



2016 中国互联网安全大会  
China Internet Security Conference

协同联动 共建安全+命运共同体

# 云时代的威胁感知与攻防转换之道

崔勤

qin.cui@chaitin.com  
长亭科技

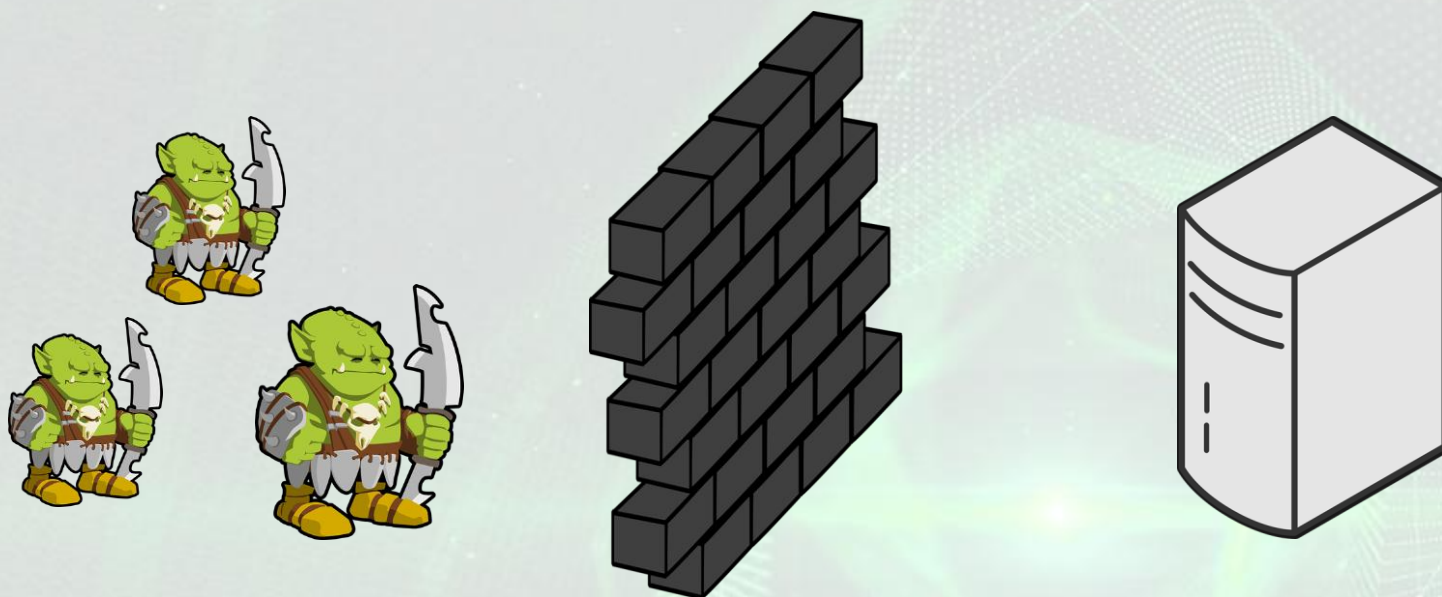
# 过去的防御思想



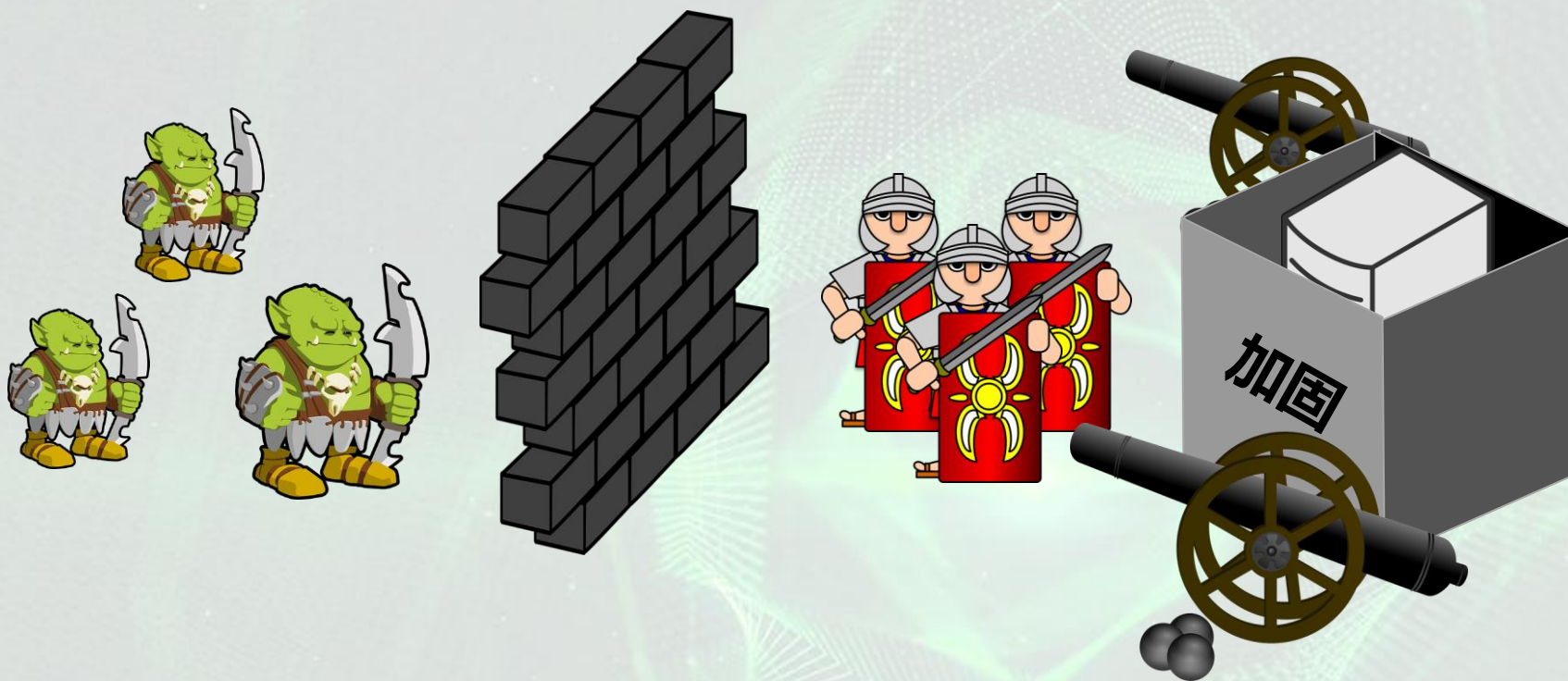
中国互联网安全大会



360互联网安全中心



# 现在的防御思想







攻击者视角更广

# 案例



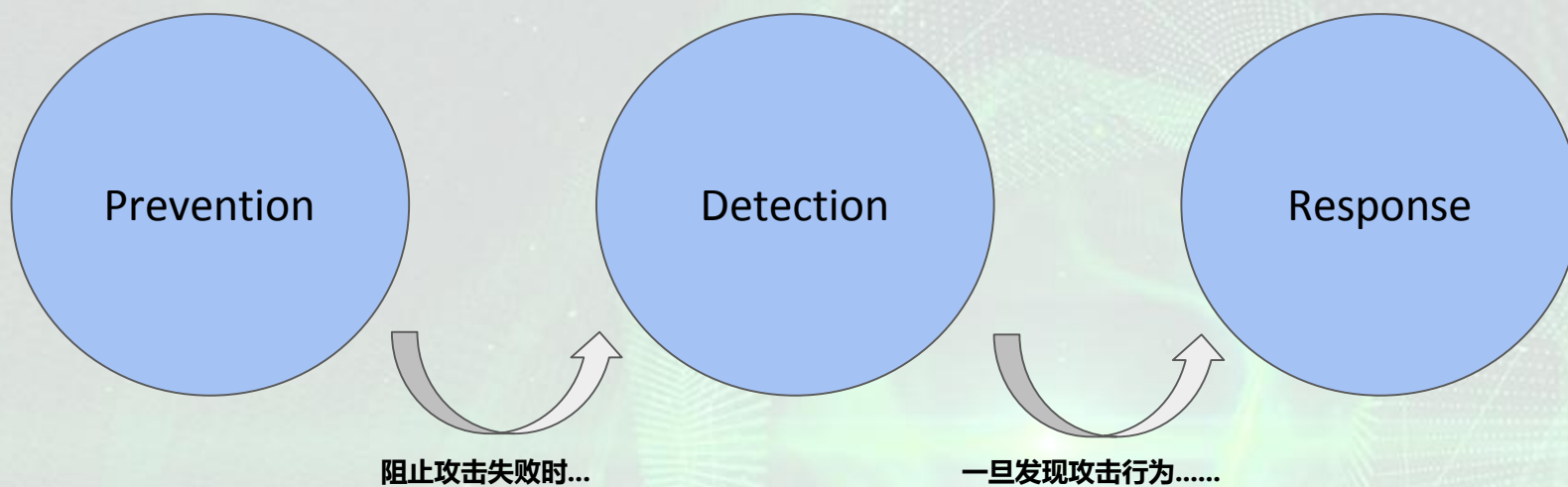
中国互联网安全大会



360互联网安全中心



# 攻防转换





# 安全厂商变化



Source : Momentum Partners

# 威胁感知



中国互联网安全大会



360互联网安全中心



阻止不了威胁，如何第一时间发现威胁？





**Firewall  
Bypass**



**Recon**



**Privilege  
Escalation**



**Data  
Disclose**



# 利用传统蜜罐检测攻击



中国互联网安全大会



360互联网安全中心



- 优点
  - 攻击威胁感知
  - 攻击行为记录
- 缺点
  - 特征明显，容易被识破
  - 易部署，难维护
  - 仅仅是发现攻击
- 目的不同
  - 公网收集情报，不适用于内网场景

Deception technologies are defined by the use of deceptions and/or tricks designed to thwart, or throw off, an attacker's cognitive processes, disrupt an attacker's automation tools, delay an attacker's activities or disrupt breach progression. For example, deception capabilities create fake vulnerabilities, systems, shares and cookies. If an attacker tries to attack these fake resources, it is a strong indicator that an attack is in progress, as a legitimate user should not see or try to access these resources. Deception technologies are emerging for network, application, endpoint and data, with the best systems combining multiple techniques. By 2018, Gartner predicts that **10 percent of enterprises** will use deception tools and tactics, and actively participate in deception operations against attackers.

Source: Gartner Identifies the Top 10 Technologies for Information Security in 2016



# 旧技术新思路



中国互联网安全大会



360互联网安全中心



**RSA**<sup>®</sup>Conference | Where the world  
talks security

**TRAPX**  
SECURITY



illusive

# 基于伪装欺骗技术的蜜罐



中国互联网安全大会



360互联网安全中心



# 蜜罐的改进



中国互联网安全大会



360互联网安全中心



- 真实的服务
- 全局的监控
- 易部署、易管理
- 数据的关联



# 伪装欺骗



- 具有更高的价值
- 阻止或者摆脱攻击者的认知过程

# 攻击者视角的变化



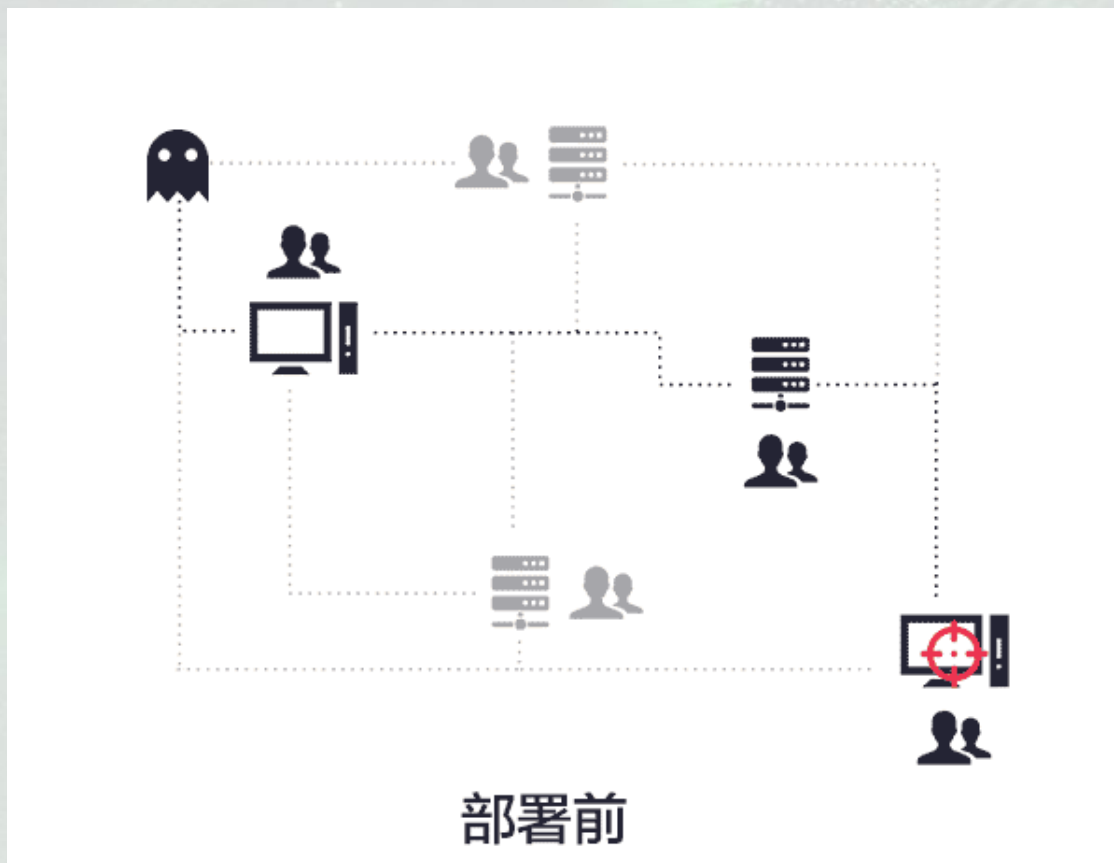
中国互联网安全大会



360互联网安全中心



长亭科技  
CHAITIN.CN



# 不仅如此.....



中国互联网安全大会



360互联网安全中心



我们还需要做的事情

- 保持与业务场景一致
- 有效的迷惑、拖延攻击者
- 更多的联动



# 内网威胁感知威胁系统



中国互联网安全大会



360互联网安全中心



## 内网威胁感知系统

- 使用基于真实服务的伪装欺骗技术
- 适配业务场景
- 事件关联能力
- 企业内部威胁情报

# 基于真实服务的伪装欺骗技术

- 真实服务 + patch 记录行为
- 伪装欺骗技术阻碍攻击者认知过程



目的：发现攻击威胁，确认攻击威胁



# 适配业务场景



中国互联网安全大会



360互联网安全中心



- 根据部署环境，适配业务场景





# 事件关联能力



中国互联网安全大会



360互联网安全中心



- 建立安全防御体系的一个闭环
- 每个安全防御阶段的联动



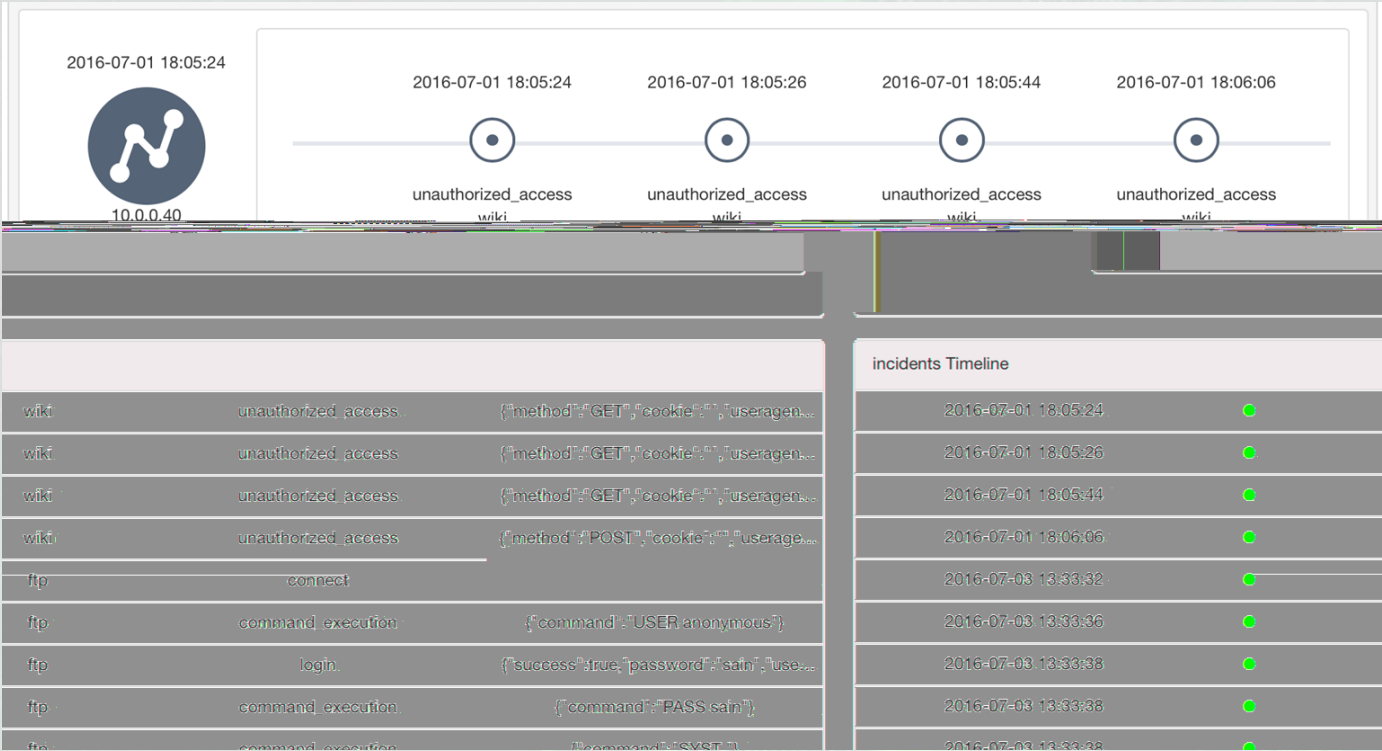
# 企业内网威胁情报



- 利用蜜网构建企业内部威胁情报
- 更多的威胁情报意味着更准确的发现企业弱点，同时可以抵御未知的攻击



# 攻击时间线





# 应用场景



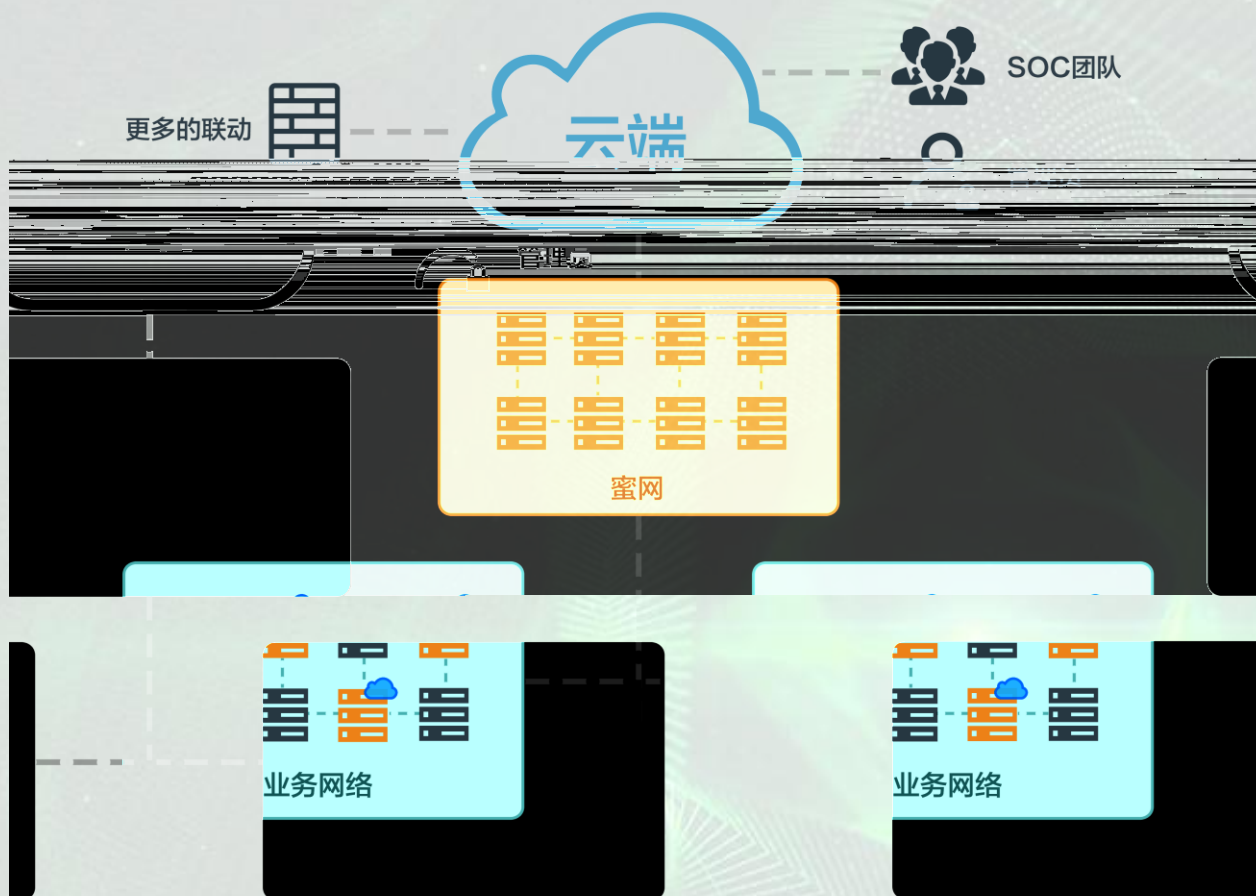
中国互联网安全大会



360互联网安全中心



长亭科技  
CHAITIN.CN



# 总结

## 内网威胁感知系统

- 使用基于真实服务的伪装欺骗技术
- 适配业务场景
- 事件关联能力
- 企业内部威胁情报



# 谢 谢



中国互联网安全大会



360互联网安全中心