络安全联合会网络安全工作组成员
- 2项国际PCT专利申请；获美、日等5个国家专利

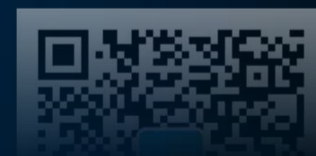


安世加

安世加 专注于安全行业，通过互联网平台、线下沙龙、培训、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站: <http://anquanjia.net.cn/>

微信公众号: asjeiss



安世加