

洞明智能安全威胁监测平台

产品介绍

2025年11月

目录

MULU

1

背景

2

核心功能

3

优势亮点

4

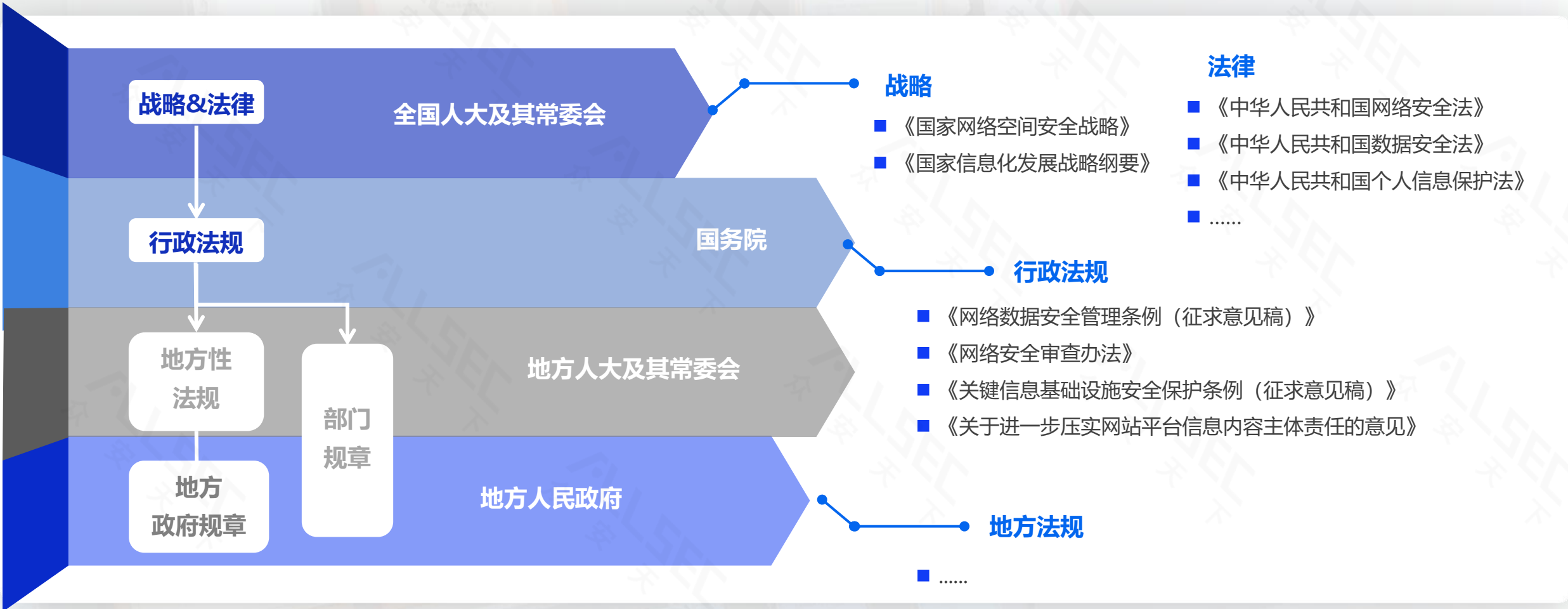
典型案例

```
if (a) {
  for (; o = i; i++)
    if (r = t.apply(e[i], a), r === !1) break
} else
  for (i in e)
    if (r = t.apply(e[i], a), r === !1) break
} else if (a) {
  for (; o = i; i++)
    if (r = t.call(e[i], i, e[i]), r === !1) break
} else
  for (i in e)
    if (r = t.call(e[i], i, e[i]), r === !1) break;
return e
},
trim: b && !b.call("\uffff\u00a0") ? function(e) {
  return null == e ? "" : b.call(e)
} : function(e) {
  return null == e ? "" : (e + "").replace(C, "")
},
isArray: function(e, t) {
  var n = t || [];
  return null != e && (N(Object(e)) ? x.merge(n, "string" == typeof e ? [e] : e) : b.call(n, e)), e
},
isArray: function(e, t, a) {
```

01 背景

国家层面对网络设施主体提出更高的要求

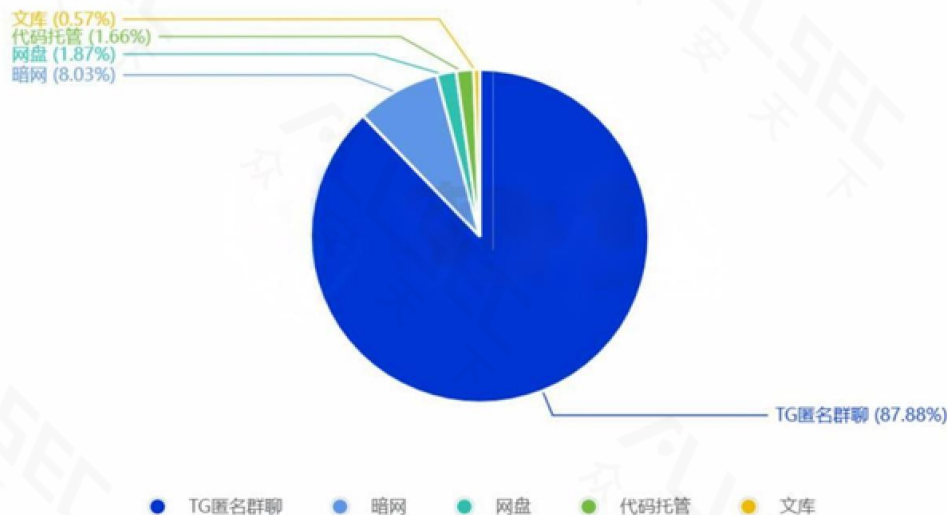
2014年4月，习近平总书记就在中央网络安全和信息化领导小组第一次会议上指出：“**没有网络安全就没有国家安全，没有信息化就没有现代化**”。2019年6月，《网络安全漏洞管理规定（征求意见稿）》要求所属单位发现漏洞后，立即对漏洞进行验证，对相关网络产品应当在**90日内采取漏洞修补或防范措施**。



网络安全漏洞数量逐年上涨

据新华三发布的《2025年网络安全漏洞态势报告》统计，2025年上半年数据泄露事件共计16011起，较2024年下半年增长59.58%。据数据泄露风险监测平台数据显示，2025年上半年（1-6月）全网监测到的1.1亿条情报中，基于真实性验证引擎及DRRC人工分析验证有效的数据泄露事件共计16011起，较2024年下半年增长59.58%，9539起。

2025年1月至6月数据泄露事件渠道分布占比情况



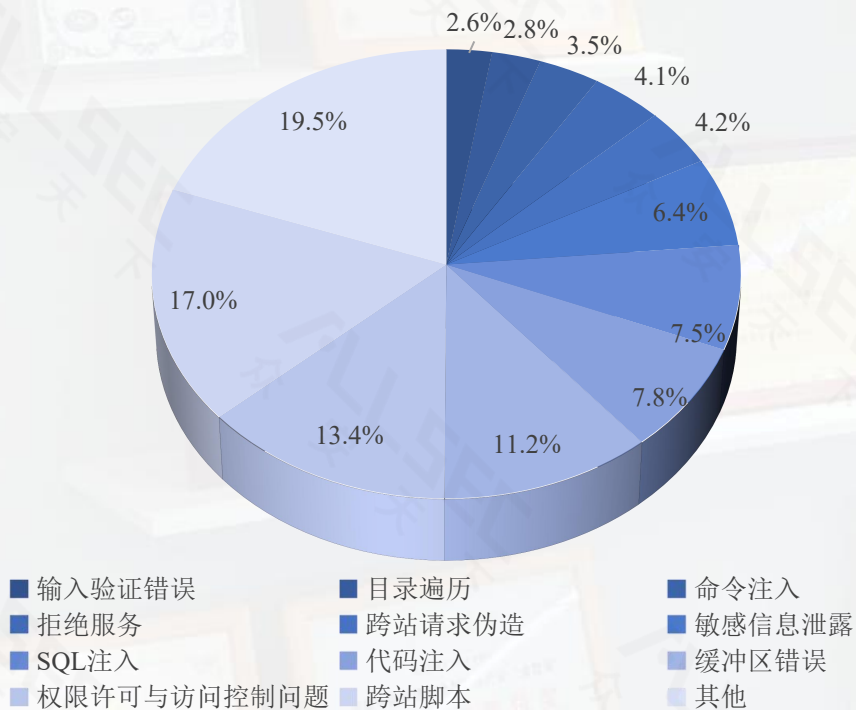
2024年7月至2025年6月数据泄露事件数变化趋势



黑客攻击手段不断演化

生成式人工智能等一批新技术在带来巨大机遇的同时，也意味着其在安全性上会产生更多挑战，2025年，针对各个领域网络资产的攻击进一步加剧。

演化特点



新华三统计了2025年漏洞攻击类别，排名前三的漏洞为跨站脚本、权限许可和访问控制、缓冲区错误，分别占比 17.0%，13.4%和 11.2%。

1

漏洞数量持续增长，0day 漏洞利用数量明显增加

大量攻击团伙利用未公开及厂商未及时修复的漏洞对目标系统进行未授权访问、数据窃取、数据勒索或其他恶意活动。如GoAnywhere 的 CVE-2023-0669 漏洞被黑客大规模利用，政府、能源、金融、医疗行业等成为攻击受害者，展现了“零日漏洞+供应链攻击”的可怕。

2

身份验证和访问权限管理不当漏洞增加

企业和组织不断推进内外网业务由线下转向线上，业务数据大量产生、传输、交互、公开。不同系统、软件 and 应用程序的默认配置、身份验证和访问权限管理等配置不当问题逐渐成为网络中最易忽视的攻击风险。错误配置可能会为攻击者提供突破口，以入侵单个安全控制点作为跳板进一步危及整个系统的安全性。

3

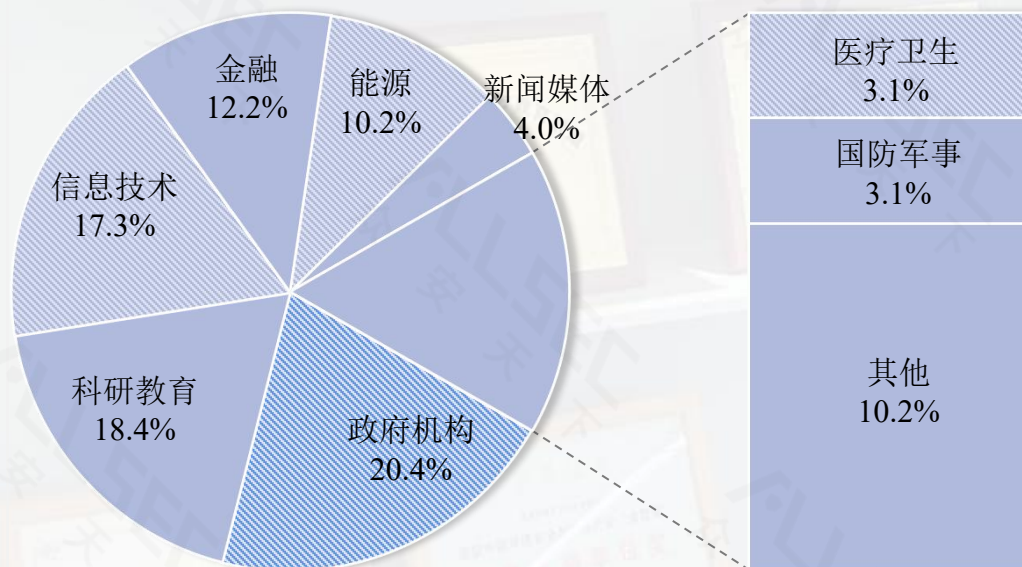
大语言模型成为攻防“双刃剑”，加剧攻防不对等

在不断对抗发展的网络安全领域，大语言模型不仅成为抵御复杂网络攻击的利器，也已然被攻击者充分利用，不断开发演进新的攻击方式。例如防御方面可以开发和建立自动化威胁检测和安全防护系统等，攻击方面可以用于攻击自动化、智能化社会工程攻击、恶意软件检测规避等，大语言模型的应用也极大地降低了攻击利用的门槛。

网络安全事件层出不穷

据奇安信威胁情报中心发布《全球高级持续性威胁（APT）2025年度报告》统计，近年来，针对关键信息基础设施的信息窃取、攻击破坏等恶意活动持续增加。

2025年公开APT报告涉及行业分布



2025年已知网络安全事件

2025-01

美国T-Mobile遭到黑客攻击，3700万用户信息被窃

美国电信运营商 T-Mobile 发布安全公告称公司网络遭到黑客攻击，并从中窃取了涉及 3700 万用户信息。

2025-02

亲俄黑客对机场网站欧管机构发起大规模DDoS攻击

亲俄罗斯黑客KillNet对德国机场、行政机构和银行的网站发起的一系列DDoS攻击，当晚导致超过2300架次航班取消，影响近30万乘客出行。

2025-06

美国俄勒冈州交通部遭遇MOVEit攻击，影响350万

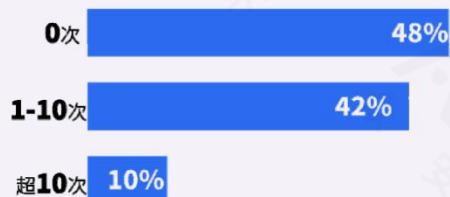
美国俄勒冈州交通部遭遇MOVEit漏洞攻击，350万人的驾驶执照、许可证和身份证的数据记录已经被黑客非法读取。

2025-08

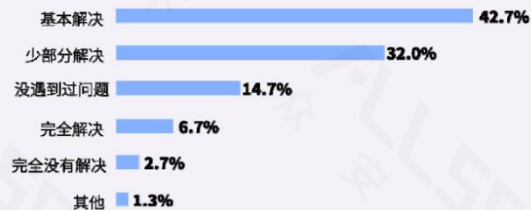
酒店巨头米高梅遭受勒索软件攻击，造成1亿美元损失

全球娱乐和酒店业巨头米高梅国际酒店集团遭到勒索软件攻击，其网站、预订系统和酒店电子钥匙卡系统受到严重影响，对公司造成1亿美元左右的经济损失。

中小企业数字化转型过程中被恶意网络攻击



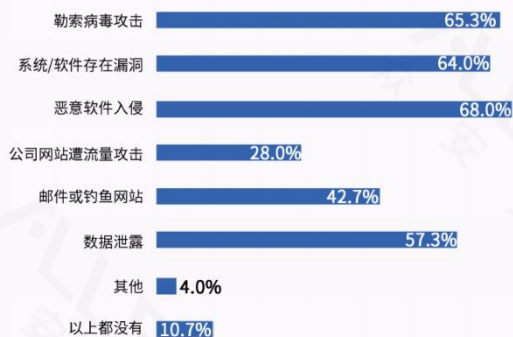
遭受过网络攻击次数
(来源: Devolutions中小企业网络安全状况报告)



遭受网络攻击后缓解情况
(来源: 360)

中小企业遭受网络攻击调查

中小企业数字化转型过程中，大约一半的中小企业(48%)自认为是安全的，没有受到黑客攻击，而事实上，大多数企业被黑客攻击后并不知情。调查数据显示我国有超过 95.3%的中小企业面临非常严峻的数字安全威胁，大量的安全问题长期无法解决，也意味着**攻击者在持续进行攻击**，且存在长期性和广泛性。



我国中小微企业最关注的安全风险
(来源: 360)

中小企业所关注的安全威胁调查

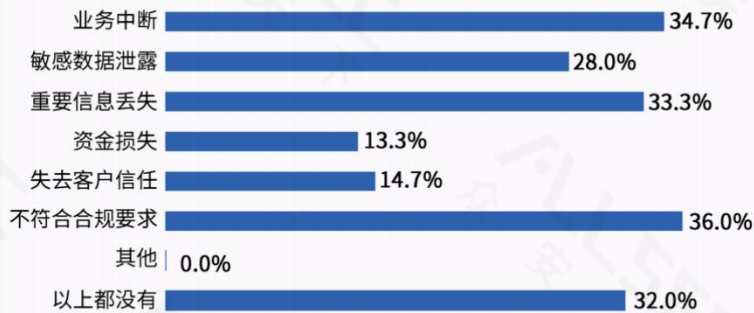


图 2-5 中小微企业数字安全的业务影响调查

中小企业收到网络攻击后产生的业务影响调查

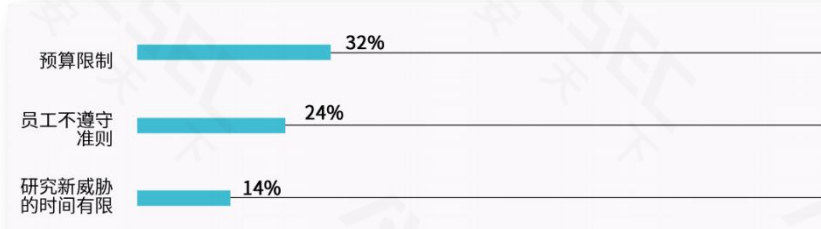
“不符合合规要求”是中小企业数字化转型过程中最担心的。其一是由于自身数字**安全建设不到位**而导致违规，其二是因为遭受黑客组织数字**攻击导致数据泄露**。其次是担心遭到黑客组织数字攻击而导致其**业务中断**，另外还关注敏感信息丢失的风险。

中小企业面临的风险管理的问题

中小企业在风险管理工作中的常见问题



中小企业IT安全方面面临的障碍



在全球信息安全调查报告 (GISS) 报告中，新冠疫情催化了云计算等技术的应用以及办公场景的变革，企业因此需要应对更加复杂多样的网络安全风险，然而**超过四分之三的中国受访企业(75%)不确定其网络安全防御体系是否足以应对黑客的攻击。**

经过走访调研，我们发现**网络资产管理混乱、网络抗风险能力差、安全人才与制度缺失、IT安全预算不足**等现象普遍存在于网络资源管理中。

```
if (a) {  
  for (i = 0; i < l; i++)  
    if (r = t.apply(e[i], a), r === !1) break  
} else  
  for (i in e)  
    if (r = t.apply(e[i], a), r === !1) break  
} else if (a) {  
  for (i = 0; i < l; i++)  
    if (r = t.call(e[i], i, e[i]), r === !1) break  
} else  
  for (i in e)  
    if (r = t.call(e[i], i, e[i]), r === !1) break;  
return e  
},  
trim: b && !b.call("\uffu00a0") ? function(e) {  
  return null == e ? "" : b.call(e)  
} : function(e) {  
  return null == e ? "" : (e + "").replace(C, "")  
},  
isArray: function(e, t) {  
  var n = t || [];  
  return null != e && (N(Object(e)) ? x.merge(n, "string" == typeof e ? [e] : e) : b.call(n, e)), e  
},  
isArray: function(e, t, n) {
```

核心功能

智能攻击面与资产治理解决方案



洞明平台深度融合AI与前沿安全技术，旨在为客户提供全面的互联网攻击面监测与资产态势深度分析。通过精准的资产建模与多源数据融合，助力企业清晰掌握网络安全现状，快速定位关键漏洞，并智能感知事件型漏洞威胁。



智能攻击面探测与数据分析

- 主动探测引擎：分布式扫描 + 空间测绘 + 被动数据，立体监控攻击面。
- 被动数据引擎：证书透明度+DNS海量数据集+搜索引擎等情报源，发现静默式资产。
- 智能关联引擎：跨域策略分析+爬虫堆积检索等技术对多源数据关联融合完善精度

利用资产指纹库，建立资产动态台账

- IP归集
- 服务识别
- 端口发现
- WAF标识

资产发现与动态台账构建

针对性发现隐藏资产，完善资产指纹

资产模型与可视化梳理

建立资产族谱及可视化清单

资产登记与责任落地

建立资产登记台账，将资产责任到人

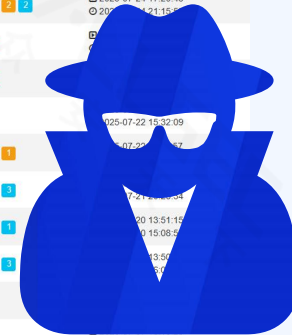
洞明系列解决方案能力已经在超过100+攻防演练与专项上输出海量高质量成果，助力高效交付。

ALLSEC
众安天下

6034 组件模块数量		1294 高危数量	343 中危数量	67 低危数量	33 提示数量				
组件名称	漏洞	漏洞ID	漏洞名称	漏洞类型	厂商/产品名称	修复方案	更新时间		
高危	✓	6014	索尼摄像头存在远程代码执行漏洞(CVE-2021-36000)	命令执行	杭州海康威视数字技术股份有限公司	CVE-2021-36000	2025-07-16 18:24:10		
中危		6013	大华摄像头存在远程代码执行漏洞(CVE-2021-33084)	命令执行	浙江大华技术股份有限公司	CVE-2021-33084	2025-07-16 18:24:10		
低危		6012	NetServer 日志管理工具存在 Remote_xxx 注入漏洞	SQL注入	NetServer	NetServer	2025-09-20 14:55:55		
提示		6011	致远互联 EIM 协作平台存在 add_header_page_sql 注入漏洞(CVE-2020-2030)	SQL注入	北京致远互联软件股份有限公司	致远互联 EIM 协作平台	2025-09-19 18:37:37		
		6010	用友 U8_CRM_blackboardcontrol 存在 sql 注入漏洞	SQL注入	北京用友软件股份有限公司	用友U8CRM	2025-05-19 18:00:00		
		6009	WordPress_depotcms 存在 sql 注入漏洞(CVE-2020-2011)	SQL注入	WordPress	WordPress_depotcms	2025-05-19 17:30:30		
		6008	7P/POA_documentshistory 存在 sql 注入漏洞	SQL注入	7P/POA	7P/POA	2025-09-19 16:05:05		
		6007	泛微 e-office_erpstatus 存在 sql 注入漏洞	SQL注入	上海泛微网络科技股份有限公司	泛微网络(e-office_erpstatus)	2025-05-19 16:55:56		
		6006	SysAid_On_Prem_MAL 存在 sql 注入漏洞(CVE-2020-2776)	XSS	SysAid Co-Prem	SysAid Co-Prem	2025-05-19 16:55:05		
		6005	Langflow AI 存在远程命令执行漏洞(CVE-2020-5246)	命令执行	Orbitalk	Langflow	2025-09-16 13:43:24		
		6004	JetWMS_IconControl 存在 任意文件上传漏洞	文件上传	JECEWMS	JECEWMS	2025-05-07 21:13:59		
		6003	JetWMS_oginurl 存在 sql 注入漏洞	SQL注入	JECEWMS	JECEWMS	2025-05-07 21:13:52		
		6002	树玟数据云运营绩效管理工具 updatelogs 存在 sql 注入漏洞	SQL注入	北京树玟网络科技有限公司	树玟数据云运营绩效管理工具	2025-05-19 15:03:02		

描述	集群	编排	流程状态	任务状态	运行	风险	时间
陕西榆林市子洲县子州镇子州村	guangzhou	new_collect_info_poc	finished	finished	总调用: 1575/1577 分任务: 1390129/1390129	2 13 4	🕒 2025-08-04 21:07:44 🕒 2025-08-07 09:51:12
陕西榆林市子洲县子州镇子州村2	hangzhou	new_collect_info_poc	finished	finished	总调用: 1575/1577 分任务: 1472441/1472441	5 22 15	🕒 2025-08-04 21:05:17 🕒 2025-08-06 13:11:28
好未来集团上海分公司	shanghai	new_collect_info_poc	finished	finished	总调用: 1575/1577 分任务: 1383359/1383359	1 3 1	🕒 2025-08-04 21:04:45 🕒 2025-08-07 13:41:51
好未来集团杭州分公司	hangzhou	new_collect_info_poc	finished	finished	总调用: 1571/1573 分任务: 1802801/1802801	6 7 7	🕒 2025-07-31 15:36:23 🕒 2025-06-01 08:27:16
好未来集团上海分公司	shanghai	new_collect_info_poc	finished	finished	总调用: 1573/1573 分任务: 165/165		🕒 2025-07-31 14:33:27 🕒 2025-07-31 15:33:22
陕西榆林市子洲县子州镇子州村	hangzhou	new_collect_info_poc	finished	finished	总调用: 1571/1573 分任务: 175131/175131	1 2 2	🕒 2025-07-24 17:20:48 🕒 2025-07-24 12:16:55
陕西榆林市子洲县子州镇子州村	shanghai	new_collect_info_poc	finished	finished	总调用: 1571/1573 分任务: 214393/214393	5	🕒 2025-07-24 17:20:48 🕒 2025-07-24 12:16:55
陕西榆林市子洲县子州镇子州村	hangzhou	new_collect_info_poc	finished	finished	总调用: 1571/1573 分任务: 82934/82934	4	🕒 2025-07-24 17:20:48 🕒 2025-07-24 12:16:55
陕西榆林市子洲县子州镇子州村	shanghai	new_collect_info_poc	finished	finished	总调用: 1571/1573 分任务: 1546/1546		🕒 2025-07-24 17:20:48 🕒 2025-07-24 12:16:55
陕西榆林市子洲县子州镇子州村及子公司扫描1	shanghai	new_collect_info_poc	finished	finished	总调用: 1571/1573 分任务: 32276/32276	1 1	🕒 2025-07-24 17:20:48 🕒 2025-07-24 12:16:55
陕西榆林市子洲县子州镇子州村公司扫描	chengdu	new_collect_info_poc	finished	finished	总调用: 1571/1573 分任务: 121328/121328	1 1	🕒 2025-07-24 17:20:48 🕒 2025-07-24 12:16:55
陕西榆林市子洲县子州镇子州村下属单位	hangzhou	new_collect_info_poc	finished	finished	总调用: 1571/1573 分任务: 53764/53764	2 1	🕒 2025-07-24 17:20:48 🕒 2025-07-24 12:16:55
陕西榆林市子洲县子州镇子州村化工扫描1	chengdu	new_collect_info_poc	finished	finished	总调用: 1571/1573 分任务: 113621/113621	4 1	🕒 2025-07-24 17:20:48 🕒 2025-07-24 12:16:55
陕西榆林市子洲县子州镇子州村自-2025-7-11	chengdu	new_collect_info_poc	finished	finished	总调用: 1571/1573 分任务: 73673/73673		🕒 2025-07-24 17:20:48 🕒 2025-07-24 12:16:55
中核集团(陕西)有限公司	dongming	collect_info	finished	finished	总调用: 23/23 分任务: 1496/1496		🕒 2025-07-07 19:02:01

立足攻击者视角

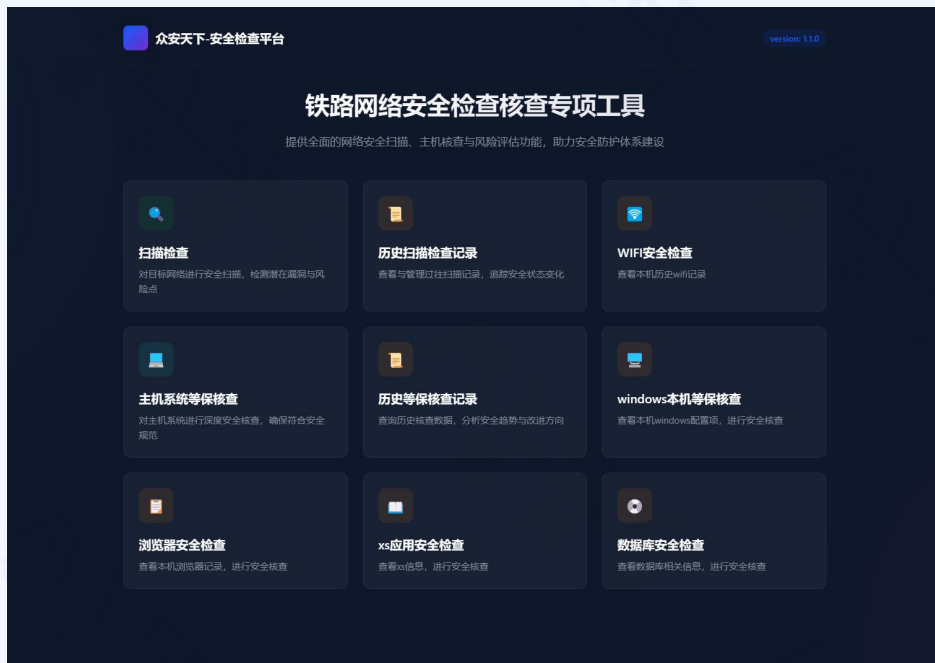


洞明- 软硬件一体化专业安全评估解决方案



软硬件一体化专业安全评估解决方案

基于超10年实战攻防经验与自主研发的核心扫描引擎，集成数千漏洞利用场景、可定制忒定行业/0day情报及白帽社区实战漏洞库，具备深度资产风险识别与精准漏洞发现能力，专为现场网络渗透与专项检查场景设计。



洞明便携式安全检查工具箱
(公安专版)
无害化攻击取证工具箱 (公安专版)

面向铁路或关基行业系统的软硬件一体化安全检查平台，提供覆盖网络、主机、数据、应用的全方位核查能力，助力构建实战化安全运营体系，可面向特定行业设计定制安全规则（供应链-通用漏洞规则）。

```
if (a) {  
  for (i = 0; i < l; i++)  
    if (r = t.apply(e[i], a), r === !1) break  
} else  
  for (i in e)  
    if (r = t.apply(e[i], a), r === !1) break  
} else if (a) {  
  for (i = 0; i < l; i++)  
    if (r = t.call(e[i], i, e[i]), r === !1) break  
} else  
  for (i in e)  
    if (r = t.call(e[i], i, e[i]), r === !1) break;  
return e  
},  
trim: b && !b.call("\uffff\u00a0") ? function(e) {  
  return null == e ? "" : b.call(e)  
} : function(e) {  
  return null == e ? "" : (e + "").replace(C, "")  
},  
isArray: function(e, t) {  
  var n = t || [];  
  return null != e && (N(Object(e)) ? x.merge(n, "string" == typeof e ? [e] : e) : b.call(n, e)), n  
},  
isArray: function(e, t, n) {
```

03

优势亮点

优势亮点：多技术引擎基底

系统漏洞扫描技术

能够快速发现远程溢出漏洞、Openssl心脏出血漏洞、Ftp弱口令漏洞、Redis未授权访问漏洞、MySQL弱口令漏洞、SSH弱口令漏洞、Mongodb弱口令漏洞、MsSql弱口令漏洞、Postgres弱口令漏洞、Rsync弱口令漏洞等。

web2.0漏洞扫描技术

针对SQL注入漏洞、跨站脚本漏洞、任意文件上传漏洞、命令执行漏洞、代码执行漏洞、目录遍历漏洞、弱口令漏洞、文件包含漏洞等数千个漏洞的检测技术。

敏感文件探测技术

针对备份文件、数据库敏感文件、管理后台、PHPinfo敏感文件、常见敏感目录的探测技术。

邮箱账户安全检测技术

识别有效账户，并对账户口令进行安全检测。

未知漏洞(0Day)

内置数百个0Day漏洞，产品风险发现能力强。

CDN识别技术

减少无效测试路径。

构建多技术引擎基底，自研应用系统识别系统及poc分布式靶向扫描框架，**打破了传统安全扫描类产品发送大量无效测试包、扫描效率低及误报高等问题，突破安全行业技术瓶颈。**

优势亮点：自动化资产发现



自动化资产发现技术

平台通过自动化资产发现技术，智能识别网络中的各类资产

实时监控

实时监控网络中的新增或变更资产，为后续提供数据支持

及时反映网络资产的当前状态

优势亮点：实时漏洞扫描

识别漏洞

平台提供自动识别和评估系统中的漏洞

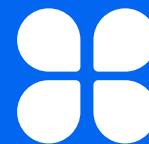
提供详细的漏洞信息

供详细的漏洞信息和修复建议，更新漏洞数据库，帮助企业有效地管理漏洞的生命周期

自动识别

详细漏洞信息

更新漏洞数据库



优势亮点：弹性资源调度

按需分配资源

实现按需分配计算资源，
实现基于流量和负载的
自动扩缩容机制

应对流量高峰

当检测到流量增加时，
自动增加资源以应对需求；
在流量减少时，相应减少资源以节省成本

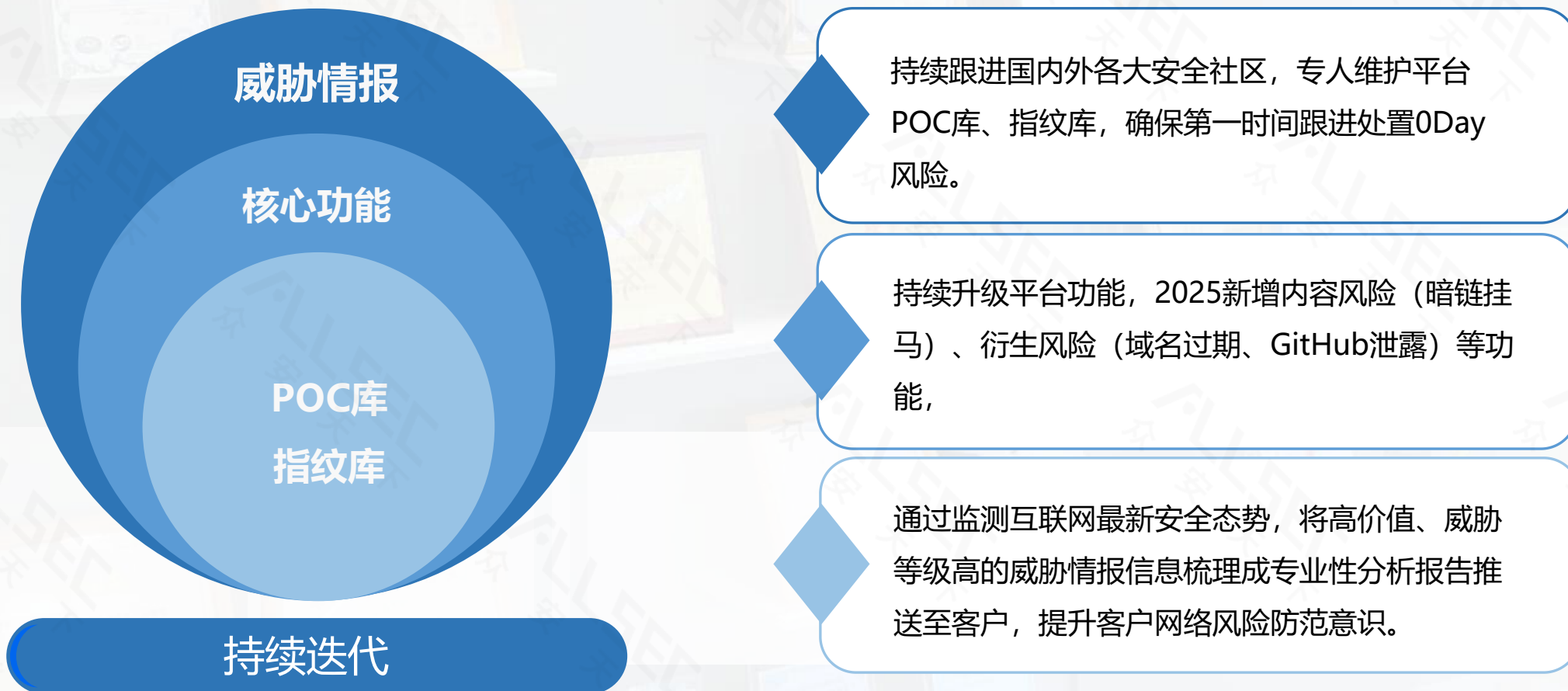
优势亮点：供应链风险评估



增强企业的风险防范和处理能力

优势亮点：持续迭代富有生命力

平台持续跟进国内外各大安全社区，如Exploit-db、Seebug、国家信息安全漏洞共享平台、国家信息安全漏洞库以及实战经验所沉淀的行业漏洞库信息等,依托数千顶级白帽专家赋能安全产品，持续性根据用户需求、市场变化、安全态势迭代产品。



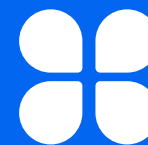
优势亮点：快速落地0day漏洞情报

- **完善的情报管理体系，迅速收集和分析0day漏洞情报**
通过实时监控全球安全情报，及时发现这些漏洞，并利用自动化工具进行深入分析，生成详细的漏洞报告
- 使用户能够及时了解最新的安全威胁，并采取措施保护关键资产免受损害

安全情报实时监控

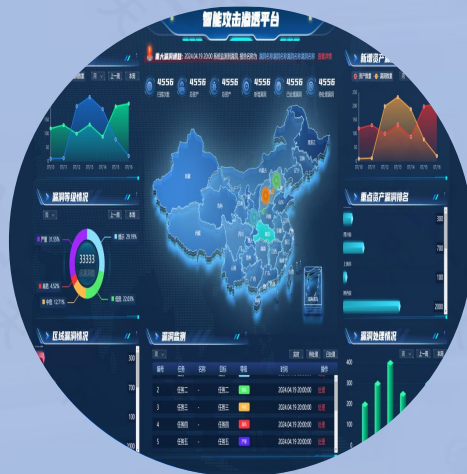
漏洞及时发现

漏洞报告生成



预知安全风险

- 集成威胁情报和大数据分析技术
- 预测潜在的安全风险，并据此提供先发制人的防护措施并且制定应对策略



深入洞察与智能决策

- 运用人工智能和机器学习技术
- 提供深入的安全洞察，帮助用户理解复杂的安全威胁
- 优化安全策略和资源分配

大型企业 网络安全管理

①

- 平台具备资产情报收集、漏洞验证、自动化攻击渗透、成果研判、漏洞利用等功能
- 帮助学员有效理解攻击原理和技术手段，提高实战能力和专业巩固



政府机构 安全态势感知

②

- 平台集成的先进威胁情报和异常行为分析工具
- 预警政府交易系统中的安全漏洞和欺诈行为
- 为政府机构提供强有力的安全保障，确保政府业务的稳定运行

云服务提供商 安全监测

③

- 平台提供了一套全面的安全防护解决方案
- 平台的事前发现并响应安全威胁功能，有并提供及时处理和技术支持，有效保护了云环境的安全性，帮助企业快速回复业务正常运行



网络安全服务公司 安全评估

④

- 洞明平台网络安全服务公司能够为客户提供全面、深入的安全评估服务
- 为网络安全服务公司提升整体安全防护水平

```
if (a) {  
  for (i = 0; i < l; i++)  
    if (r = t.apply(e[i], a), r === !1) break  
} else  
  for (i in e)  
    if (r = t.apply(e[i], a), r === !1) break  
} else if (a) {  
  for (i = 0; i < l; i++)  
    if (r = t.call(e[i], i, e[i]), r === !1) break  
} else  
  for (i in e)  
    if (r = t.call(e[i], i, e[i]), r === !1) break;  
return e  
},  
trim: b && !b.call("\uffff\u00a0") ? function(e) {  
  return null == e ? "" : b.call(e)  
} : function(e) {  
  return null == e ? "" : (e + "").replace(C, "")  
},  
isArray: function(e, t) {  
  var n = t || [];  
  return null != e && (N(Object(e)) ? x.merge(n, "string" == typeof e ? [e] : e) : b.call(n, e)), e  
},  
isArray: function(e, t, n) {
```

04 典型案例

某科技公司风险管理平台

ALLSEC
众安天下

问题背景

网络资产不清晰
漏洞扫描器误报率高
技术支撑不完善，缺少闭环管理

目标

解决网络资产管理混乱、网络抗风险能力差、安全人才与制度缺失等问题

价值

识别资产

识别潜藏在背后的隐匿资产，获得登对完善的网络资产清单。

发现漏洞

深挖网络资产中潜在风险，

修复支撑

通过工单闭环体系及专属管家服务构建闭环管理机制



某局网络风险监管平台

ALLSEC
众安天下

问题背景

对管辖单位的网络资产不清晰
管辖范围网络资产繁多
缺少跨单位之间的风险推送机制
如果误报漏洞影响单位权威性

目标

建立区域安全态势感知机制
建立区域网络资产风险清单
建立专属安全支撑团队

价值

基于指纹库的资产扫描发现大量隐匿WEB资产。
在2周内完成对1000家单位的网络安全风险评估
基于多家单位的数据构建区域安全态势图谱



众安天下 · 天下众安



公司公众号

公司官网: www.allsec.cn 电话: (010) 86395035 邮箱: BD@allsec.cn

