

# 字节跳动安全事件运营体系建设

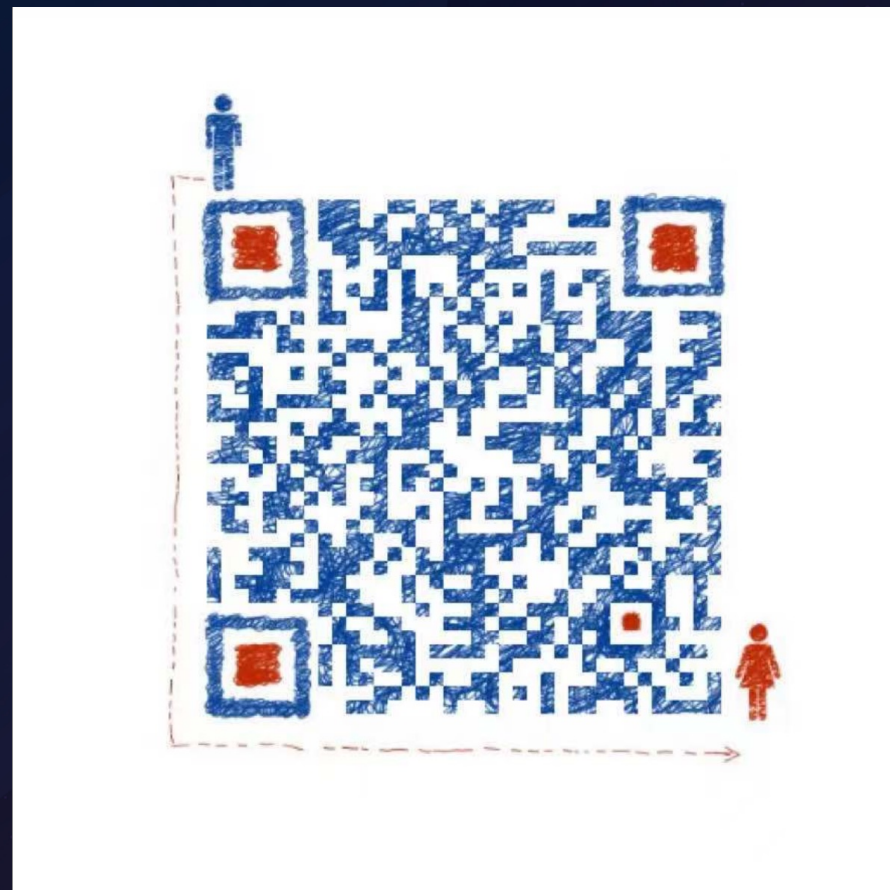
字节跳动安全中心  
陈明

实战攻防



# 关于我

- 目前在字节跳动安全中心团队负责安全事件运营工作
- 曾在腾讯云先后负责DDoS防护产品和云平台安全
- 10年信息安全从业经验
- CISSP、CISA、CCSK



# 大纲

安全事件运营体系介绍

## 01

安全运营做什么  
安全运营怎么做

运营落地思路

## 02

痛点和难点  
如何应对

未来展望

## 03

从繁琐的运营工作中抓住本质



PART

01

安全事件运营体系介绍



# 安全事件运营做什么

负责公司反入侵相关安全事件的运营，包括告警和规则运营、分析研判、溯源取证、调查整改，并为结果负责

涵盖国内各类业务



覆盖主要安全产品和能力

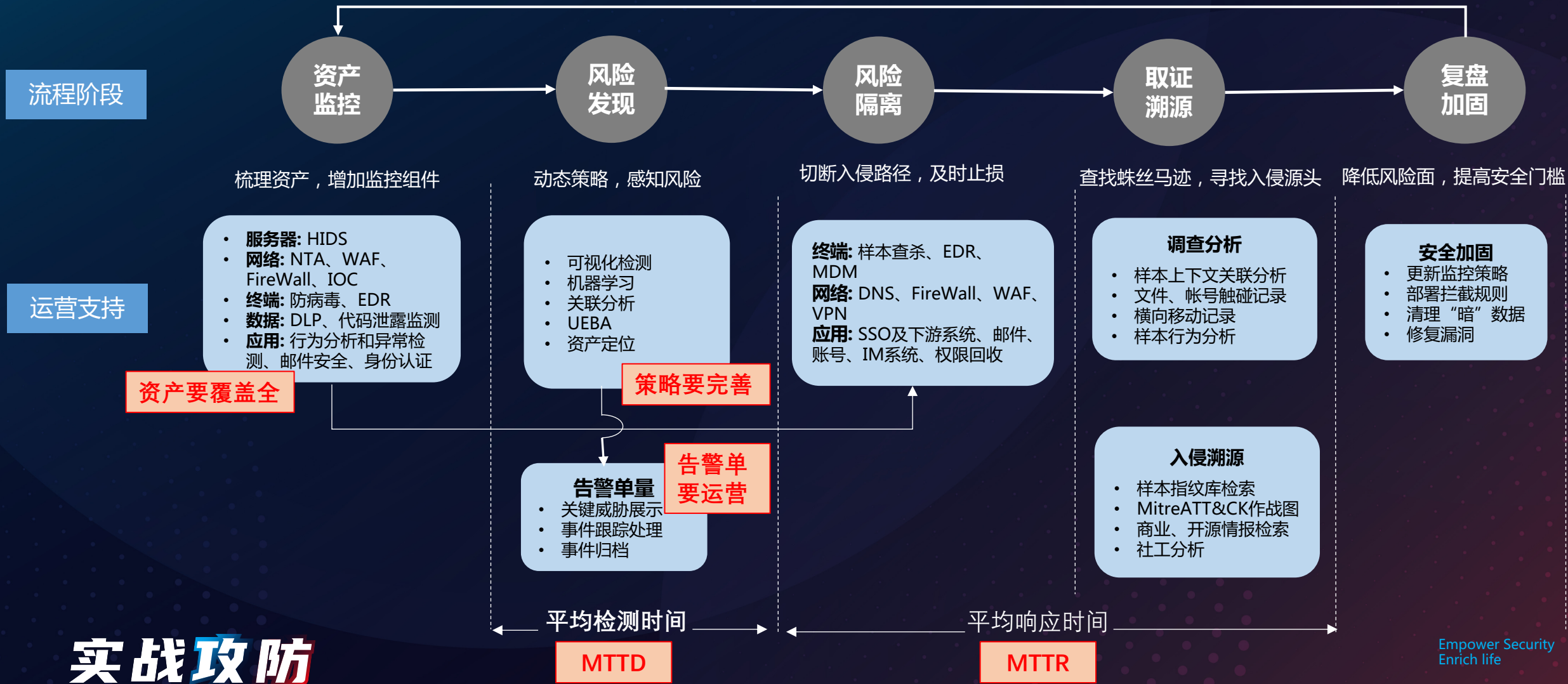
服务器：HIDS  
网络：NTA、WAF、防火墙、IOC情报  
终端：防病毒、EDR  
数据：DLP、代码泄露监测  
应用：行为分析和异常检测、邮件安全、身份认证、RASP

应急响应和HVV

主导开展应急响应  
组织HVV防守工作

## 实战攻防

# 安全事件运营体系





## 难点和痛点

漏水



资产覆盖、规则完整度  
有效的检测和防御

海量告警



如何找到真实有效的告警  
如何找到最需要关注的告警

速度 (MTTD、MTTR)



和攻击者的赛跑，事后发现几乎无济于事  
运营成本高，分析和处置繁琐

# 实战攻防

PART  
运营落地思路

02





# 运营思路

## 基础安全能力的覆盖

确保各项基础安全能力的全覆盖

## 重点环节设防、保护核心资产

针对入侵中的关键环节和核心资产重点保护

## 借鉴业界成熟框架，查漏补缺

参考att&ck、killchain框架，确保每个ttps都能覆盖



## 优先关注内网告警事件

相比外网，需要优先关注内网环境的告警

## 红蓝对抗，以攻促防

通过持续不断的红蓝对抗去暴露和发现防守中的薄弱点，持续改进

## 专项收敛风险，从根源解决风险

共性问题通过专项形式推动收敛，从源头入手，规避风险产生

# 实战攻防

# 基础安全能力的覆盖

持续建设和完善

资产管理  
主动探测  
被动流量发现

从源头和关键节点入手，四两拨千斤

关键点覆盖  
网络出口、网关覆盖  
镜像母版  
终端基线

上线卡点，高风险资产重点覆盖

安全卡点  
SDLC  
白名单申请

实战攻防

# 重点环节设防、保护核心资产

## 边界突破

网络：私搭wifi治理、wifi认证异常（非常用设备、IP、多终端、多地域）、VPN盗用  
EDR：终端入侵检测、钓鱼、水坑攻击  
互联网暴露面：收敛对外暴露的高危端口和服务

## 横向移动

ueba：账号、IP行为基线（网络行为、各类应用系统操作、身份认证）  
敏感系统操作：跳板机、代码平台、数据分析平台、任务管理系统

## 围绕数据和核心系统

数据：有哪些敏感数据、触碰数据的路径有哪些、针对数据库的操作审计、本地sql工具直连、后台系统操作监控、通过票据定位到人  
核心系统重点保障



# 策略实现不难，难的是如何运营

通过wifi、vpn接入身份和sso身份比对发现账号盗用

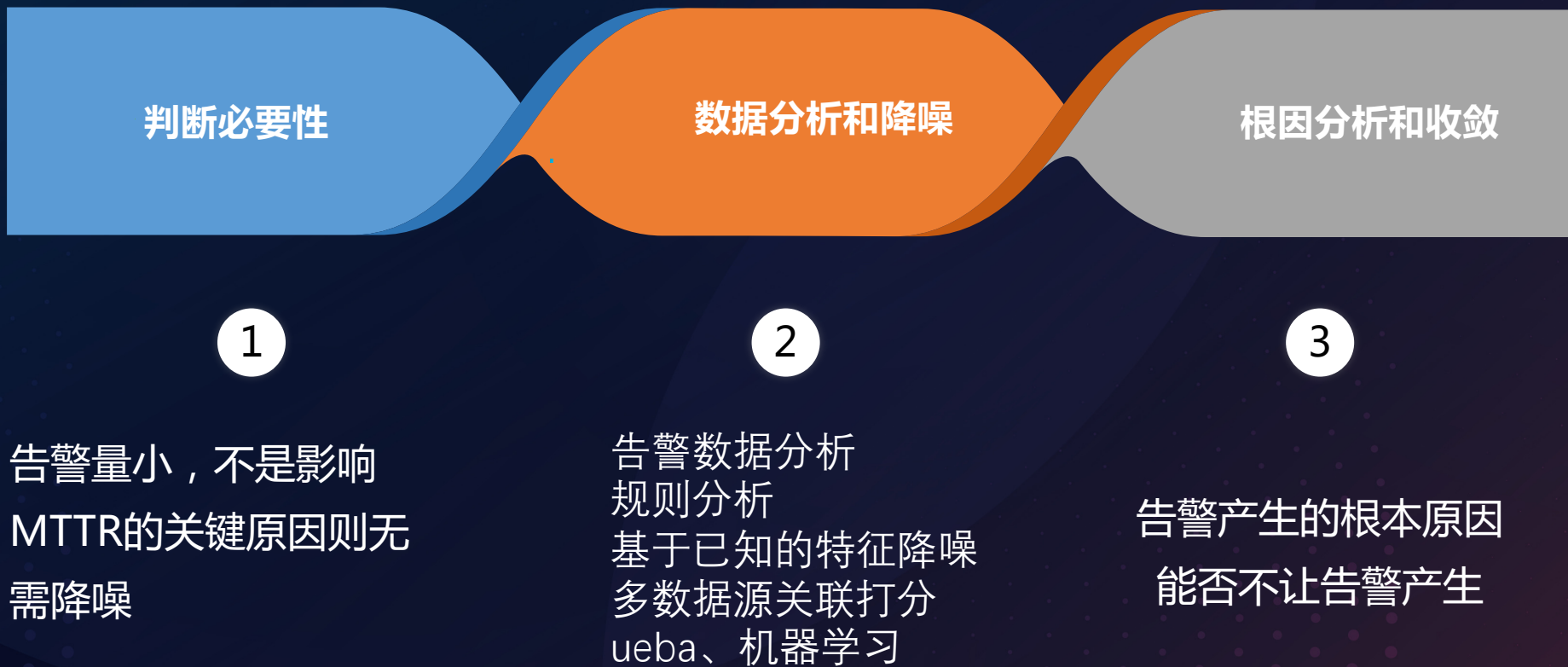
user\_login\_risk ⓘ

序号	ip	账户异常标签 ...	源用户登录时间 s...	网络持有人登录时...	盗用源用户名 src...	源用户部门 src_dep	源用户序列src_seq	网络持有人 dst_u...	网络持有人部门 dst_dep
1	192.168.1.1	sso_wifi	2021-07-03 19:...	2021-07-01 17:2...	张三	技术部	10000000000000000000	张三	技术部
2	192.168.1.1	sso_wifi	2021-07-03 16:...	2021-07-01 23:0...	李四	技术部	10000000000000000000	李四	技术部
3	192.168.1.1	sso_vpn	2021-07-03 13:...	2021-07-03 12:0...	王五	技术部	10000000000000000000	王五	技术部

需要通过告警**降噪**，从技术和管理两个维度去持续优化

**实战攻防**

# 如何做告警降噪



## 举例：NTA告警降噪

办公网nta两周告警量在40万条以上，单日告警量接近3万

数据分析：占比最大的为其它攻击利用（主要为矿池域名访问）、Sql注入（内部黑盒扫描）、信息泄露（未按目标系统聚合）

检测逻辑：部分规则只检测请求，未关联响应

降噪思路：

- 1、规则优化，关联响应及会话
- 2、针对不同规则的检测逻辑做告警聚合
- 3、内部扫描加白
- 4、恶意域名封禁，阻断访问并给予引导
- 5、关联终端、网络等其它数据
- 6、ip行为建模，挖掘更高优的告警



## 专项收敛风险

共性和经常发生的问题不能只是处理单个case，需要进行根因分析并对症下药

案例：发现内网出现大量存在远程代码执行的系统

根因分析：1、由于办公网到生产网的网络隔离，部分研发为了方便操作线上服务器，自行搭建webshell平台 2、部分研发同学认为在内网很安全，不清楚此举对公司的危害

应对方案：联合运维、安全培训、研发团队启动专项 1、加强安全意识宣贯，让研发同学意识到危害 2、完善制度，加入安全红线 3、加强检测，定期通报违规 4、优化跳板机体验



## 优先关注内网告警

### 内网不安全

- 员工会普遍认为内网很安全，反而放松警惕，认为内网安全问题不重要
- 外网系统有严格的上线卡点（SDLC），每天遭受大量攻击（SRC、黑客等）
- 以上两点导致内网的安全问题更多

### 依赖人的安全一定会漏水

- 依赖员工安全意识的防护体系一定会漏水
- 安全意识培训仍需要做，可以把及时反馈也做为目标之一

### ROI更高

- 会涉及更为敏感的系统和数据
- 相比外网告警更好治理
- 整体量级更少



# 红蓝演练，以攻促防



## 定期演练

尽量使用不同的  
攻击手法



## 针对性演练

对补齐的能力点  
针对性检验



## 持续改善

确保改进措施落地

实战攻防

# 借鉴业界成熟框架，查漏补缺

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (5)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (6)	Access Token Manipulation (6)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Infer-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deofuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repositories (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Escape to Host	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)	Network Authentication Process (4)	Domain Trust Discovery	Taint Shared Content	Data from Local System	igmpres Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Exploitation for Defense Evasion	OS Credential Dumping (8)	Network Service Scanning		Data from Removable Media	Non-Application Layer Protocol	Resource Hijacking	Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	File and Directory Permissions Modification (2)	Steal Application Access Token	Network Share Discovery		Data Staged (2)	Non-Standard Port	Service Stop	System Shutdown/Reboot
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (7)	Hide Artifacts (7)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Email Collection (3)	Protocol Tunneling		
				Modify Authentication Process (4)	Valid Accounts (4)	Hijack Execution Flow (11)	Steal Web Session Cookie	Password Policy Discovery		Input Capture (4)	Proxy (4)		
				Office Application Startup (6)		Impair Defenses (7)	Two-Factor Authentication Interception	Peripheral Device Discovery		Man in the Browser	Remote Access Software		
				Pre-OS Boot (5)		Indicator Removal on Host (4)	Unsecured Credentials (7)	Permission Groups Discovery (3)		Man-in-the-Middle (2)	Traffic Signaling (1)		
				Scheduled Task/Job (7)		Indirect Command Execution		Process Discovery		Screen Capture	Web Service (3)		
				Server Software Component (3)		Masquerading (6)		Query Registry		Video Capture			
				Traffic Signaling (1)		Modify Authentication Process (4)		Remote System Discovery					
				Valid Accounts (4)		Modify Cloud Compute Infrastructure (4)		Software Discovery (1)					
						Modify Registry		System Information Discovery					
						Modify System Image (2)		System Location Discovery					
						Network Boundary Bridging (1)		System Network Configuration Discovery (1)					
						Obfuscated Files or Information (5)		System Network Connections Discovery					
						Pre-OS Boot (5)		System Owner/User Discovery					
						Process Injection (11)		System Service Discovery					
						Rogue Domain Controller		System Time Discovery					
						Rootkit		Virtualization/Sandbox Evasion (3)					
						Signed Script Proxy Execution (11)							
						Signed Script Proxy Execution (11)							
						Subvert Trust Controls (6)							
						Template Injection							
						Traffic Signaling (1)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						XSL Script Processing							

PART

未来展望

03





# 从繁杂的工作中抓住本质

## 安全能力的持续覆盖

持续完善各类安全产品和能力的资产及策略覆盖，持续提升单点检出及防御能力



## 风险的持续收敛

持续不断的分析根因，从根源收敛风险



## 运营效率的持续提升

持续关注MTTD、MTTR，提升运营团队综合作战能力



## 平台的持续建设

结合业务和运营需求，持续完善SOC平台能力，为运营做好支撑



实战攻防

# THANK YOU FOR READING

---

## 实战攻防



字节跳动  
安全中心



安全范儿  
BYTEDANCE SECURITY