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

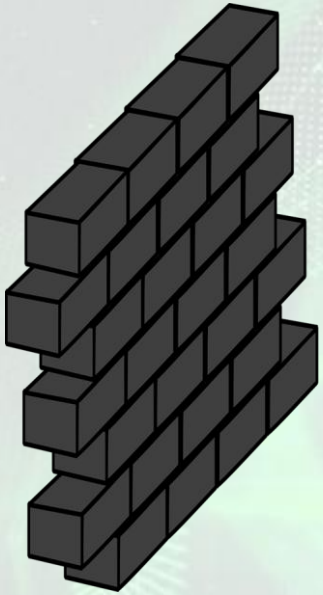
协同联动 共建安全+命运共同体

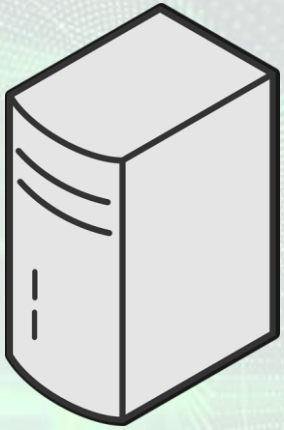
云时代的威胁感知与攻防转换之道

崔勤

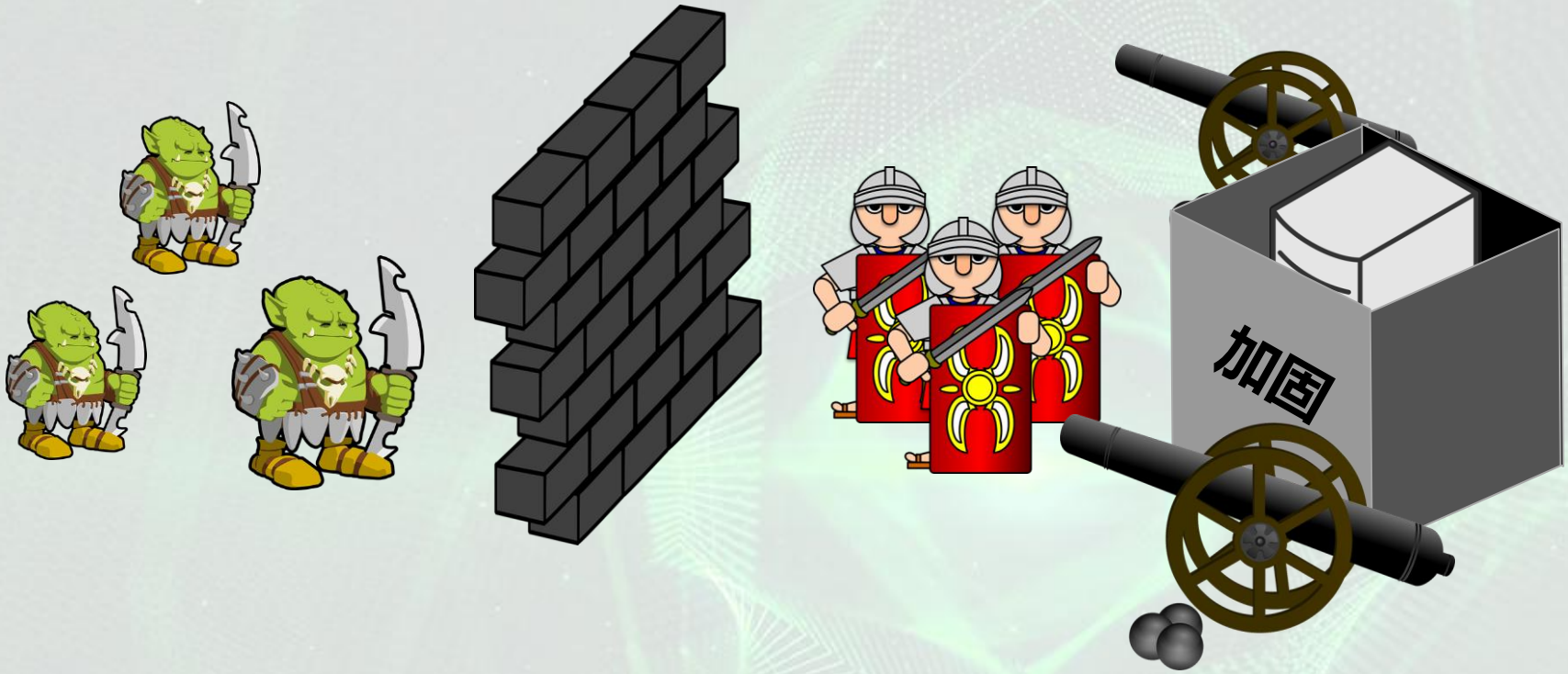
qin.cui@chaitin.com
长亭科技

过去的防御思想





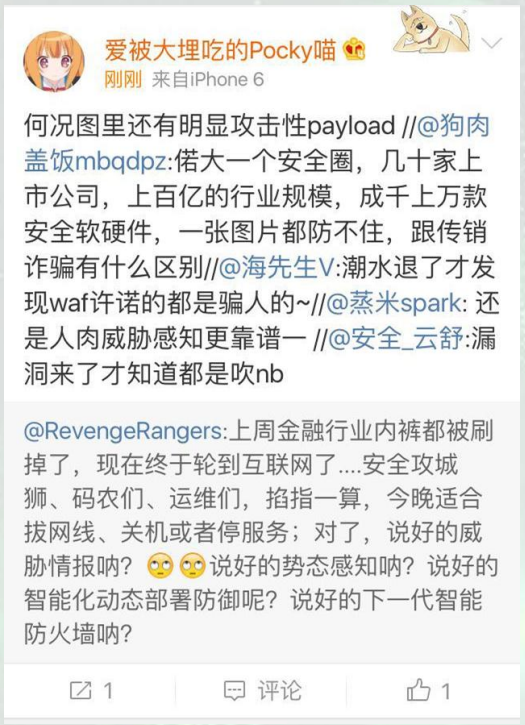
现在的防御思想



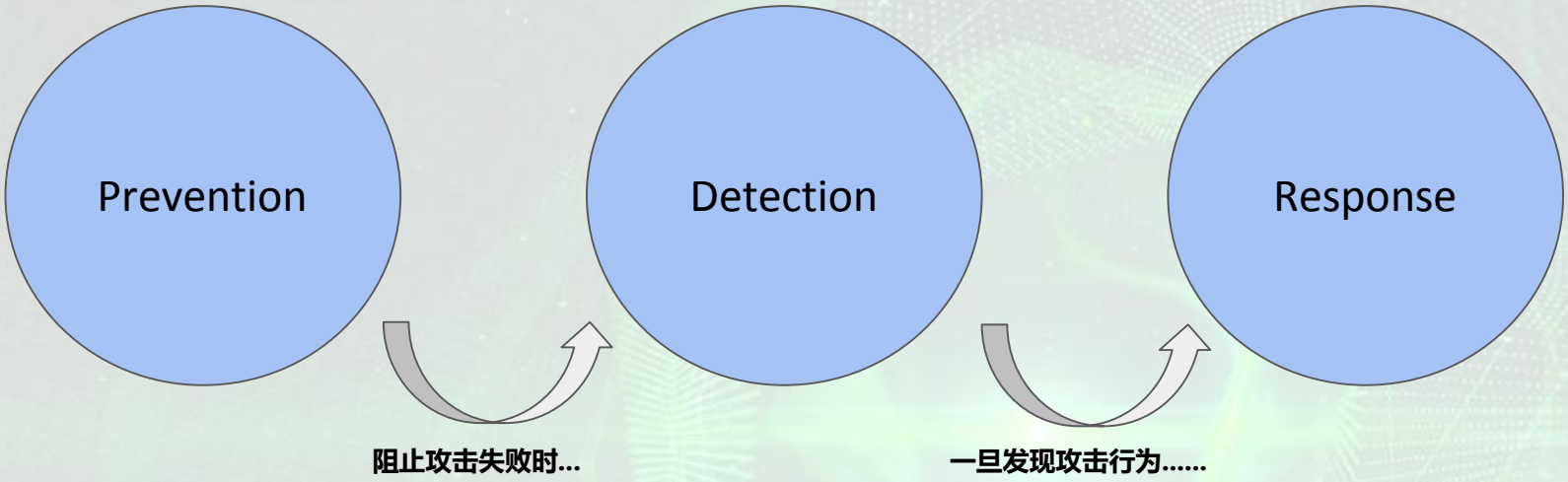
新时代攻击手段

攻击者视角更广

案例


爱被大埋吃的Pocky喵
刚刚 来自iPhone 6
何况图里还有明显攻击性payload //@狗肉盖饭mbqdpz:偌大一个安全圈，几十家上市公司，上百亿的行业规模，成千上万款安全软硬件，一张图片都防不住，跟传销诈骗有什么区别//@海先生V:潮水退了才发现waf许诺的都是骗人的~//@蒸米spark: 还是人肉威胁感知更靠谱一 //@安全_云舒:漏洞来了才知道都是吹nb
@RevengeRangers:上周金融行业内裤都被刷掉了，现在终于轮到互联网了....安全攻城狮、码农们、运维们，掐指一算，今晚适合拔网线、关机或者停服务；对了，说好的威胁情报呐？说好的势态感知呐？说好的智能化动态部署防御呢？说好的下一代智能防火墙呐？
1
评论
1

攻防转换



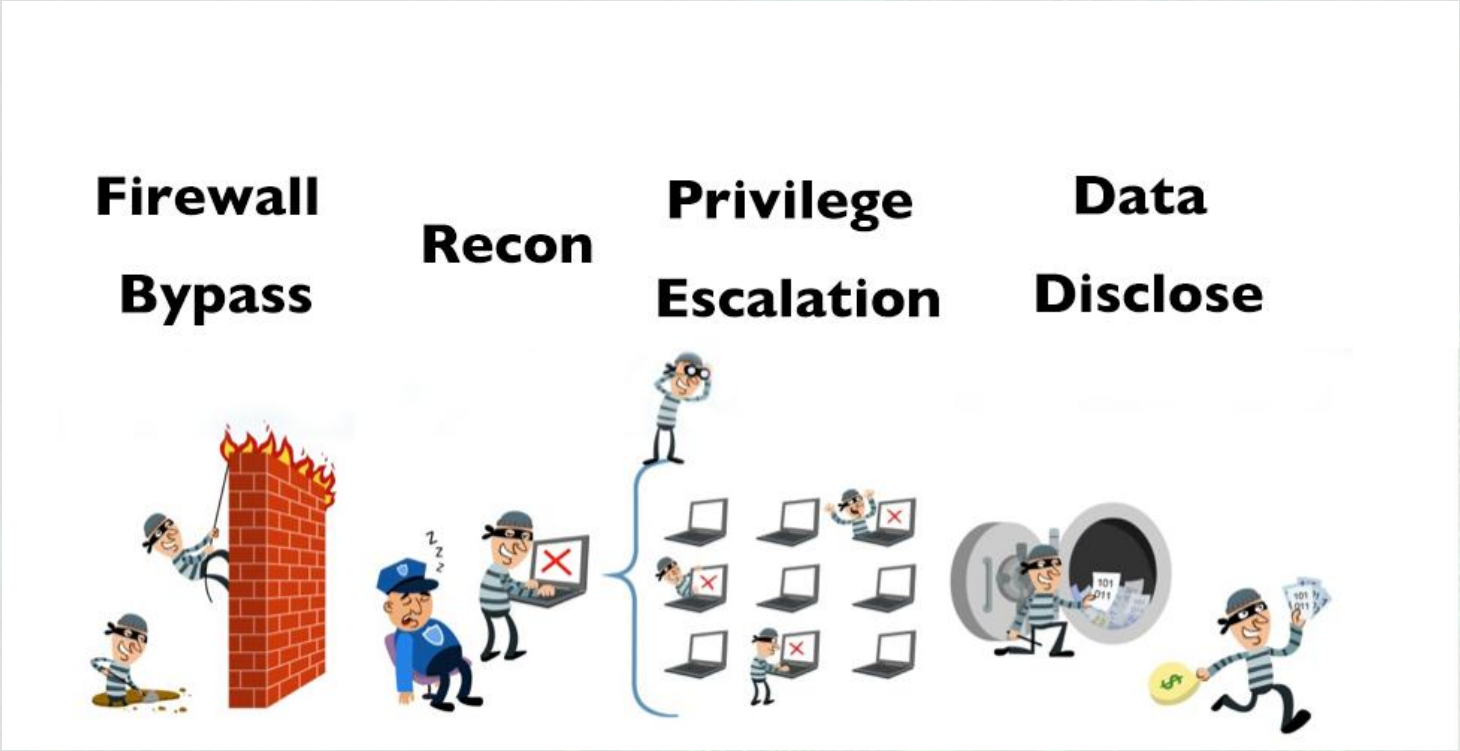
安全厂商变化

Source：Momentum Partners

威胁感知

阻止不了威胁，如何第一时间发现威胁？

攻击分析


Firewall
Bypass
Recon
Privilege
Escalation
Data
Disclose

利用传统蜜罐检测攻击

- 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

伪装欺骗技术

Deception technologies are defined by the use of deceits 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 combing 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

RSA Conference | Where the world talks security

TRAPX SECURITY

illusive

基于伪装欺骗技术的蜜罐

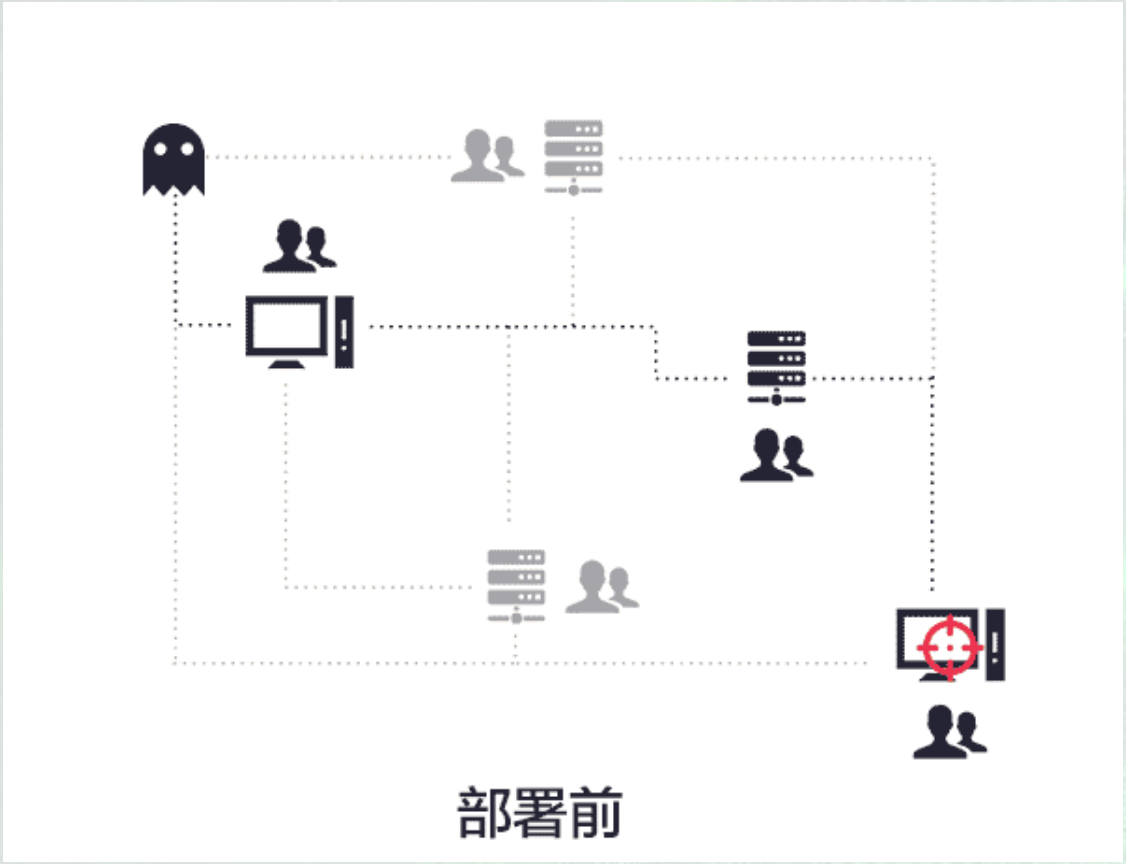
蜜罐的改进

- 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



不仅仅如此……

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

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

- 根据部署环境，适配业务场景

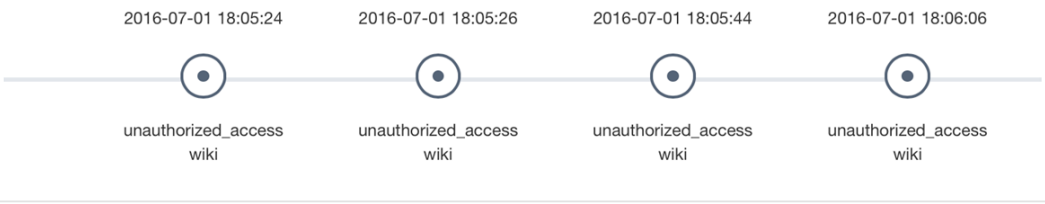
事件关联能力

- 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

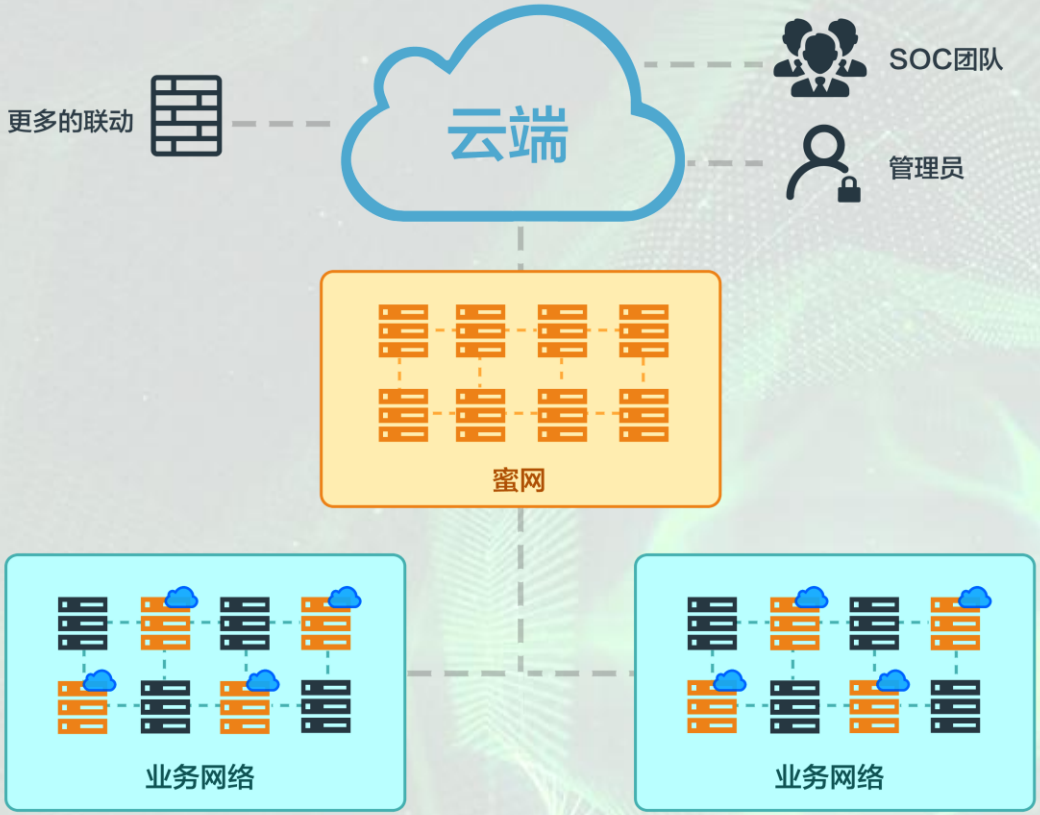
攻击时间线



incidents Timeline

2016-07-01 18:05:24	●	wiki	unauthorized_access	{"method":"GET","cookie":"","useragen...
2016-07-01 18:05:26	●	wiki	unauthorized_access	{"method":"GET","cookie":"","useragen...
2016-07-01 18:05:44	●	wiki	unauthorized_access	{"method":"GET","cookie":"","useragen...
2016-07-01 18:06:06	●	wiki	unauthorized_access	{"method":"POST","cookie":"","userage...
2016-07-03 13:33:32	●	ftp	connect	
2016-07-03 13:33:36	●	ftp	command_execution	{"command":"USER anonymous"}
2016-07-03 13:33:38	●	ftp	login	{"success":true,"password":"sain","use...
2016-07-03 13:33:38	●	ftp	command_execution	{"command":"PASS sain"}
2016-07-03 13:33:38	●	ftp	command_execution	{"command":"SYST "}

应用场景



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