圣博润
SBR-info

LanSecS®网络安全事件调查处置工具箱

调查工作专业化　调查分析智能化　调查处置规范化

北京圣博润高新技术股份有限公司

SBR-info

LanSecS® 网络安全事件调查处置工具箱

产品概述

LanSecS ®网络安全事件调查处置工具箱（以下简称：调查处置工具箱），是专门针对网络安全事件调查处置工作设计开发的一套专业设备，该设备可实现调查工作专业化、调查分析智能化、调查处置规范化。

该产品依据网络安全事件调查处置国家标准规范设计开发，融入了圣博润公司多年来在安全领域积累的咨询服务经验和安全工具开发经验。产品将现场处置访谈、攻击日志采集、安全事件回溯、处置报告自动生成进行有机结合，实现网络安全事件调查处置工作从任务部署、调查执行、结果分析和报告处理的闭环管理，协助调查处置人员快速完成网络安全事件的定性分析、过程取证以及事件回溯，并给出详细的调查处置报告。在完全满足公安机关、政府部门、企事业单位网络安全事件处置工作的同时，提升了网络安全事件处置的专业性和有效性、提高了工作效率和工作质量。

产品功能

调查处置工具箱由管理系统和采集分析工具组成：

管理系统：包括任务管理、文件管理、知识库管理、系统管理四个模块。其中任务管理实现了制定采集任务、生成采集U盘、现场数据采集、采集数据分析、攻击事件回溯、生成调查报告六步处置过程管理。

采集分析工具：包括主机资产采集分析工具、系统信息采集分析工具 、WEB信息采集分析工具 、日志信息采集分析工具 、内核安全采集分析工具 、网站开发框架采集分析工具六个工具。

黑客对网站进行扫描,发现漏洞进行入侵

功能描述

任务管理

☒ 制定调查任务：登记网络安全事件基本信息，并将处置任务分配给具体处置人。

☒ 生成采集U盘：依据任务信息，按照安全事件处置要求生成采集U盘。

☒ 现场数据采集：通过访谈采集事件基础信息，使用采集工具获取相关日志信息。

☒ 采集数据分析：依据访谈及采集数据，对主机层、网络层、应用层、管理层进行深度数据分析。

☒ 攻击事件回溯：包括扫描网站、发现漏洞、发起攻击、入侵主机、高危后果五个过程进行回溯。

文件管理

包括WEB日志、现场访谈提交附件、WEB文件、数据库日志、系统日志、系统痕迹、资产信息七类信息，一方面将这些原始的信息作为调查处置证据进行存档，另一方面将这些原始信息上传到网络安全事件调查处置管理平台进行智能关联分析。

知识库管理

☒ 漏洞库：包括操作系统、WEB中间件、数据库、开发框架等漏洞情况，并提供漏洞危害级别。

☒ 恶意代码样本库：包括事件处置过程中采集的恶意代码样本，并提供危害描述和处理建议。

☒ 安全事件处置库：提供安全事件处置的规范和标准，并提供安全事件产生原因和处置方法建议。

调查处置工具集

工具名称	主要功能
主机资产采集分析工具	对主机操作系统、硬盘、内存、CPU、应用软件、系统补丁、服务、进程等信息进行采集分析。
系统信息采集分析工具	对信息系统的联网痕迹、USB 使用情况、文件操作痕迹、系统基线安全等信息进行采集分析。
WEB 信息采集分析工具	对 WEB 文件、 WEB 日志进行采集，支持 WINDOWS 和 LINUX 操作系统。
日志信息采集分析工具	对操作系统的系统日志、安全日志、应用程序日志、数据库日志等进行采集分析。
内核安全采集分析工具	对 WINDOWS 系统内核信息、内核钩子、应用层钩子、驱动模块、网络、启动项等进行采集分析。
网站开发框架采集分析工具	对网站所用的开发语言、平台、中间件、服务器类型、远程运维等信息进行采集分析。

网安民警前往事发现场进行调查

产品规格

网络安全事件调查处置工具箱		网络安全事件调查处置管理平台		
产品组成	LS-INV-2000	产品组成	LS-INM-基础版	LS-INM-增强版
调查处置工具箱管理系统	✔	通知公告管理	N/A	✔
主机资产采集分析工具	✔	事件登记发布管理	✔	✔
系统信息采集分析工具	✔	调查结果管理	✔	✔
WEB信息采集分析工具	✔	结论报告管理	✔	✔
日志信息采集分析工具	✔	事件归档管理	✔	✔
WEB攻击采集分析工具	✔	综合查询	N/A	✔
内核安全采集分析工具	✔	统计分析	N/A	✔
网站开发框架采集分析工具	✔	知识库管理	N/A	✔
加固式三防本	✔	系统管理	✔	✔

网安民警形成安全事件调查处置报告

产品价值

★ **调查处置规范化**：产品按照网络安全事件调查处置规范设计开发，实现了网络安全事件调查处置工作从任务部署、调查执行、结果分析和报告处理的闭环管理，提升了工作标准化和规范化。

★ **调查工作自动化**：调查处置工具箱提供数据采集分析工具自动采集日志信息，提供分析引擎自动分析事件攻击过程，提供报表生成工具一键生成调查处置报告。通过自动化工具使得调查处置工作质量不再依赖处置人员业务能力和处置经验，从而提高调查处置工作效率和质量。

★ **调查分析专业化**：调查处置工具箱内置数据分析引擎，将采集的数据进行关联性分析，自动进行攻击事件回溯，解析事件发生的重要痕迹、成因，辨析攻击者IP、攻击手法、攻击轨迹，提取关联证据，还原安全事件发生的始末，自动生成网络安全事件分析报告，并提供调查处置结论报告、限期整改通知书等工作文档。

★ **大数据分析智能化**：调查处置工具箱数据可以导入网络安全事件调查处置管理平台，通过大数据分析技术，能够预知、预判网络安全事件的发展和爆发趋势，及时进行通报预警。并且可以作为“重要信息系统基础数据库管理系统”和“网络安全态势感知与通报预警平台”的数据来源，提供精准的网络安全事件数据。

为用户解决的问题

★ 解决了网络安全事件调查处置工作抓手问题

★ 解决了调查处置工具一体化、标准化问题

★ 解决了调查处置报告自动化、科学化问题

★ 解决了调查处置工作效率提升问题

★ 解决了安全事件大数据分析问题

★ 解决了威胁情报和态势感知数据源问题

北京圣博润高新技术股份有限公司

办公地址：北京市海淀区高梁桥斜街长河湾大厦2号楼3层 邮编：100044

咨询热线：400-966-2332

电　话：8610-82138088

传　真：8610-82137982

邮　箱：Support@sbr-info.com

公司网址：www.sbr-info.com

公司简介

北京圣博润高新技术股份有限公司2000年成立于中关村科技园区，目前公司人数近300人。总公司设在北京，在华东、华南设有分公司，在中国29个重要城市设有办事机构，拥有北京和南京两个研发中心，研发和技术团队人数占员工总数64%，产品用户超过10000家。

圣博润旗下拥有完全自主知识产权的内控管理 、安全防护、安全管理、工控安全、云计算安全、大数据安全、移动安全多个产品系列，同时拥有专业的信息安全服务团队，提供信息安全咨询服务和培训服务。