聚·变

第二届顺丰信息安全峰会分论坛

大数据及AI安全

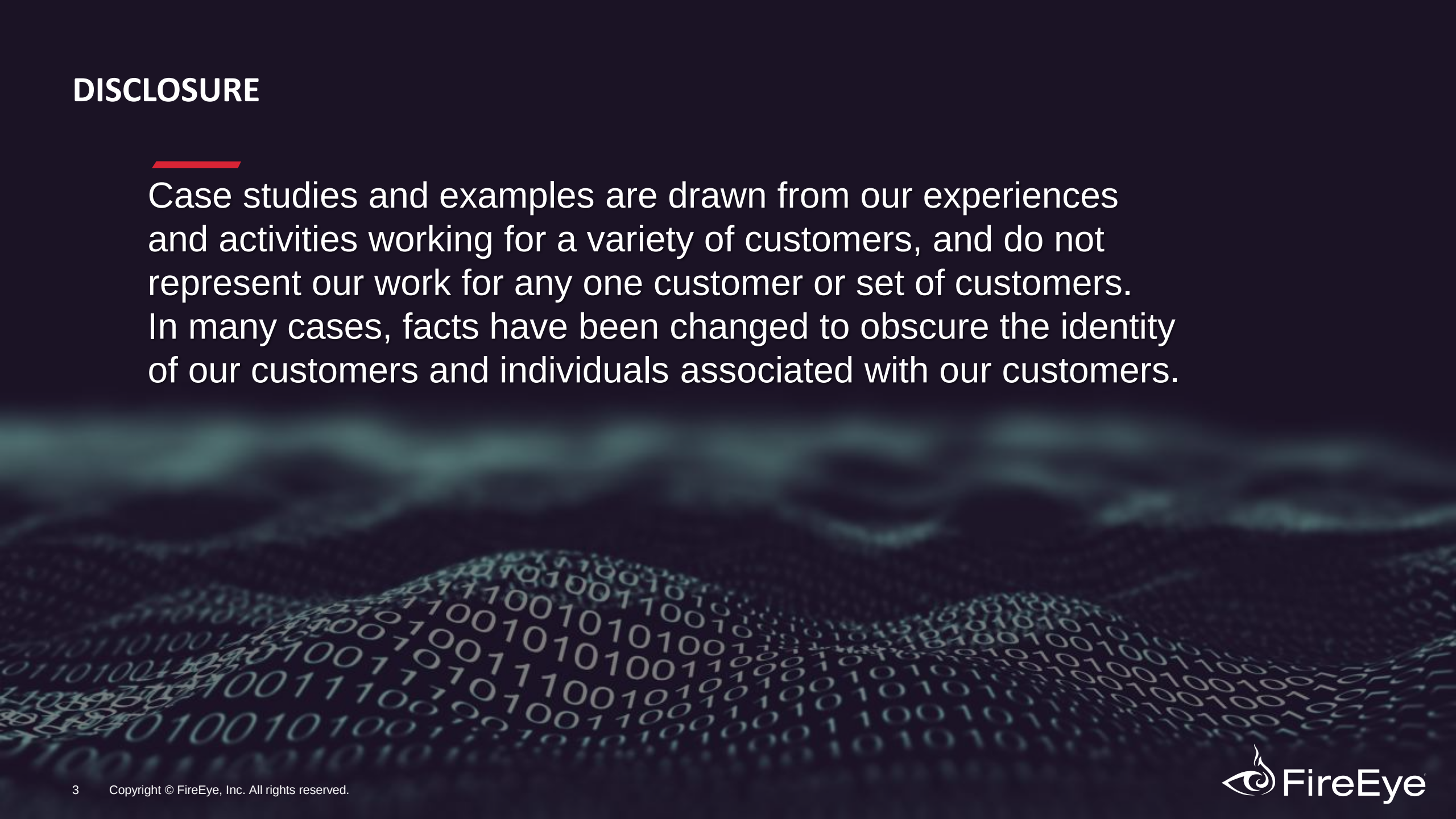
FireEye

AI 安全未来人机关系展望: 对抗或者共生

萧松瀛 Nicholas Hsiao
FireEye 首席技术顾问

DISCLOSURE

Case studies and examples are drawn from our experiences and activities working for a variety of customers, and do not represent our work for any one customer or set of customers. In many cases, facts have been changed to obscure the identity of our customers and individuals associated with our customers.



FireEye

FireEye - 全球排名第一阻截进阶网路攻击的领先者 (APT)

成立於

2004

年收入

$700M+

60多个国家

6,300

个客户

福布斯全球2000强中有

40%+

是FireEye的客户

700

前线网络安全专家

16M

全球部署传感器

50,000

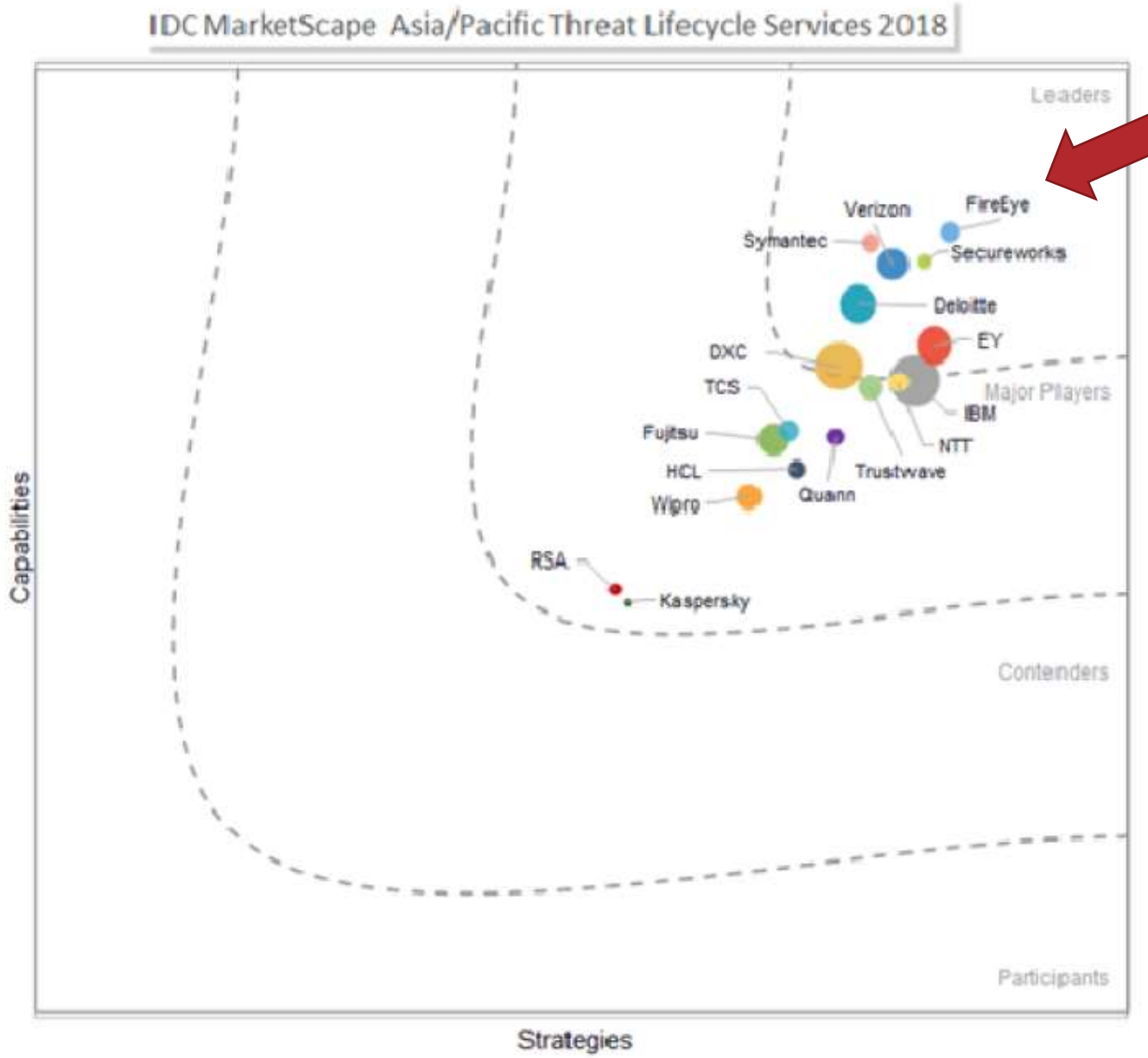
每个月发布的指标

10M

威胁源頭追踪

IDC MarketScape: Asia/Pacific **Threat Lifecycle Services 2018** Vendor Assessment

- According to customer feedback included in the report, FireEye provides **threat intelligence** competitors don't offer.
- IDC noted that FireEye's global network of intelligence specialists collect and **analyze adversarial intelligence and machine intelligence** based on FireEye detection technology deployed in client environments.
- One important differentiation highlighted in the report is FireEye's more **complete visibility into attackers and threat evidence** across the organization captured by FireEye technology and analysts.



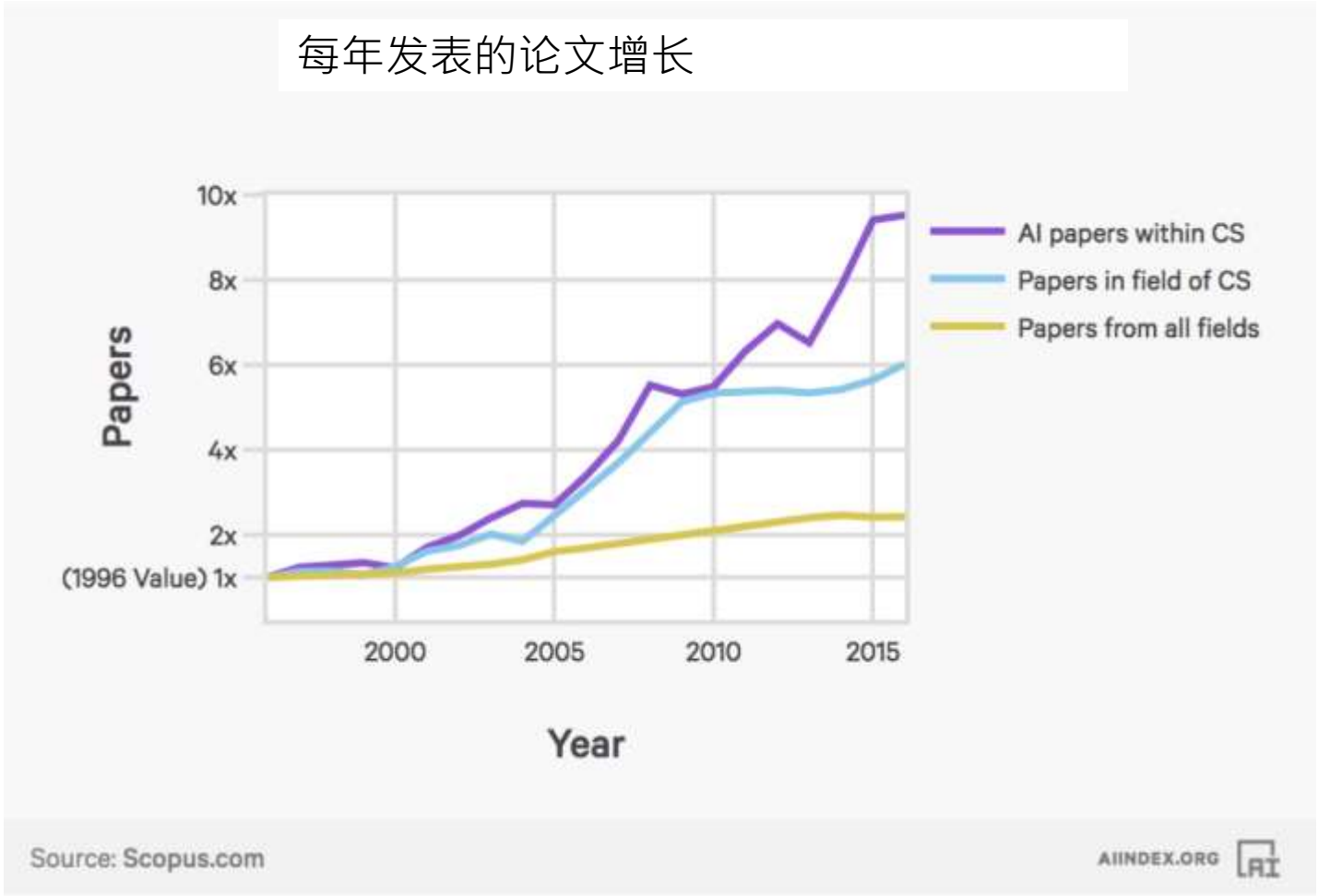
Source: IDC 2018

目录

1. 网络主题中的人工智能
2. 将AI应用于网络域
3. 网络中的AI和ML：当前的能力

1. 网络主题中的人工智能

- 技术民主化
- 标准和风险缓解
- 学术界与工业界的差距



2. 将AI应用于网络域

- 机器学习 (Machine Learning – ML) 的好处：分类，聚类，异常检测
- 人类更好的地方
- 访问数据和使用的数据类型
  - 主办
  - 网络
  - 行为

3. 网络中的AI和ML：当前的能力

APT 34

网络中的AI和ML：当前的能力

- 鱼叉钓鱼
- 恶意软件 (POWRUNER)
- DGA (BONDUPDATER)

网络钓鱼电子邮件的剖析

1. 电子邮件地址不是来自St.Thomas，与发件人的姓名不符

From: "IT DESK" <dhernandeza@uc.cl>
Date: Wed, Mar 9, 2016 at 7:59 AM -0800
Subject: Final Warning
To: "info@maiil.com" <info@maiil.com>

2. 紧急或威胁的语气

3.错字，拼写错误和不正确的语法

Dear user
We inform you that Your e-mail account was login by Unknown IP address: 116.204.148.216, kindly click on the Administrator link below and login to validate and verify your e-mail account or your e-mail will be temporary block we are still waiting for you to verify your accout before it get block.
http://stthomasitdesks.weebly.com
Thank you for your cooperation.
Copyright ©2016 T All rights reserved.

4. St.Thomas从不要求您通过电子邮件提供您的用户名或个人信息

5.虚假的网址设计看起来像是与圣托马斯相关，而是引导到其他地方

恶意软件攻击检测

网络中的AI和ML：当前的能力

- 特征码的方法无法跟上新的恶意软件生成
- 最新进展：
  - 使用内存访问模式检测
  - 使用Word2vec分析恶意软件代码
  - RNN，CNN
- 问题
  - 内容可以被加密并且基本上随机地到神经网络
  - 由于函数调用和跳转命令，函数之间的复杂空间相关性
  - 倾斜的数据可能导致偏差模型

算法生成的域名和恶意域名

网络中的AI和ML：当前的能力

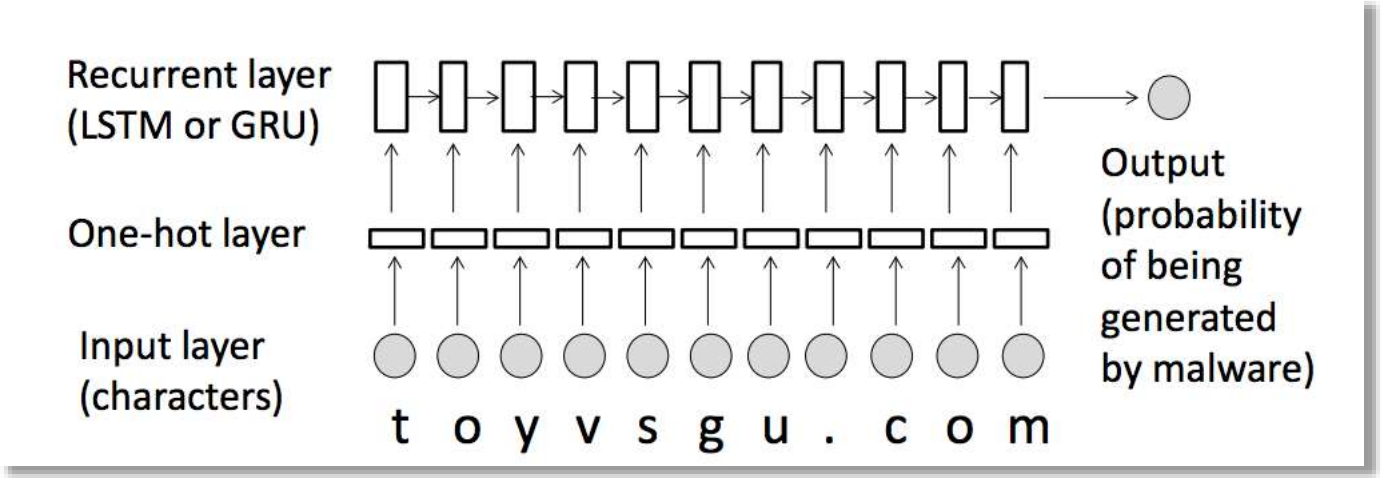
恶意软件通过算法生成大量域名

尝试连接到这些域的一部分

哪个选择是算法生成的域名？	
选择1	*Hyehgnr*
选择1	Reykjavik
选择1	lqnueumtiy
选择1	msnbc

恶意域名功能

网络中的AI和ML：当前的能力



- 词汇结构（字符分布和n-gram）
- 基于IP的功能
- 网络流量模式/ netflow
- 失败的DNS查询数
- 深度神经网络

密码破解

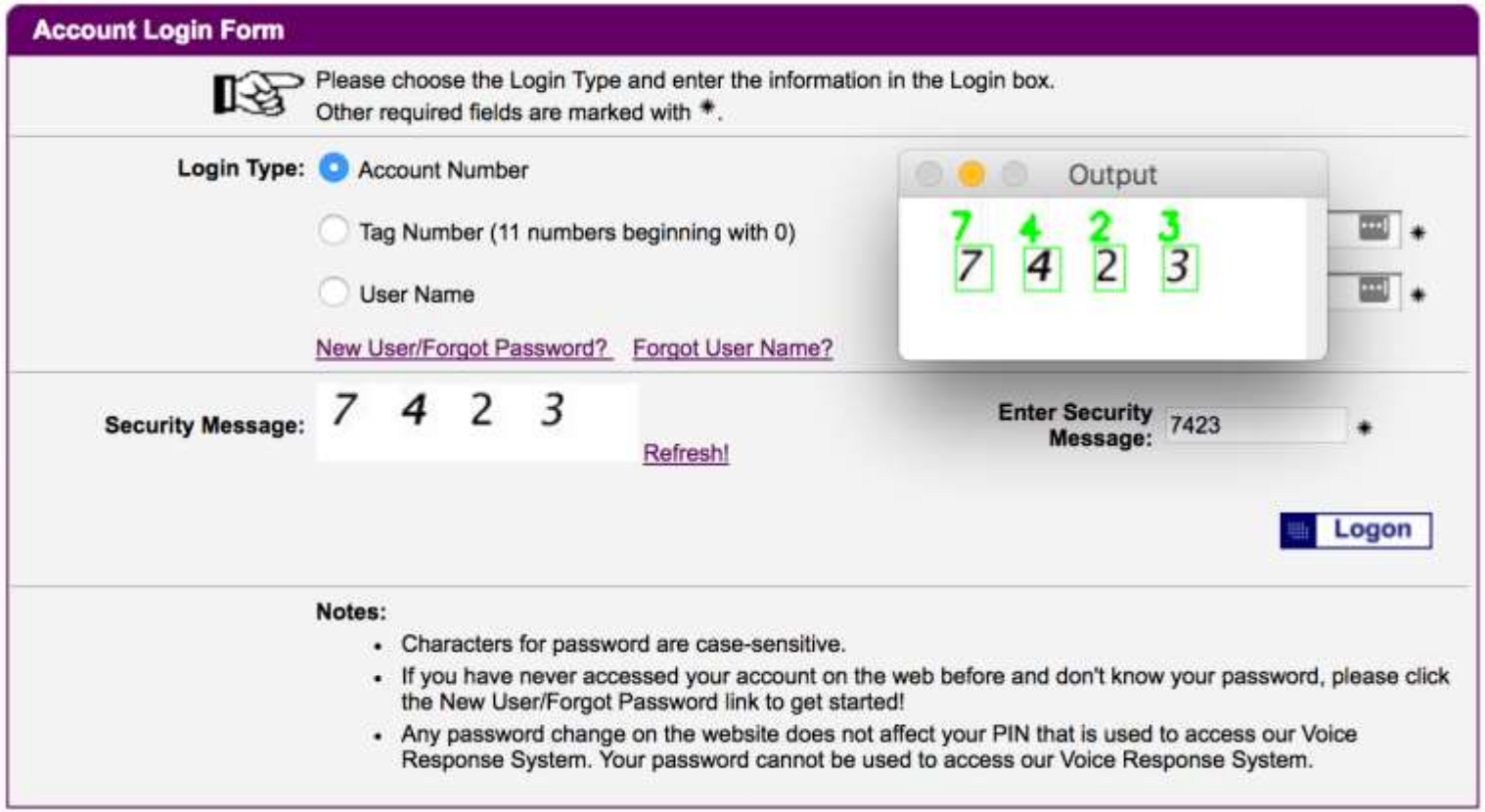
网络中的AI和ML：当前的能力

- AI如何帮助破解密码
- 对威胁的影响
- 未来的意义

解决验证码

网络中的AI和ML：当前的能力

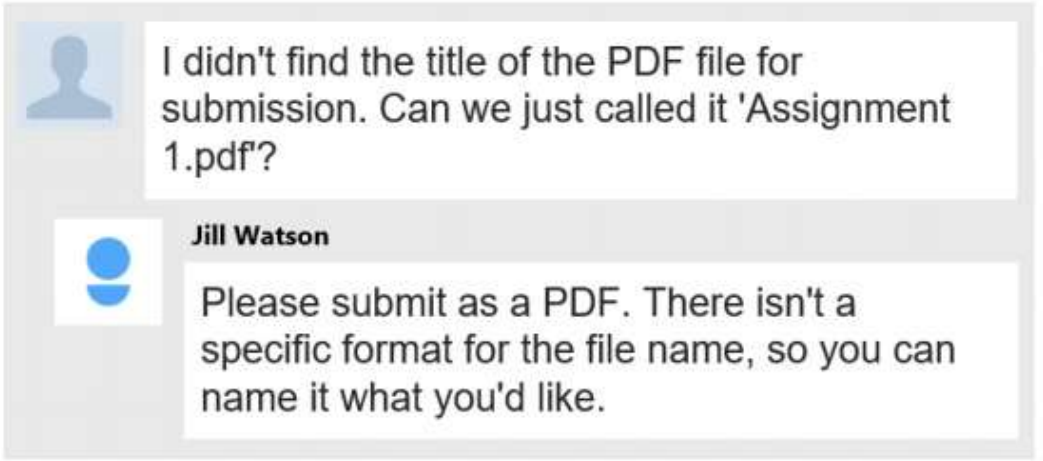
- 验证码
- AI如何帮助击败它
- 对未来威胁形势的影响

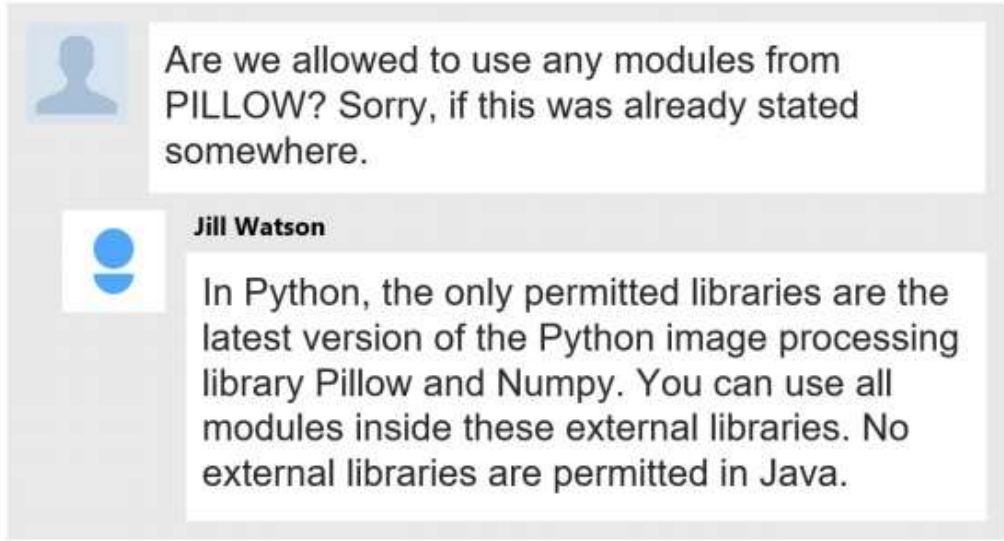


社会工程攻击

网络中的AI和ML：当前的能力

- AI帮助机器人听起来更人性化
- 改善诱惑内容
- 导致更有效的社会工程攻击

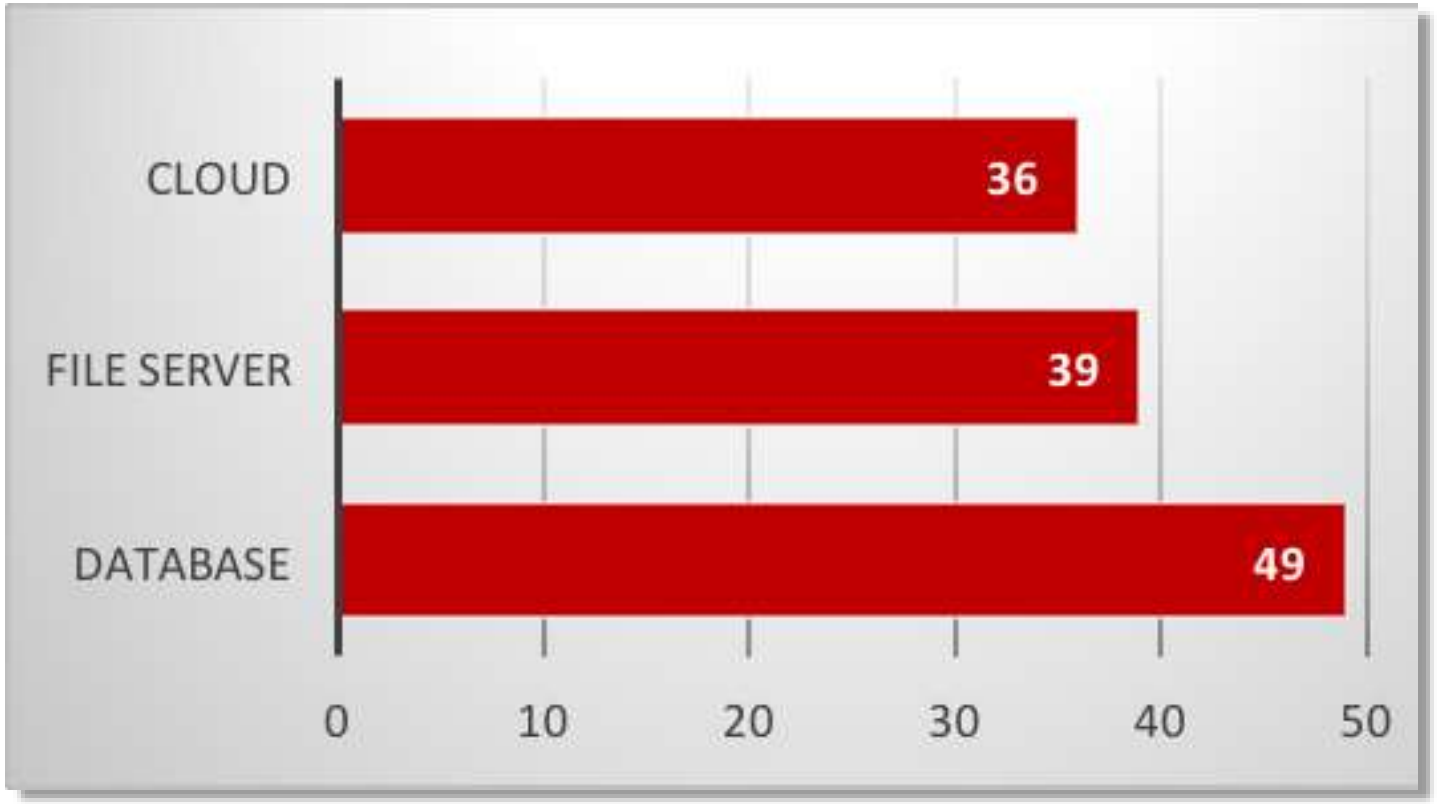


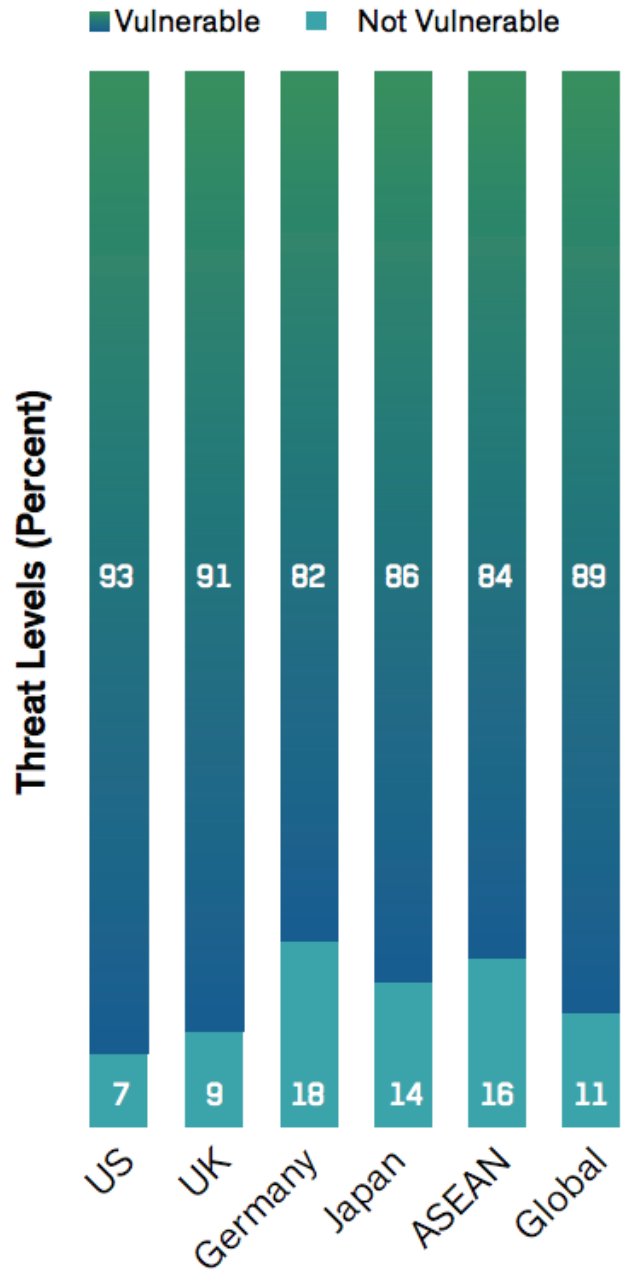


内部威胁检测

网络中的AI和ML：当前的能力

数据存在风险的前3个位置





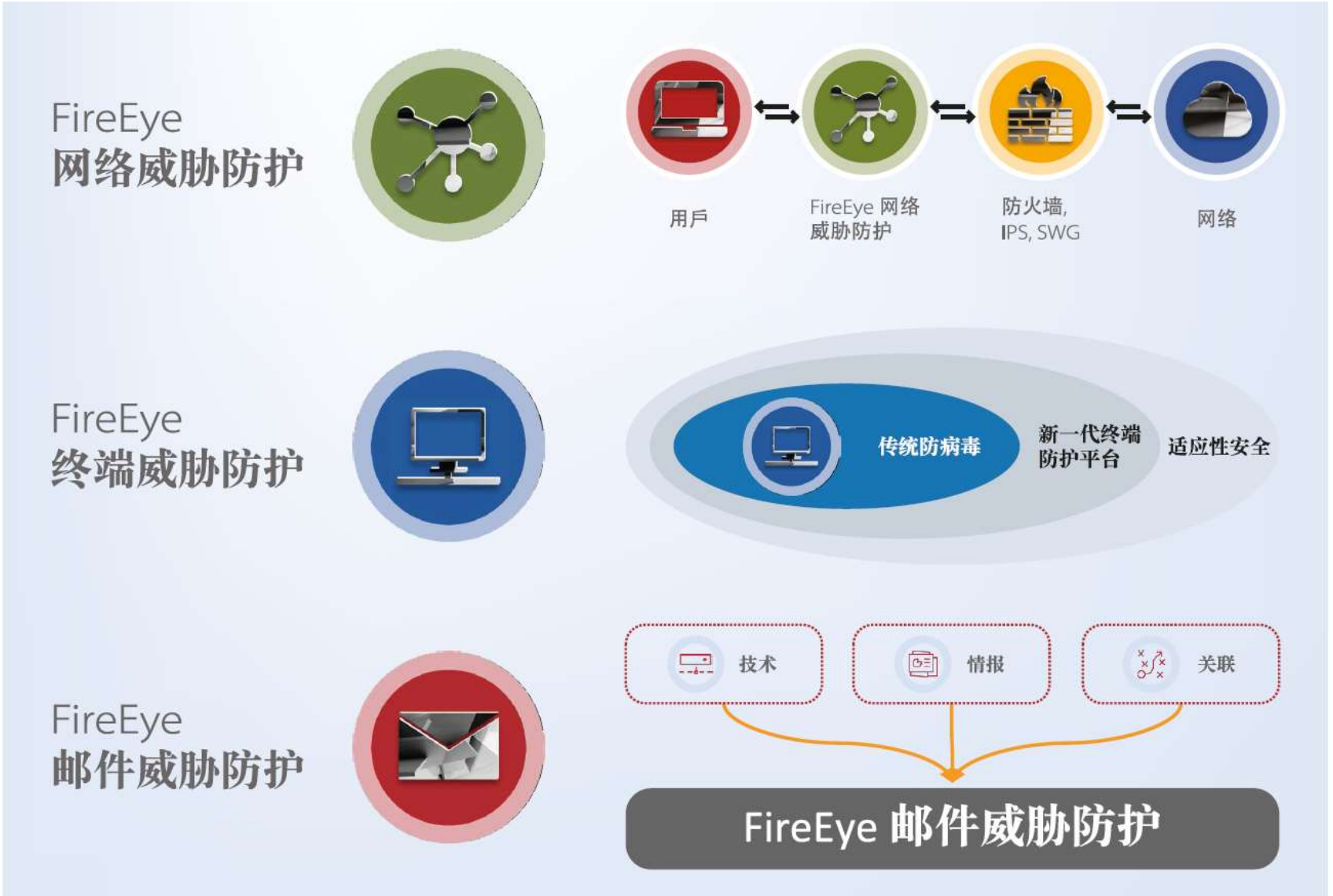
内部威胁检测

网络中的AI和ML：当前的能力

- 活动类型
  - 登录
  - USB插入
  - 电子邮件
  - 文件访问
  - 网页浏览
- 如果活动率不同
- 如果是新类型的活动
- 如果用户被授权执行此活动

- 问题
  - 误报太多了
  - 需要上下文
  - 相关人员的人必须评估情况

FireEye 生态系统



THANK YOU