

第十九届全国大学生信息安全竞赛

创新实践能力赛 Build 环节

（基于多源日志的攻击溯源工程）

赛前须知

随着网络攻击日趋智能化、规模化、复杂化，传统人工溯源模式难以适配智能安全运营的高效处置需求，企业安全运营中仍存在多源数据割裂、证据关联困难、攻击链路复盘不完整、分析经验难沉淀等问题。本届比赛 Build 环节以“基于多源日志的攻击溯源工程”为主题，围绕综合企业环境中的多源安全数据，考察参赛队伍对攻击者痕迹的工程化提取、归一化建模、时间线还原和攻击路径图谱构建能力。

Build 环节设置创新实践榜单，并以 5% 的总分占比计入战队总分。Build 环节成果将在比赛结束后面向参赛队伍进行分享交流，用于促进各队伍在安全数据工程、攻击链路分析和自动化溯源方法上的相互学习。

一、基本信息

时间	环节	内容
8 月 12 日	赛题分发	发布选手题目附件包、选手手册和样例提交；选手熟悉数据结构、提交格式和本地校验工具。 发布方式：通过选手预留邮箱发送赛题数据包，数据包内包含赛题、操作方式、上传方式等比赛操作所需指导文件。 发布对象：赛题附件包发送到参赛队伍预留的领队联系邮箱，如未能收到或领队信息有变可及时联系组委会服务人员处理解决。

时间	环节	内容
8 月 12 日 至 17 日	Build 竞赛答题 与提交	选手完成多源日志、PCAP、Windows Event XML 等证据分析，构建证据数据集、攻击时间线、IOC 和攻击路径图谱。 选手根据赛题数据包内的要求对完成的赛题内容通过预留的赛题平台上传。上传截止时间为 8 月 17 日 23 时 59 分 59 秒。 登录方式：报名预留手机号加验证码登录；队伍上传提交时使用唯一 token 进行认证。 注：每队最多 3 次上传机会，系统取该队最高分进入 Build 环节排行榜；上传文件为 submission.zip，最大 30MB，解压后最大 80MB，平台自动解包、校验和评分。 manifest.json 中的 team_id 必须与队伍 token 对应编号一致。到规定时间冻结提交通道并完成客观评分。评分会根据要求发送到参赛选手的邮箱。

时间	环节	内容
8 月 17 日 至 21 日	结果复核与成果整理	组委会技术裁判会根据选手上传的赛题答案进行评分，包括系统自动评定及人工复核，组委会会针对异常提交进行答案及内容的复核。
8 月 22 日	Build 赛成绩公布	公布 Build 环节成绩。

二、赛制介绍

2.1 题目设计考查重点

- 多源异构安全数据处理能力，包括 CSV、JSONL、纯文本日志、PCAP 和 Windows Event XML 等数据类型的解析与关联。
- 攻击链条关联分析能力，能够从外部入口、主机失陷、跳板利用、横向移动、数据收集和外传等阶段中还原攻击路径。
- 自动化证据抽取与归一化能力，能够将日志和 artifact 证据统一映射到可评分的 event_id。
- 攻击路径图谱建模能力，能够用节点和边表达攻击者、主机、账号、服务、数据库、文件、域名等实体关系。
- 面向平台评分的工程化提交能力，能够按照固定 schema 输出可解析、可验证、可复现的结构化结果。

2.2 比赛任务要求

主办方将提供一个模拟真实企业的五天多源取证附件包。包含资产清单、账号清单、网络分区、边界设备日志、网络流量日志、Linux/Windows 主机日志、应用审计、数据库审计、云与容器审计、安全告警、PCAP 流量包和 Windows Event XML 导出。参赛队伍需

要从附件包中识别成功发生且对攻击链有因果贡献的行为，提交结构化证据、时间线、IOC 和攻击路径拓扑。

本题不以 flag 为核心目标，也不要求提交自然语言报告。所有得分均由固定字段与标准答案自动比对计算；多报无关事件会降低准确率。

2.2.1 攻击者痕迹证据数据集构建

任务背景：企业真实安全运营场景中，攻击证据通常分散在不同设备、不同格式、不同时间窗口的日志与流量材料中，单一日志源很难完整支撑攻击链路判断。

任务目标：从主办方数据包中提取攻击者相关证据，形成可由平台自动评分的证据数据集、时间线和 IOC 集合。

识别外部攻击入口、命令执行、持久化、凭据访问、凭据使用、发现、横向移动、数据收集、规避和外传等关键阶段证据。

PCAP 与 Windows Event XML 为正式证据源，选手必须将分析得到的 packet 或 XML event 映射为 artifact event_id 后提交。

只提交成功发生且对后续攻击链有因果贡献的行为；失败登录、拒绝访问、正常扫描、正常发布和正常备份等噪声不应作为攻击路径提交。

2.2.2 攻击路径拓扑图谱构建

任务背景：复杂入侵往往不是单一路径，而是一个入口、一个或多个跳板、多条并行分支和最终汇总外传的组合过程。

任务目标：围绕攻击者、主机、账号、文件、服务、数据库、云资源和外联域名等实体，构建攻击路径拓扑图。

攻击图节点应表达攻击涉及的核心实体，如 IP、主机、账号、文件、服务、数据库、域名、对象存储桶和 Kubernetes 集群。

攻击图边应表达实体之间的攻击行为关系，包括 from、to、action、stage、time_start、time_end 和 evidence_ids。

选手可以直接编写 attack_graph.json，也可以先维护 graph_nodes.csv 和 graph_edges.csv，再使用工具生成 attack_graph.json。

攻击图应覆盖主路径和并行分支，避免只提交入口攻击或只提交单条线性路径。

三、提交文件与格式

最终提交文件为 submission.zip，解压后根目录应直接包含以下核心文件：

文件	是否必需	说明
manifest.json	必需	队伍标识、schema 版本和生成时间等提交元信息。
evidence.csv	必需	攻击证据列表；字段要求见选手手册与 submission_schema.md。
timeline.csv	必需	攻击时间线；字段要求见选手手册与 submission_schema.md。

文件	是否必需	说明
attack_graph.json	必需	攻击路径图谱，顶层包含 schema_version、incident_id、nodes 和 edges。
ioc.csv	必需	IOC 集合，包含 IP、域名、文件、账号、token 等指标。
graph_nodes.csv / graph_edges.csv	可选	用于辅助生成 attack_graph.json；平台最终以 attack_graph.json 为准。

平台只读取固定核心文件，并按照字段枚举、引用关系和标准答案进行客观计算。

正式提交前，建议队伍使用数据包内 tools/validator.py 对提交目录进行本地校验，确认文件完整、JSON/CSV 可解析、event_id 与 evidence_id 引用关系正确。

四、评分规则

Build 环节总分 100 分，全部为客观自动评分，不设置人工主观分。评分项如下：

评分项	分值	评分说明
-----	----	------

评分项	分值	评分说明
格式合规	10	严格检查文件、schema、枚举、时间、唯一性和引用关系；任一错误使本次提交无效，总分为 0。
证据发现	25	按 event_id 命中情况计算 precision、recall 和 F1。
攻击阶段分类	10	检查命中关键证据的 stage 是否正确。
时间线还原	15	保序一对一匹配；必需证据 70%、stage 15%、起止时间各 7.5%。
拓扑节点	10	规范化实体集合按 precision、recall 和 F1 评分。
拓扑边关系	20	from/to 40%、action 15%、stage 15%、时间 10%、必需证据 20%，再计算质量 F1。
IOC 提取	10	type/value F1 占 7 分，时间、关联资产和证据元数据占 3 分。

为避免通过堆叠可疑事件刷分，证据发现和图谱关系评分均强调准确率与召回率的平衡。选手应提交经过分析确认的攻击证据，而不是提交全部可疑日志。PCAP 和 Windows Event XML 中的 artifact event_id 与普通日志 event_id 使用同一套评分口径。

五、操作指南

5.1 平台登录

比赛平台开放后，选手使用规定方式登录。首次进入 Build 环节页面后，应核对队伍信息和队伍 token。

5.2 下载赛题数据包

进入 Build 环节页面后下载选手数据包，优先阅读 README.md、docs/player_manual.md、docs/submission_schema.md 和 docs/sample_submission/。

5.3 本地分析与校验

先阅读 env/ 下的资产、账号、网段和服务关系，建立企业环境上下文。结合 logs/ 和 artifacts/ 进行多源关联分析，将确认的证据写入 evidence.csv。

根据证据构建 timeline.csv、attack_graph.json 和 ioc.csv。

使用 tools/validator.py 进行本地格式校验。validator 仅代表格式和引用关系通过，不代表最终得分。

5.4 上传文件

点击平台上传入口，选择 submission.zip 并提交。单个 zip 最大 30MB，解压后最大 80MB。

5.5 查看结果

平台完成自动解包、校验和评分后，显示本次提交结果。每队最多 3 次上传机会，最终取最高分进入 Build 环节排行榜。

六、注意事项

参赛团队须独立完成全部分析、构建与提交内容，严禁复制、抄袭或交换其他队伍成果。

选手不得攻击、干扰比赛平台或其他队伍环境，不得提交恶意文件或比赛任务无关的内容。

提交文件应遵守主办方给出的固定格式。文件缺失、字段错误、引用不存在或压缩包目录层级错误会使本次提交无效并计为一次上传。

比赛过程中如遇平台访问、数据包下载、提交失败等问题，请通过竞赛官方沟通渠道联系工作人员，并保留必要的错误截图和提交时间信息。

本 Build 环节相关规则及未尽事宜，最终解释权归第十九届全国大学生信息安全竞赛创新实践能力赛竞赛组委会所有。

第十九届全国大学生信息安全竞赛
——创新实践能力赛竞赛组委会
(齐鲁工业大学网络空间安全学院代章)

2026 年 8 月 12 日

附：第十九届全国大学生信息安全竞赛创新实践能力赛决赛
队伍名单

序	队伍名称	学校名称	所属赛
1	Lilac	哈尔滨工业大学	辽宁赛
2	天枢 Dubhe	北京邮电大学	辽宁赛
3	Opsu3	中国人民公安大学	辽宁赛
4	Calil	哈尔滨工业大学	辽宁赛
5	redbud	清华大学	辽宁赛
6	Opsu3	中国人民公安大学	辽宁赛
7	圣地亚哥皮蛋	山东警察学院	辽宁赛
8	Spirit-Grad	吉林大学	辽宁赛
9	Rrwebb	大连民族大学	辽宁赛
10	HASHTeam	山东大学	辽宁赛
11	老谭酸菜面	中国科学院大学	辽宁赛
12	BlueWhale	中国海洋大学	辽宁赛
13	TimeKeeper	山东科技大学	辽宁赛
14	AAA	浙江大学	浙江赛
15	Ph0t1n1a	上海交通大学	浙江赛
16	0x3B	宁波工程学院	浙江赛
17	Sn0w	南京理工大学	浙江赛
18	ORAYS	杭州电子科技大学	浙江赛
19	一剑霜寒十四州！	浙江警察学院	浙江赛
20	白泽	复旦大学	浙江赛
21	EDI-NU1315-1	合肥师范学院	浙江赛
22	不管了直接加钠	安徽师范大学	浙江赛
23	Alnatas	浙江师范大学	浙江赛
24	雨蓝	上海公安学院	浙江赛
25	农奴	宁波城市职业技术学院	浙江赛
26	SimpleGipsy	杭州师范大学	浙江赛
27	0x04	温州商学院	浙江赛

28	hnnutech	淮南师范学院	浙江赛
29	tluSec	铜陵学院	浙江赛
30	crychic	上海交通大学	浙江赛
31	cha0s	郑州轻工业大学	湖北赛
32	SSSec007	郑州大学	湖北赛
33	SeeU-Sec	中国人民警察大学	湖北赛
34	Fotsec	安阳工学院	湖北赛
35	彩虹七号	郑州警察学院	湖北赛
36	NYSEC	南阳理工学院	湖北赛
37	All1n	武汉大学	湖北赛
38	witctf	武汉工程大学	湖北赛
39	babyL3H	华中科技大学	湖北赛
40	NEUQRO	东北大学秦皇岛分校	湖北赛
41	云帆 NSN	河北大学	湖北赛
42	CTF_Forerver	华中科技大学	湖北赛
43	sssec777	郑州大学	湖北赛
44	TorchWood	江西警察学院	广东赛
45	烽火戏诸侯	南昌大学	广东赛
46	广外女生	广东外语外贸大学	广东赛
47	火炬木	江西警察学院	广东赛
48	风信子	江西师范大学	广东赛
49	BinX	广州大学	广东赛
50	WYE	五邑大学	广东赛
51	Become	广东轻工职业技术大	广东赛
52	广外幽灵	广东外语外贸大学	广东赛
53	我搞丢了可乐和鸡排	暨南大学	广东赛
54	NISA-325Spark	福建师范大学	广东赛
55	Xp0int	暨南大学	广东赛
56	SumY2i3	国防科技大学	重庆赛
57	0x401	四川大学	重庆赛

58	NSTL	电子科技大学	重庆赛
59	网安笑传之长城杯	国防科技大学	重庆赛
60	Xu7e45	重庆电子科技职业大	重庆赛
61	Dino	成都理工大学	重庆赛
62	LVV	湖南警察学院	重庆赛
63	AegisForce	四川文理学院	重庆赛
64	0xFA	重庆邮电大学	重庆赛
65	Dlno	成都理工大学	重庆赛
66	Flyteam	西南民族大学	重庆赛
67	挂科不可耻，ctf0 解遗臭万	贵州大学	重庆赛
68	莫问	西安理工大学	陕西赛
69	N05ecUltra	兰州大学	陕西赛
70	N05ecMax	兰州大学	陕西赛
71	XJUSEC-只是回忆上了发条	新疆大学	陕西赛
72	F14GThi3f	西安邮电大学	陕西赛
73	L_2026	西安电子科技大学	陕西赛
74	NWU0SEC	西北大学	陕西赛
75	Starfall Koi	西安电子科技大学	陕西赛
76	JK	西北工业大学	陕西赛
77	Taru1	塔里木大学	陕西赛
78	甲壳虫安全团队	新疆财经大学	陕西赛
79	我想把回忆拼好给你--终章	新疆大学	陕西赛
80	k410ng	兰州理工大学	陕西赛