ISC 2019 7th
第七届互联网安全大会

大型企业威胁情报运营与思考

美团点评信息安全中心 —— 李中文（e1knot）

ISC 2019 7th
第七届互联网安全大会

Agenda

- 大规模复杂系统下的威胁
- 如何构建威胁情报能力
- 如何评价威胁情报能力建设的好坏
- 威胁情报生命周期与威胁情报体系建设
- 威胁情报的闭环与运营

第七届互联网安全大会

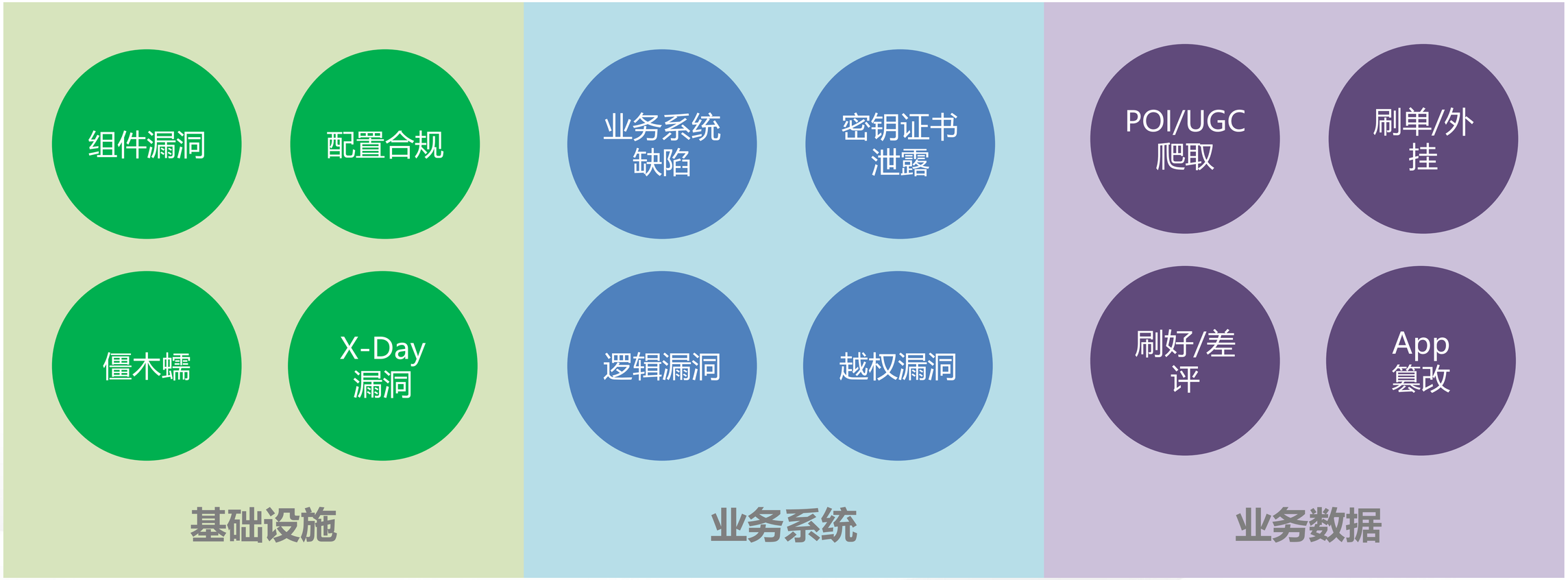
Intro

- Id: e1knot
- 美团点评集团（3690.HK）信息安全中心基础设施安全团队
- 负责集团内威胁情报与态势感知的能力建设
- 多年安全数据与威胁情报分析和运营经验
- ISC2017、DEFCON China等会议的Speaker

大规模复杂系统下的威胁

- 业务数据多：核心系统日均PV超过数十亿级
- 业务规模大：数百个复杂业务应用系统，代码总数超过亿行
- 资产列表长：数百万级别的IDC资产、软件资产和终端资产
- 资产类型杂：数十万种不同种类和版本的中间件和开源组件
- 告警数量多：N多种设备可以产生告警，日均产生数以万计的告警
- 企业威胁现状：每年安全上砸了那么多钱可还是因为安全问题损失惨重

大规模复杂系统下的威胁



如何构建威胁情报的能力

- 只买买买真的能解决问题么?
- 如何评价威胁情报对信息安全产生了作用?
- 威胁情报团队的绩效怎么给?

威胁情报数据的运营之殇

威胁情报很重要
虚假情报一大票

假情报泛滥

应急全靠朋友圈
口口相传得情报

消息不对称

情报数据千万兆
能运营的就几条

无效情报多

消息滞后很痛苦
业务损失不知道

消息滞后影响

威胁情报能力的灵魂N问

- 买买买了很多威胁情报数据和服务 —— 这些服务和数据是否用起来?
- 威胁情报数据和服务已经和资产对接 —— 威胁情报的质量如何?
- 威胁情报有效情报数量占比高于30% —— 是否能产生有效的情报通知?
- 威胁情报平台可以推送有效的情报 —— 是否有人跟进这些情报?
- 有对应的安全运营同学处理了威胁情报 —— 是否跟进闭环?
- 所有的情报已经闭环处理完毕 —— Where is Cases Study & TODOs?

如何构建威胁情报的能力

威胁情报到底对企业的安全有什么作用?

威胁 -> 威胁情报 -> 威胁情报能力

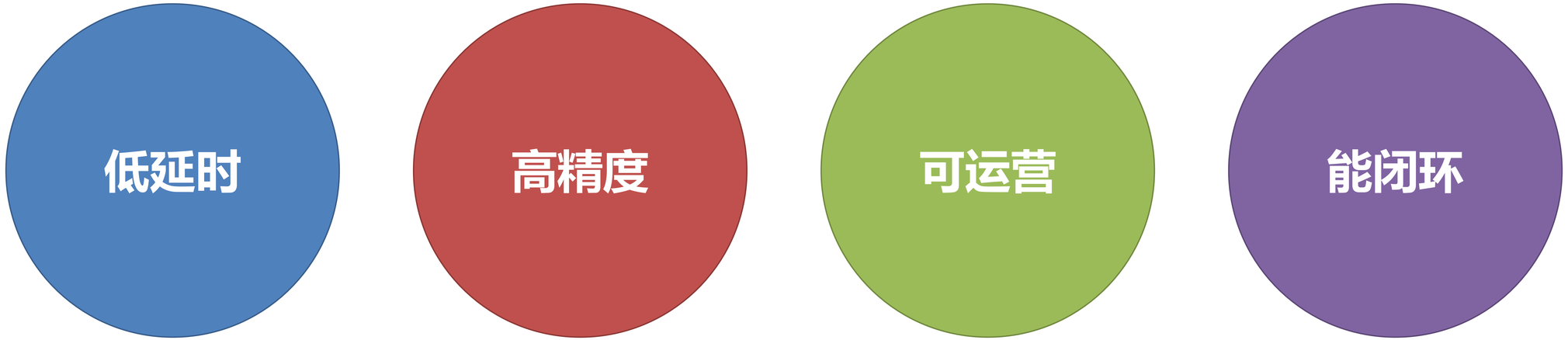
威胁情报是一种基于证据的知识，包括了情境、机制、指标、隐含和实际可行的建议。威胁情报描述了现存的、或者是即将出现针对资产的威胁或危险，并可以用于通知主体针对相关威胁或危险采取某种响应。

—— Gartner（2013）

能够为发现潜在或已发生的威胁（包括但不限于业务数据、业务系统和基础设施）提供有效且可靠的消息类型或者知识类型的数据，且该数据能够通过安全运营进行高自动化的闭环处理能力称之为威胁情报能力，提供的数据称之为威胁情报。

—— 鲁迅（一个带着远大理想的小目标）

如何评价威胁情报能力建设的好坏



- 尽可能快的同步安全团队内部，减少等待
- 情报运营自动化率与有效情报转化化率

- 稳定可靠的情报渠道、数据质量和数据来源
- 不断迭代的高精度和稳定可靠的算法

- FINTEL质量是否足够可读可用可闭环
- 提供保障运营可用的快捷操作指引

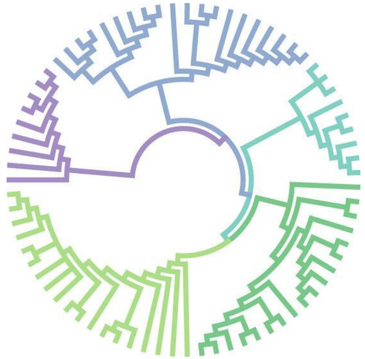
- 事前选择正确的情报闭环方式与方法
- 事后复盘和改进
- 情报算法迭代优化

注：FINTEL = Final Intelligence，代表情报部门所交付给使用方的情报成品，可不拘泥于形式

如何评价威胁情报能力建设的好坏

威胁情报组件与运营体系

威胁情报数据
(Data Grids)



情报生产工具
(Production)

情报管理平台
(Platforms)

安全运营团队
(Operators)

威胁情报能力建设四重奏

- 一个体系：基于威胁情报生命周期且兼容现有安全体系的威胁情报运营体系
- 两个平台：威胁情报通知平台（MT-Radar）和威胁情报管理平台（MT-Nebula）
- 三个数据：自主构建的外部资产设备指纹库、通用漏洞数据库、外部情报数据库
- 四个渠道：人工反馈渠道、自动化采集、第三方情报服务、安全响应中心（SRC）

威胁情报运营生命周期

情报策略制定

- 确定评价指标
- 确定运营策略
- 效果持续运营
- 情报接入需求
- 情报输出规范

情报采集与分析

- 数据完整可用
- 情报分析建模
- FINTEL效果
- 修饰与调整
- 机器学习？

情报交付与运营

- 闭环处置方式
- 运营数据积累
- 关注有效情报
- 交互标准化
- 安全设备联动

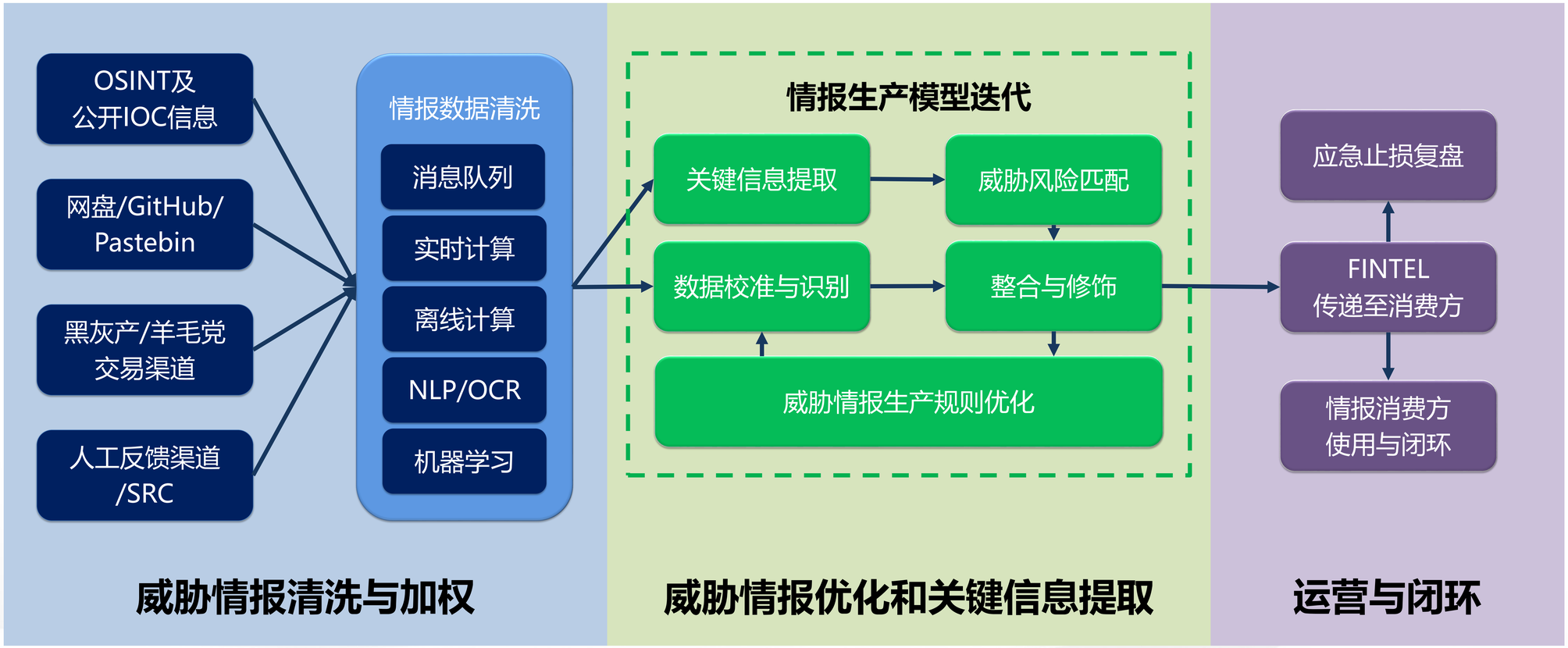
Cases Study & TODOs

- 完善情报质量
- 找到问题根源
- 解决问题
- 安全专项
- 改进安全规划

威胁情报能力体系矩阵

注：TIMC = Threat Intelligence Management Center，负责管理所有的威胁情报并且跟进闭环

威胁情报数据采集与分析



威胁情报数据采集与分析

Openwall
bringing security into open environments

Products | Services | Publications

Follow us on Twitter

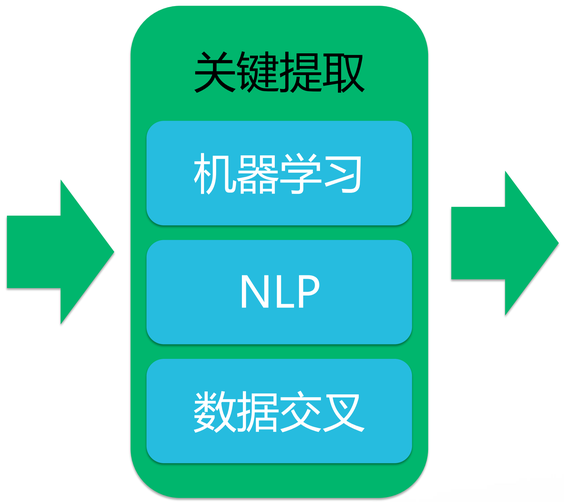
[<prev] [next>] [day] [month] [year] [list]

```
Date: Tue, 28 May 2019 14:25:13 +1000
From: Aleksa Sarai <cyphar@...har.com>
To: oss-security@...ts.openwall.com
Subject: CVE-2018-15664: docker (all versions) is vulnerable to a
 symlink-race attack
```

A vulnerability in all versions of Docker can be potentially exploited by miscreants to escape containers' security protections, and read and write data on host machines, possibly leading to code execution.

This is according to senior SUSE software engineer Aleksa Sarai, who said the flaw is a race condition bug in which a file path is changed after it has been checked as valid, and, crucially, before it is used.

The flaw, designated CVE-2018-15664, can be, in certain circumstances, abused to read and write arbitrary files on the host with root permissions from within a container, Sarai explained on Tuesday. This is possible provided there are no file system restrictions on the Docker daemon, such as those imposed by AppArmor.



```
{
    "product": [
        "Docker", "SUSE",
        "Docder daemon", "APPArmor"
    ],
    "version": ["all version"],
    "cve_id": ["CVE-2018-15664"],
    "vul_type":[
        "escape", "code execution",
        "race condition", "arbitrary files"
    ],
    "author": ["Aleksa Sarai", "Sarai"],
    "time": ["Tuesday"]
}
```

威胁情报数据采集与分析

CVE-ID	
CVE-2018-15664	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
In Docker through 18.06.1-ce-rc2, the API endpoints behind the 'docker cp' command are vulnerable to a symlink-exchange attack with Directory Traversal, giving attackers arbitrary read-write access to the host filesystem with root privileges, because daemon/archive.go does not do archive operations on a frozen filesystem (or from within a chroot).	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	

CVSS v3 metrics

CVSS3 Base Score	7.5
CVSS3 Base Metrics	CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H

```
<cpe-item name="cpe:/a:docker:docker:0.1.0">
  <title xml:lang="en-US">Docker 0.1.0</title>
  <references>
    <reference href="https://docs.docker.com/release-notes/docker-engine/">Version</
    reference>
    <reference href="https://www.docker.com/">Vendor</reference>
  </references>
  <cpe-23:cpe23-item name="cpe:2.3:a:docker:docker:0.1.0:*:*:*:*:*:*:*"/>
</cpe-item>
```

数据清洗

影响范围

漏洞危害

风险评级


```
{
    "timestamp": "2019-05-23T10:29:07.453000",
    "cvss_score": "6.2",
    "cvss_detail": "CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H",
    "cve_id": "CVE-2018-15664",
    "last_modified": "2019-06-25T08:15:10.187000",
    "references": [
        "http://lists.opensuse.org/opensuse-security-announce/2019-06/msg00066.html",
        "http://www.openwall.com/lists/oss-security/2019/05/28/1",
        "http://www.securityfocus.com/bid/108507",
        "https://access.redhat.com/security/cve/cve-2018-15664",
        "https://bugzilla.suse.com/show_bug.cgi?id=1096726",
        "https://github.com/moby/moby/pull/39252"
    ],
    "summary": "In Docker through 18.06.1-ce-rc2, the API endpoints behind the 'docker cp'
    command are vulnerable to a symlink-exchange attack with Directory Traversal, giving
    attackers arbitrary read-write access to the host filesystem with root privileges, because
    daemon/archive.go does not do archive operations on a frozen filesystem (or from within a
    chroot).",
    "vuls": ["17.x","18.x"],
    "type": ["RCE"]
}
```

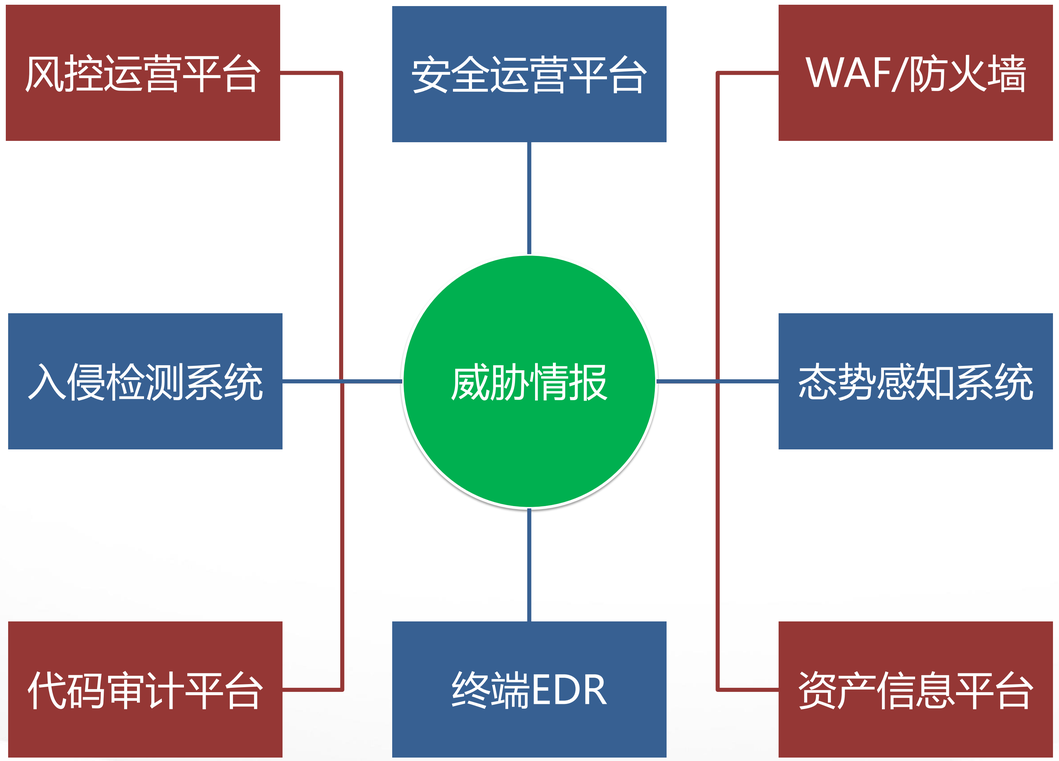
威胁情报数据采集与分析

- 基于互联网设备指纹、OSINT、监控安全信息交换渠道和交付规范构建可运营的威胁情报数据库
- 通过优化和改进采集规则、关键字匹配规则和情报生产规则，使用 OCR、NLP 等技术识别与分析捕获到的威胁情报中的关键信息，提升情报的精准度和可阅读性
- 通过人工/自动化修饰为 FINTEL 可阅读性和可运营性
- 选择正确的渠道传递 FINTEL 至需求方，通过工单完成催促和运营闭环
- FINTEL 一定要经历第三方验收，保证 FINTEL 的可用性和准确性

威胁情报数据运营与通知

- FINTEL交付的目标：
  - 保证情报内容可在短时间之内读懂
  - 所有评估所需要素一应俱全
  - 提供闭环所需解决方案
  - 影响范围一目了然
  - 方便后续运营闭环操作

威胁情报数据运营与通知



Coda

- 从获取威胁情报到完全闭环一个告警是一个极其困难且有很大挑战的过程
- 一直买买买实际上不能解决“未运营的威胁情报不会产生任何使用价值”的问题
- 情报能力对于企业安全的价值：减少信息不对称带来的损失、赋能于安全提高威胁发现率
- 威胁情报是规划导向的产物：坑在规划，重在生产，难在运营，结果取决于闭环的结果
- 评价威胁情报能力好不好的四大标准：速度快、情报准、可运营、能闭环
- 威胁情报体系建设四重奏：情报体系、自动化平台、数据资源、获取渠道
- FINTEL的好坏直接决定运营难度，好的FINTEL需具备易读懂、可操作、能运营

第七届互联网安全大会

THANK YOU

2019.8.20