





# 场景, 网络安全实践教育的基础

李炜。永信至城副总裁

ISC 互联网安全大会 中国・北京

Internet Security Conference 2018 Beijing · China

(原"中国互联网安全大会")

# 从女儿的英语课外班说起 - 场景式教育方法





#### 孩子的英语认知不是从ABCD开始,识字、造句从SIGHT WORDS起步

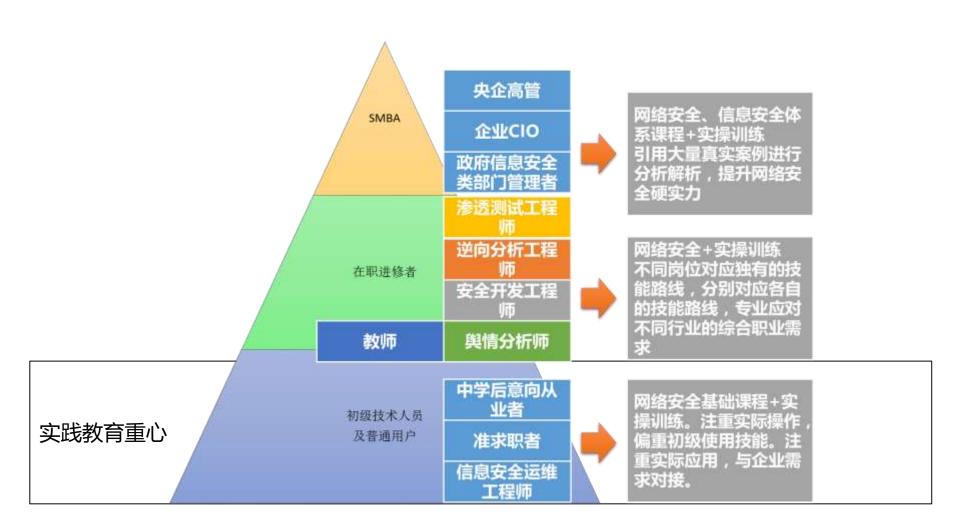




#### 实践教育的目标是培养什么样的人才?





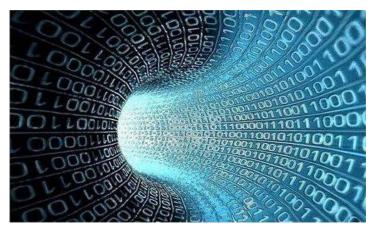


"安全人口"基数是解决企业人才问题的重中之重,实践教育是扩大"人口基数"的核心

### 网络安全的特点是什么?









更新快 偏应用 工程化 要动手





每一个网络安全问题都是一个独特场景,每一个安全产品都是解决特定场景中的问题

#### 网络安全教育面临哪些挑战?





# 应用

•不仅仅是在校园中。网络安全教育全社会必须 共同面临的问题就是如何跟上最新的形势,更 新知识结构

- •新技术不断涌现
- •新威胁不断发现
- •太多未知因素
- •如何结合应用?

- •任何技术和知识都是 在特定场景中得到应用
- •如何避免"新技术"研究的"政治正确"?
- •扁平化的沉淀,如何 "立体化"起来?从沙 子还原成<u>"塔"</u>

沉淀

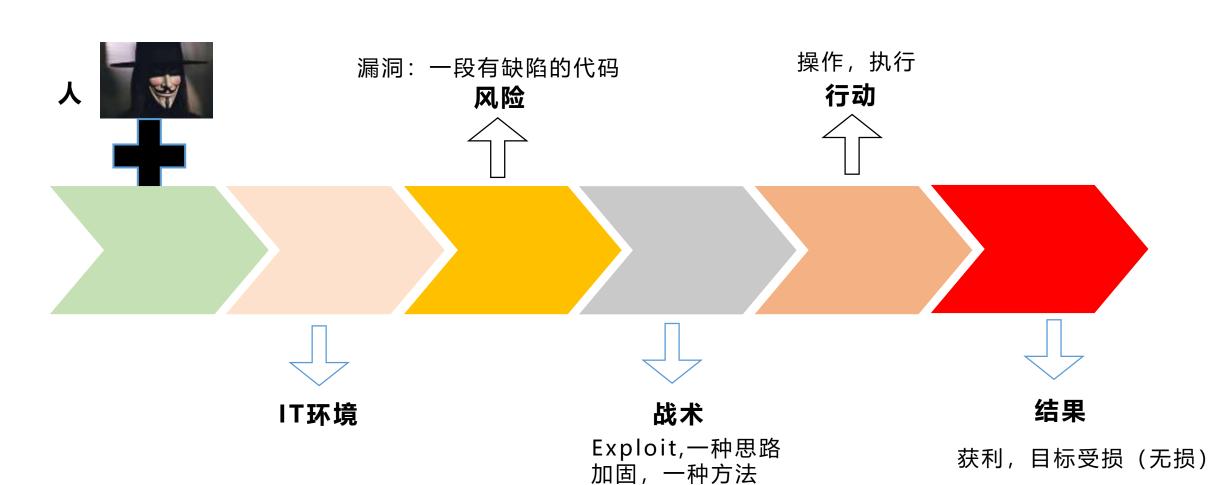
# 更新

### 场景 - 是提升实践应用能力的基础





#### 6个元素



## 科研、教学的"简单"场景 - 实验





#### 网络安全的本质在对抗,对抗的本质在攻防两端能力较量。

实验,实训

- - 习近平



#### 教学中的"对抗"的场景, 竞赛







然而,竞赛的目标还是让人员更好在实际场景中应用技术水平,脱离了场景的对抗,没有价值

### 竞赛支撑实践教学 - 从怎么做到怎么用再到在哪用





#### 2014年至今, 支撑国内省部级以上各类比赛超400场



### 设定底线场景 - 红线意识





















#### Web安全工程师

想成为Web安全工程师?不知道该如何入门?不要着急,本计划分五个阶段,包含最基本的Web漏洞检测、理论基础、原理分析及安全防护,帮助你成为优秀的Web安全工程师!

189 节课程 47 小时 1343144 已学

概	念基础	技术基础	入侵防范	Web安全漏洞分	渗透实战	安全开发
	0	0	(0)		. 0	(6)

			○ 日学完 ○ 学习中 ○ 未学习		
Miss Att No. 40 T. Prints 7					
1 DOPPOSE DENOMINACIONES ANNO MENTE STUDIO	0	a. museummatiemmentemisc.c.m.	0	A. 事的使用MSF技能的的方面。	0
4. 松块银用MSF附属注意制度?	0	1. GERTHELE-BATE	0	※、ACHTPROMERTINGSTEEPINGST	0
/ MUSICIPOLYCETT . DECEMBER !	0				
characteristic and control over					
L. BURN PANCETE SYANDSKINGSKICKERSE	0	at make processors were	0	A. KINK PADPERLIZAVENIANOS	(0
L AWVS ( 050)	0	2. AWVS 1 SEGR	0	II. AWVS : MARKER	0
4. AWVS - Felling #59WF		S. AWVS : Site Crawler® HTTP Editor	0	6. ASVV5 : Target Finder & Subdorrei	0
7. AWVS - Authentication Tester	0	8. AWVS   HTTP Shifter	0	9. AWVS / HTTP Fuzzer	0
Robbie Swit I II : Nimop					
to the total or seems	0	2. F389F1-R48	0	A E-HAPDINGH-HIPPH NAZIONI FT NE	0
4. ESEMPTION/POSMANICS	0	S. EDPSTEISSELL-DWINER AN NO.S	0	6. OUTSTONESSEE CHARGES IN THE SECTION	0
r symptemice	0	B. MACHERINANI	0	O. HARDINGHI	0
O. WINNINGS Park!	0	11 Printing Parts	0	12, X086/A:480/(H-20)	0
3. hpmsmcuscom	0	14. aperementalism	0	15. Nmapirilli + TIM	0
to. Zenmapphythttthi		17. IDENSIGNATIONAL PROPERTY IN THE PROPERTY I		18. NOW HOMES 1	10



#### WEB安全工程师 安卓安全工程师



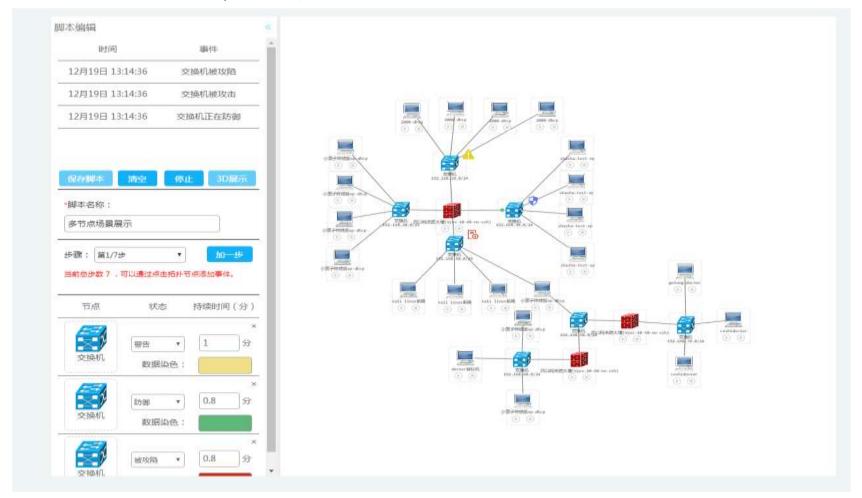
ZERO TRU

## "简单"场景积累聚合,形成"复杂"场景的基石





# **靶场**是承载和生成场景的基础条件



## 让错发生在靶场——提升教学效能,锤炼综合能力



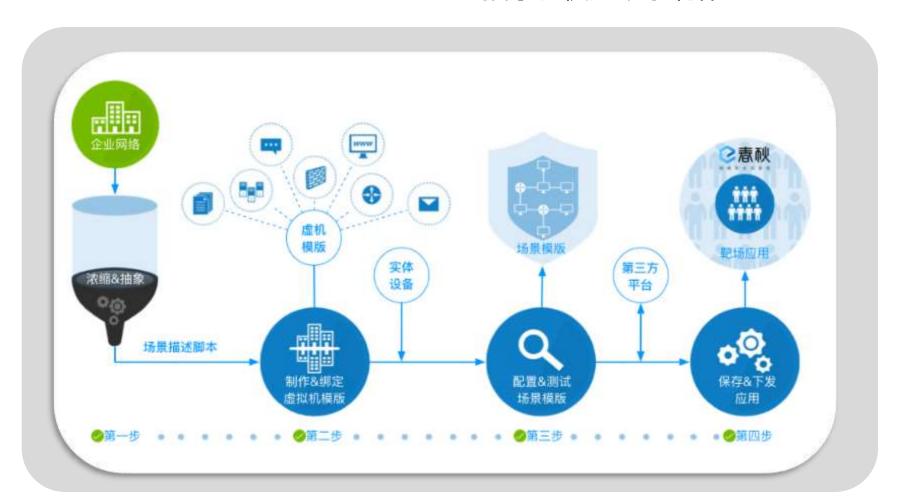








#### 抽象、快速场景制作

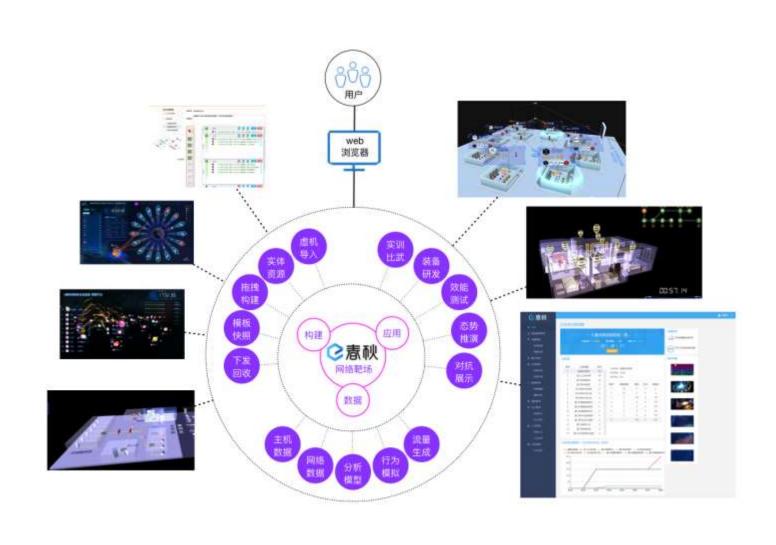


- red/blue team
- ❷ 操作系统
- ❷ 应用&服务
- ❷ 漏洞
- ❷ 工具
- ❷ 网络
- ❷ 数据监控
- ❷ 统计&展示
- 0 0 0 0 0 0





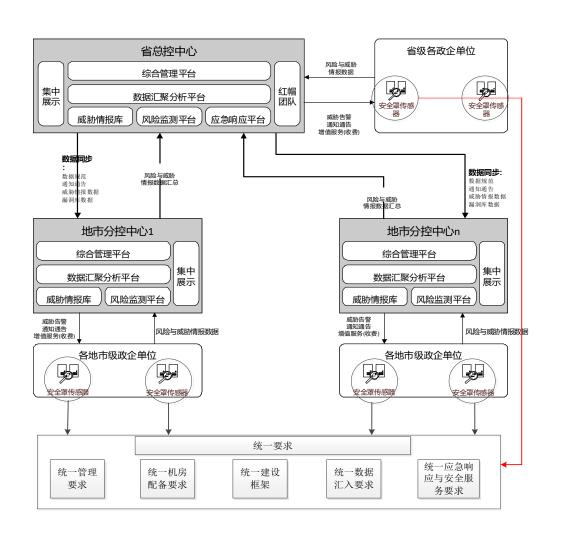




#### 社会治理场景 - "高处置" 态势感知







#### 架构设计:

- 三级架构: 省总控中心、市级分控中心、政企用户三级 架构, 省级监管部门统一指挥全局, 地市监管部门分管 各地。
- 数据统一汇聚:各总控、分控中心收集下辖各地政企单位探针引擎数据及其他数据汇聚源。各分控中心按照省级监管要求和数据标准将数据汇总至省总控中心。

#### 部署规划:

- 统一要求:管理要求、机房配套要求、建设框架、数据 汇入要求,应急响应和安全服务要求;
- ・赋权地方: 赋予地市监管部门统一调度、协调、汇聚各 地政企用户、安全企业,服务团队的权利。

以各地监管部门和配套团队为支点,撑起全国范围内第一个覆盖全行业的,政府监管部门主导的安全罩体系。

ZERO TRUST SECURITY

# 高处置态势感知 - 落地广东全省



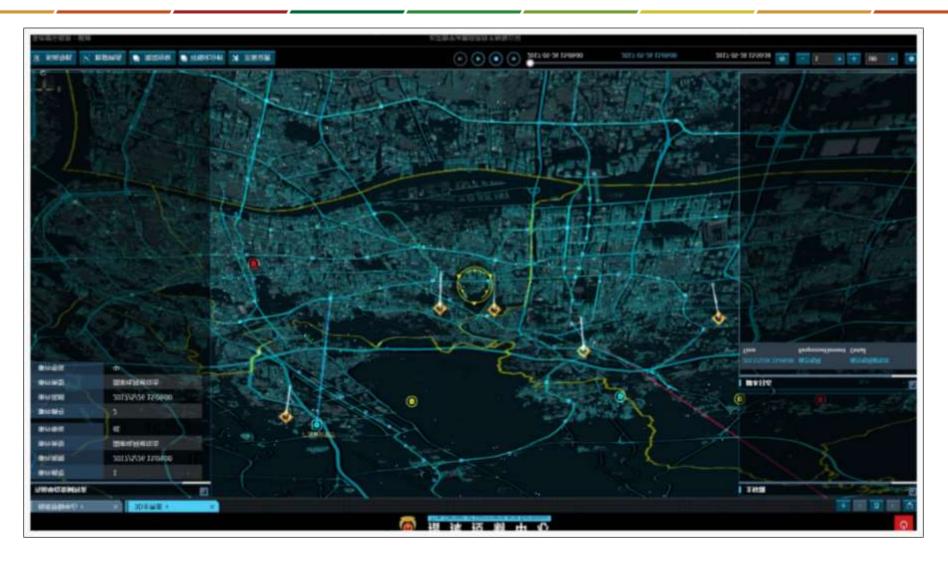




# 践行网络安全防护理念 - 安全罩







# 应急响应中心运营团队



分析

转化







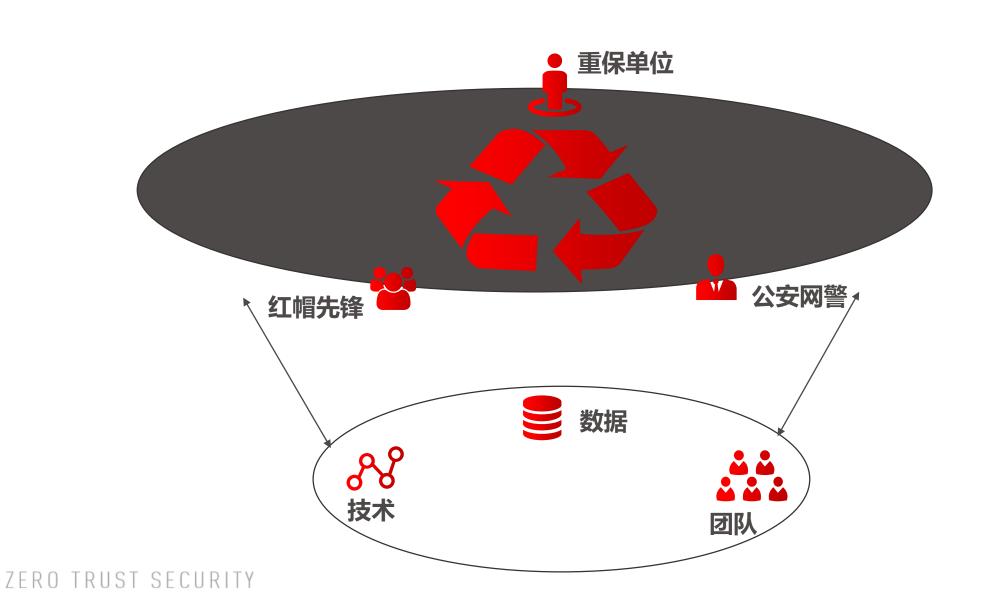


广东省安全罩项目中,应急响应中心协调省内广大院校中的红帽先锋协助 重要行业进行应急处置。

# 安全罩 - 整合社会力量, 联防联动联控



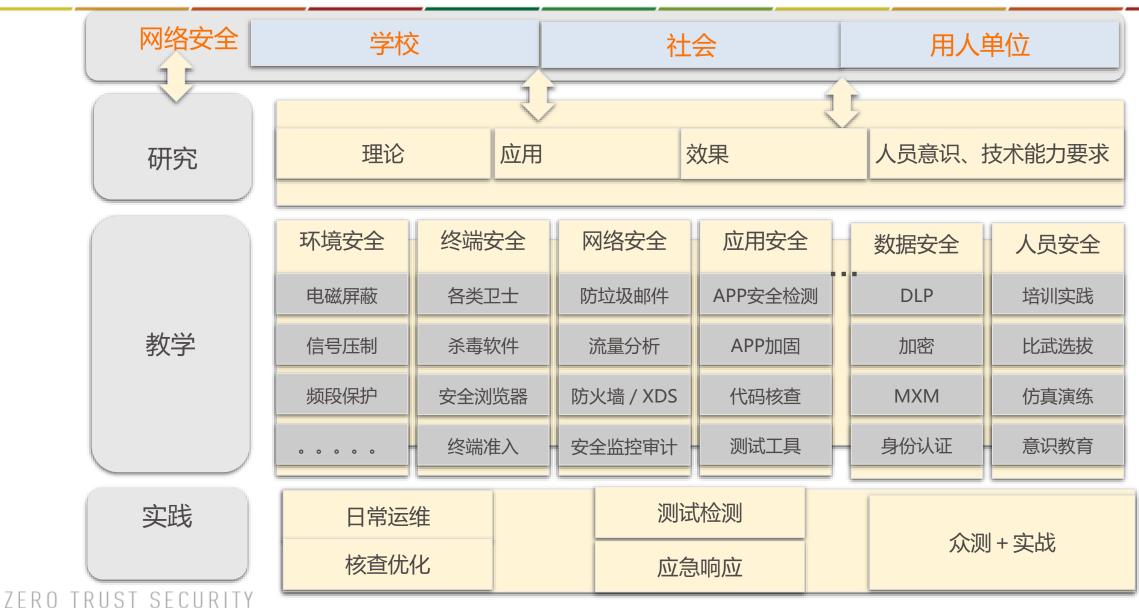




#### 场景为基础的网络安全人才培养框架







### 教育, 终将需要理论化、体系化, 我们以场景梳理体系





#### 4大实训基地

- 北京国关

#### 学习建议

作为网络空间安全的人门路材。本书为美统技术和 行业价格为证券解码网络空间安全的标识证量、同 修空司安全知识体系是广、技术更新建筑体、宝珠 **健求施、株村協立注意存安3の計算部以下開始** 

- 本书的每一面并及构在空间完全的一个信息。這 似乎与过每一年之后,而最善单的工能和要点、建 立匠科性空间安全的部分模型。 位于部分核型的信 的世界人学切取研究某一个安全领域是关键器。
- 由于是符论课程数付、因此本书每一量只给出某 · 你就要要我们就写了你。如果你对对中国个工 **日本川道、建立石田水東東川刊立四日一ナサロ**材 科提高主题相关的核材、参考市进一步学习、学等 网络上桌排填套架每一套相关的字可裹材和资源。 METTERNANTH.
- 用格里利亚士芸一个深刻的形面的字件、建设信 五学记本书时位要并初于实践。
- 此學习过程中将老师或地人通常知识完是前时的 学习方式、建议位文注网络空间变变相关的技术。 学习社区、公众号等、以获取技术和学习方法方面 SHEEK.

协会行政关节使用从约束长型标的将本书更多否等 与农场机场报。

STREET, SEE

网络空间安全导论

#### Introduction to Cyber Security

网络空间安全涉及多学科交叉、知识结构和体系宣广、应其结果基础。同时,网络空 阅安全技术更新建度快、因此、本书面向网络空间安全的初学者、力课规模网络空间安全 的技术赔偿和基本的知识体系,为读者后续的专业课学习和完造打下基础。

- 以行业提集下的网络空间安全技术体系体型用金并型构、为体素展示从技术提集业里 的网络空间安全知识体系。
- 本书以技术与管理为基础、内容从网络空间安全领域的基本知识点到实验的反用场 量。使读者了解每个网络空间空空领域的知识主线。再通过食能的案例,使该套理解 如何应用网络安全技术和知识解决实际场景下的综合性问题。最终,使读者企業掌握 网络空间安全的基本技术架构。
- 架出救治性和实践性。除了基本的网络空间安全知识、本在在对大数据、公计算、物 据尚非热点领域困难的安全问题和企业养现有的解决方案做了介绍。同时,书中引入 而多作者实际工作中的案例、网络其安全需求避免离开、特试者引入到实际运算中。 并给出货额的解决方案。使读者了解和掌握常见的安全技术和工具。
- 突出安全消費的培养。開降空間安全从业人因与其他行业人员最大的不到在于其接有。 的一意思维方式。本有在介绍知识体系积同时、他智力有网络空间安全领域分析问 题。解决问题的思维方式、方法提炼出涨、使理者享受从网络空间安全的角度里考问 题。存我解决方案。
- 本书配有丰富的数学和学习资源。债者和用书数师可量录率章网站下载。







网络空间安全学科规划教材 主编介绍

**最高額 厚纬○主編** 

**模器传 孙推搡 赵永 张光文〇参编** 

Introduction to

Cyber Security

○ 馬馬玉点魚魚盖



競議器 北京み信室 循环技术附近型创 知人, 董事任, 从 単円性至立形米工 erits, modes 百姓科亚亚亚亚之

一体、培养出许多安全专家、中国国家信息安全 MERNAGE, DERROSPECTORES 货、2006年世份任务后女保证联邦应协处量技术 研究用处理学科人团的结果, 企业安全能力的研 高灰公司安全推问的银开。然为约4条标学院已成 为因为影响力量大的农务业全部有机构、业务外科 班安定实验室已成为因内活动位立得着的支持型



學株 北京市田泉 域科技教育公司制 **公和、同株空河**全 全有物的基的证明 果實性用用服務之. **非常正规集和企业** 任。从事他把安全

行业程本工作出15年、我力于安全规则、安全 的护理会研究以及网络安全人才给养模式。 程 2、石式的原素的复数,中国网络中国安全协 分联第人才培养工作组取组标、中国 - 批划第 十九次中部前导入槽台数于经济与网络安全专家 工作的信息、新知林林、信任实现的大学和会认 **业标架**,与中国也是安全认识中心的同主导展出 CISAVILLE 'Works' 'BORS' BO 全新的职业认证、其称"中国信息业业结合管 確確" "關稅MCSEUZ专案" "Symantor 551" WIEE,

京商16首章的6米从商店部的10分全部。



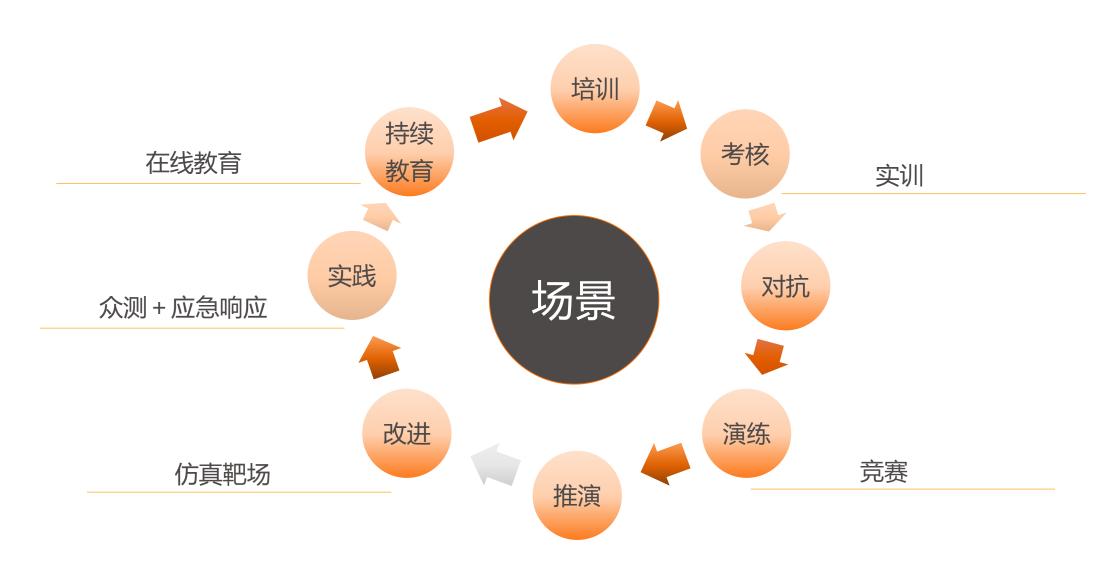


#### ZERO TRUST SECURITY

## 场景支撑网络安全实践教育形成闭环







### 不忘初心,继续前行











聚焦优势 言作其生 有信有诺







# 谢谢!

ISC 互联网安全大会 中国·北京

Internet Security Conference 2018 Beijing · China

(原"中国互联网安全大会")