

安恒 AICSO 网络防御运营管理平台

V2.32

用户使用手册

文档版本: 2.32

发布日期: 2022-03-29



www.dbappsecurity.com.cn



本文中出现的任何文字描述、文字格式、插图、照片、方法等内容,除另有特别注明,版权均属杭州安恒 信息技术股份有限公司(简称"安恒信息")所有,受到有关产权及版权法保护。任何个人、机构未经安恒 信息的书面授权许可,不得以任何方式复制或引用本文的任何片段。

经授权使用本文中内容的单位或个人,应在授权范围内使用,并注明"来源:安恒信息"。违反上述声明者, 安恒信息保留追究其法律责任的权利。

除杭州安恒信息技术股份有限公司的商标外,本手册中出现的其他商标、产品标识及商品名称,由各自权 利人拥有。



文档说明

产品名称		AiCSO 网	络防御运营管理平台
适用平台	/版本	V2.32.0 集	欠件版本
拟制人	AH9997 (安全运营部-杭州安全运营 部)	评审组	AH9997 (安全运营部-杭州安全运营部)
发布人	AH9997 (安全运营部-杭州安全运营 部)	备注	受控文档

修订记录

日期	修订版本	修改记录	修改人
2022-01-18	2.28	初次发布	AH9997 (安全运营 部-杭州安全运营 部)
2022-02-14	2.28	扫描类工作流新增定时功能;原 更改责任人改为更改处理人;渗 透类、通告类流程新增资产责任 人筛选	AH9997 (安全运营 部-杭州安全运营 部)
2022-02-23	2.29	版本更新	AH9997 (安全运营 部-杭州安全运营

杭州安恒信息技术股份有限公司



			部)
2022-03-07	2.30	工作流新增资产退网和资产变更 优化业务准入工作流	AH9997 (安全运营 部-杭州安全运营 部)
2022-03-14	2.31	启动台一级菜单文字修改;工作 流新增资产风险自查工作流	AH9997 (安全运营 部-杭州安全运营 部)
2022-03-29	2.32	开启管理员和 opdmin 对工作流的 编辑权限	AH9997 (安全运营 部-杭州安全运营部



|--|

1	产品概述	1
2	WEB 概述	2
	2.1 功能简介	2
	2.2 WEB 登录	2
	2.3 退出 WEB 登录	3
	2.4 WEB 页面布局	3
3	AICSO 网络防御运营管理平台	5
	3.1 权限控制	5
	3.1.1 superadmin	5
	3.1.2 useradmin	5
	3.1.3 opadmin	6
	3.1.4 generaluser	6
	3.1.5 auditadmin	7
	3.2 账户详情	7
	3.2.1 修改账户详情	8
	3.2.2 修改密码	9
	3.3 设置	9
	3.4 身份认证管理1	0



3.4.1	角色管理	10
3.4.2	用户管理	11
3.4.3	跳转链接配置	15
3.5 编辑	辑工作流	
3.5.1	工作流列表	
3.5.2	新建工作流	
3.5.3	编辑工作流	19
3.5.4	删除工作流	19
3.6 配置	置启动台	
3.6.1	功能简介	
3.6.2	新增子平台	
3.6.3	编辑子平台	
3.6.4	删除子平台	22
3.6.5	新增彩虹标签	22
3.7 配置	置管理	
3.8 角色	色管理	
3.9 审议	计日志	



	3.10 授权信息	25
	3.11 待办任务	25
4	工作流	28
	4.1 扫描类工作流	28
	4.1.1 新增扫描任务	28
	4.1.2 解析方式确认	28
	4.1.3 资产确认	33
	4.1.4 责任人处置	34
	4.1.5 项目经理评审	35
	4.1.6 结果查看	36
	4.2 渗透类流程	37
	4.2.1 添加计划	37
	4.2.2 选择资产	38
	4.2.3 导入漏洞	38
	4.2.4 资产确定	39
	4.2.5 责任人处置	40
	4.2.6 项目经理评审	40



4.2	2.7 结果查看	41
4.3	通告类流程	. 42
4.3	3.1 添加计划	. 42
4.3	3.2 选择资产	. 43
4.3	3.3 上传外部文件	43
4.3	3.4 责任人指定	. 44
4.3	3.5 责任人处置	. 44
4.4	云 EDR 告警工作流	. 45
4.5	港中旅工作流	. 49
4.5	5.1 敏感信息发现与排查	. 49
4.5	5.2 互联网资产发现与管理	. 52
4.5	5.3 钓鱼邮件测试	54
4.5	5.4 安全应急演练	56
4.5	5.5 玄武盾监测告警分析与处置	. 58
4.6 5	安全运维工作流	. 59
4.0	5.1 安全设备及平台巡检	. 59
4.6	5.2 安全设备及平台维护记录	61

杭州安恒信息技术股份有限公司



	4.6.3 安全设备及平台策略调优	62
	4.6.4 安全设备基础信息收集	63
	4.6.5 安全设备及平台故障报告	64
	4.6.6 安全工作报备	65
4.	7 周期计划	69
	4.7.1 安全告警监控数据录入工作流	69
4.	8 情报转事件工作流	70
	4.8.1 AiLPHA 告警转事件	74
	4.8.2 EDR 告警转事件工作流	75
	4.8.3 新系统上线评估	76
4.	9 安全服务工作流	84
	4.9.1 渗透测试服务	84
	4.9.2 WEB 漏洞扫描服务	85
	4.9.3 主机漏洞扫描服务	86
	4.9.4 基线核查扫描服务	87
	4.9.5 弱口令扫描服务	88
	4.9.6 新系统上线安全评估服务	89

杭州安恒信息技术股份有限公司



4.10 运营成熟度工作流
4.10.1 运营雷达评估91
4.10.2 运营风险趋势92
4.11 资产管理工作流
4.11.1 资产业务准入
4.11.2 资产变更报备工作流
4.11.3 资产退网工作流



1 产品概述

AICSO 网络防御运营管理平台是一款为政企单位、行业用户提供安全服务运营分析与协作管理服务的 产品,用户可以在平台上进行身份认证管理、配置工作流、配置启动台、配置管理等操作,通过该平台直 接免登陆跳转到各个模块。



2 WEB 概述

2.1 功能简介

用户可以通过 Web 界面对 AICSO 网络防御运营管理平台进行配置和维护。

2.2 WEB 登录

以 Google Chrome 浏览器为例, 在浏览器中输入 https://aicso.dbappsecurity.com.cn/网络防御运营管理平

台链接,进入登录窗口。



平台支持钉钉扫描二维码登录,也可以输入手机号获取验证码登录。在扫码登录页点击右上角电脑图标按钮,输入手机号和验证码后获取短信验证码输入,点击<登录>后,进入网络防御运营管理平台。



2.3 退出 WEB 登录

在 OS 启动页面右上角,单击用户,点击<退出>,退出 WEB 登录。



2.4 WEB 页面布局

WEB 页面布局共分为:顶部彩虹导航栏,核心功能区,设置和待办任务。

核心功能为安全防护、暴露面检测、数字驾驶舱、运营管理、威胁狩猎、应急响应。





杭州安恒信息技术股份有限公司



3 AICSO 网络防御运营管理平台

安全运营平台 OS 启动页可以配置相关的平台链接,点击跳转到相应的平台。

3.1 权限控制

平台设置 superadmin、useradmin、opadmin、auditadmin、generaluser 一共 5 种角色,可以根据需要在 "角色管理"里对上述 5 种角色进行再修改。

3.1.1 superadmin

Superadmin(超级管理)拥有所有权限,包含身份认证管理、编辑工作流、角色管理、配置启动台、 配置管理、审计日志、授权信息等。



3.1.2 useradmin

Useradmin (用户管理) 只能管理用户, 权限包含身份认证管理、查看工作流、查看授权信息等。

杭州安恒信息技术股份有限公司



3.1.3 opadmin

Opadmin (运维管理) 管理平台运行配置, 权限包含编辑工作流、配置启动台、角色管理、配置管理、 审计日志和授权信息等。



3.1.4 generaluser

Generaluser (普通用户) 只有用户权限, 包含查看菜单、查看工作流和查看授权信息。

杭州安恒信息技术股份有限公司



3.1.5 auditadmin

auditadmin (审计管理员)



3.2 账户详情

在安全运营中心页面的右上角单击<用户>按钮有"账户详情"、"退出登录"的功能,点击下拉的<

杭州安恒信息技术股份有限公司





账户详情>按钮,页面跳转至 KEYCLOAK -编辑账户。

3.2.1 修改账户详情

页面跳转至 KEYCLOAK -编辑账户,可进行用户手机号、电子邮箱、姓名等信息的修改,点击<保存>, 成功修改。

OREACTOVIC		⇒32864 v - 1018
能户	编辑账户	*cm2
EH.	 第三条 Transistion 第44号 * Transistion 第44号 * Internation 第44号 * International Control 第44号 第4日 * International Control 第44日 * International Contro 第44日 * International Control 第44	
	803 (AF) 6 * 10 (AF)	
		80.M 66.07



3.2.2 修改密码

页面跳转至 KEYCLOAK -编辑账户,点击<密码>,可输入新密码和确认密码,点击<保存>,成功修改。

() KEYCLOAK		97.7368 × 1916
872	更改密码	INTERNAL DESIGNATION
EH	300 Second Control of	

3.3 设置

点击右上角<设置>按钮有"身份认证管理"、"编辑工作流"、"配置启动台"、"配置管理"、"授权信息"、"角色管理"的功能,分别可以进入 Keycloak 身份认证管理平台、工作流列表、启动台页面、配置管理页面、授权信息页面、角色管理页面。



3.4 身份认证管理

keycloak 身份认证管理,用来管理系统用户、模块跳转链接配置管理。Superadmin 权限的用户可以直接点击 OS 启动页的 "身份认证管理" 跳转到 keycloak 管理页面。或者访问 https://ip/auth/admin,使用 admin/Cq9ayCyt50elI@ub 登录

3.4.1 角色管理

登录身份认证管理系统后,点击左侧的<角色>,可以看到当前系统中设置的角色列表。

		Bernith SUURS				
		##- Q				8488
	N/H	8548	Compatito	84	80	,
	RP-RMS	automation in the second se	8	#1983, 3807265433	88	80
-	ABL .	the back of which doesn		Revie default roles annue	10	
	A CONTRACTOR OF	provident	8	225*	98	814
	a contraction of the second se	offere, allocat		form attine event)		
	NPM II	104810		ATTRA, 280798240, AROLD, DIEFE	80	80
	WAR .	same about		REPRA ARNYWEING AREAS, STRE. BUILDY		
		smit, Automotion	8	Scott, and automatical	910	818
		restation		APERA IRAPAGAI		
	₩					
	ALC: N					
	00					
	-					
	ateli.					
	677					
	86					

杭州安恒信息技术股份有限公司

安恒信



点击添加角色,输入角色名称、描述后,点击<保存>,添加角色成功。

添加角色后,需要登录网络防御运营管理平台后, superadmin 或者 opadminer 登录后,点击右上角的 <角色管理>,给该角色设置访问权限。

A ⁸ CSO 安全	运营平台	1 Advan -
Alcas -	88 - 8285	
Acco -	*** · #### 添加角色 *#88## ##	

3.4.2 用户管理

登录身份认证管理系统后,点击左侧的<用户>,可以看到当前系统中设置的用户列表。

	111							
	#18.							
II WEEK	18	Q 28168/*					810.07*	84.87
U. SPR	0	80.4	97419	85	47	80		
A 87485	Intibute tead-mut-fee.	the second se				418	400	80
E 44	TRATELIN- 2015-040-011-	-					-000	801
- BORRE	Distant's Alle Address	Conception of the local division of the loca				974	100	810
	LEADERS AND AND ADDRESS AND ADDRESS ADDRES ADDRESS ADDRESS ADD					414	40	414
E WARN	#24940 c)(%498.885.	a second				418	80	88
# 0.0	1012001-4009-424-521	1000				44	831	818
	COMPANY CONTRACTOR	-				578		404
6 K 2 MP								
- 10 C								
H 40.								

杭州安恒信息技术股份有限公司



3.4.2.1 添加用户

点击右上角<添加用户>,出现以下添加用户页面,在"用户名"处输入手机号,点击<保存>,创建用 户成功。

ACSU \$	王运营平台		4 Advin
Akso	8º · 325*		
	添加用户		
il ment			
4 BPB	197		
de Armain	ars.		
= **	0.7470		
= m/wn	2.9		
- VII	RA		
	用"已在有 0		
5 8	9749453	1.A.	
I MP	4804745	uten .	
0.88		88-7	
D BR			

3.4.2.2 用户属性

在属性 tab 页面中输入以下字段信息,添加后点击<保存>。

Key: fullname, value: 用户姓名

Key: phone, value: 手机号



A∜CSO ₿	2全运营平台		£ 8,000
Noter Elle			
 < 874 ∆ 87448 < 55 < 55 	Key Galanne phore	Value Bill 198000000	85 53 53
- uz - uz - t			
4 M/ 0 D2 2 FA			
15 9 91			

3.4.2.3 用户凭据

在"凭据" tab 页面设置用户密码。输入"密码"、"密码确认",点击<设置密码>,用户密码设置成功。

密码限制: 8~16个字符, 需包含大小写字母、数字和特殊字符 (@.*=_!?)。

A & CSO 安全;	运营平台				4 Atro -
Actas -	19900000000 @ 1980 Rrs. 15.85 199255.85	8243 K 73	1 10.8		
- Brand - Aritha - Aritha - UE - UE	(1) (2) (注意) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	Terr	8/162	*	**



3.4.2.4 密码策略

在验证 - 密码策略中,可设置进行密码的限制条件,点击<添加策略>,选定策略后,策略列表内该策 略对应消失。

添加策略后,可在"策略值"内设置相应限制条件。点击<保存>,密码策略设置完成。

A表CSO 安全运行	曹平台		à commune -
	- 松田		
40 4 minute 4	NA NE clin inne Desi Desi Milian Ni ini	Internet (Construction)	## ## ## ## ## ## ## ## ## ##

3.4.2.5 角色映射

在"角色映射"页面设置用户所属的权限组。权限控制参考 3.1 权限控制。

在"可用角色"列表选中角色权限,点击<添加选择>;在"分配的角色"列表内选中角色权限,点击 <删除所选项>。

	. 180000800				
2	1990000000 🖷	C)			
I WEAR	26 Rt 28	80HH 15 HIE	22		
0.878	hunda.	NEMO	187.65 ×		
to Ministratio		aud/tadmin	generalizer	presentation .	
e na		(operadros)	one adversarios	one, address pre-	
animite =		(original and the			
a mirinda		89684	1.000000000		
÷ 948	87588.0	3.001118.			
6) A.P.					
5 80 5 80 5 80					
5 MP 0 88 2 94 2 95					
a mp più a m a m a m a m a m a					

3.4.3 跳转链接配置

Aicso-左侧配置中选择"客户端",选择"aicso",点击进入。

	22340					* Adver
isa 👘	客户铺					
	GREE					
	dir. Q.					
😌 8/H	878.0	He	#101.	1817		
A WOMEN	attant		http://it.tt.42.4.au/t/hat-scattaracter/it	416	. 8.8.	
	ACCOUNTS OF A		Nepp 112 22 42 Annual Annual Statement	818	83	800
	advisor.		822	82	81	
			883	8.8	88	800
E NEWE	broke		823	81	80	
6 W.C.	Carry of Landson Day, Samuel		F21	818	81	800
	rame nursparted	.#	821	8.8	81	200
	revumbliknige		883	8.6	88.	818
	terrority adverse contains		March 111 11 42 4 to Water and Sciences	84	81	
1.00						
1.95						
22 単出						

进入"客户端"用户详情,页面跳转至"设置"tab页,在"有效的重定向URI"和"Web起源"中输入配置的url信息。

在正常安装部署情况下:

(1) 有效的重定向 URI 需要添加:



- https://{ip}/*
- https://{ip}:5443/*
- https://{ip}:6443/*
- https://{ip}:7443/*
- https://{ip}:40008/*
- (2) 管理员网址需要添加: https://{ip}

(3) Web 起源需要添加:

- https://{ip}
- https://{ip}:5443
- https://{ip}:6443
- https://{ip}:7443
- https://{ip}:40008

(4) 其他情况:

- 如果需要添加其他第三方平台,也需要在有效的重定向 URI、Web 起源添加地址:https://{ip}/*
- 有效的重定向 URI: https://{ip}/*
- Web 起源: https://{ip}

A ⁸ CSO 安全运营平台		1 Adres =
Acia 🕞 👘		
Aicso 🗑		
U BEAR	and within yoke the 240 minute and	
C 1/10 1/100	400	
A BURRE		
12 45		
= 80804 MAO		1
2 APRA 86		
	177 m	
HEAR C	11 A	
22 24580	2011	
A 10	sandornat	
(* 197		
C PR SHADE	Page (A	
2 8A DAMAGE	10 C	
St. 45.		
17 Mat		
自用重要达用提供 G		
10.0L0		
	(CONTRACTOR) IS	
* HIMESHAND	MagArid SEAT A MIR	
	Handrich Baldatt	
	Rept. V13.10.42.4.40000/*	
	ing:/localioa/4	
	mps//1156-042404*	
	W(01.1/1336.42.45443**	
	Http://15.56.42.3/4	
	addenvieren 2006 auge -	
	1	
€us.o		
111101 (TELEVILLE)	Way / Nacifrian	1
the second s	anne chaile ar a feala.	
weathe	Web.213.26.7 M.244	
	Http://decalition	
	Peppi,P13.06.42.4	
	M3p4.073.08.43.4.8443	
	https://10.36.41.4.40038 -	
	W104/713324245663	
	W(0.070.0.4C3	
Contraction of the Contraction	1997	
Fine Grain OpenID	連接配置 (2)	
→ OpeniD 進接兼容得	式0	
* 高級设置 の		
>身份验证完理意 @		
	8.7 8.8	

杭州安恒信息技术股份有限公司

了安恒信息



3.5 编辑工作流

3.5.1 工作流列表

工作流列表包括序号、工作流名称、KEY、部署时间和操作列下的查看、编辑、删除。

工作流列表的工作流名称取新建工作流时用户自定义的工作流名称, KEY 取用户导入的.bpmn 文件内的 ID。

INAM	8				8.0	8.8
	Image	REY	10010		3819	
13	according to the second se	14,0,011	1021-00 m m (1m)	-	-	-
1	(au)189	545,5,110	and the second		-	-
3	Tourseast,	0.01/1.021	1010 - An-An (10 - 15 - 15 - 15 - 15 - 15 - 15 - 15 -		85 1	-
	wint	Provinsi, turksta P	2021 Jan 36 11 107 21		ste :	-
4	000x.9.001830611698	19CM_0.013	and on an inclusion of the	-	506 F	-
	1000013 \$1000000	1404_0_011	aran kinak kinak ar		-	-
17 - C.F.	1909, JL (0.2 web/#019) #	HOLD, HO	ana i de an renación		102 1	ee i
	INCOLUTION 2 STATERING	10144, 8, 10, 2	and an according		-	-

3.5.2 新建工作流

点击<新建>,页面跳转至新建工作流。

输入工作流名称,点击<导入>,选择.bpmn文件上传,点击<确定>。

当 KEY 唯一时, 点击<部署>, 新建工作流成功。

当 KEY 已存在时,点击<部署>,提示失败。

	1070	2245	-	Chine	RATER	17240	0.007 B
#18271X	87748				1		
		0.11094937		LLR-128			
	_	_			-		

3.5.3 编辑工作流

点击<编辑>,页面跳转至编辑工作流。

输入更改工作流名称,点击<导入>,导入更改后的 KEY 相同的工作流文件,点击<部署>,工作流编 辑成功。



3.5.4 删除工作流

点击<删除>,二次提示删除工作流会影响进行中的任务,若删除,则任务被挂起。

杭州安恒信息技术股份有限公司

C50 👳	黄杨尔曾理平白	63-60 AB778	#±89	847229	112	50	0.104	1
工作原则	N				в	R 45		
.00	1/488#	NEV.	2811		1615			
	STORE BORD	49,0,021	2025-08-0130-24-08		-	-		
4	candil Bith	SRLC, H 8	2021 AN 10 10 10 10 21	e saria	1.141	LEEGG#UR	Ran Int	17
3	Internet	1604,0,002	2021-08-09 19 19 22	-	104	201		
2	india.	0 ⁰⁰ aannoo_tipiig765 0	2010/08/07 07 07 25		572	***		
	9004,5,003 868913668	100M_B_012	2011/08/01 00:42:44	-	-	-		
	action (whith the g	lacai a di 2	2010/02/11/06/25		576	-		
19	000.0.0 (wei#100#	linear a card	2021-07-01-0108-08		-	-		
	ACM & NO TRUNCK	1000 0 000			-	-		

3.6 配置启动台

3.6.1 功能简介

配置启动台的主要功能是对子平台进行新增、编辑和删除,实现对启动台子平台的自由配置。方便用 户根据自己的需求增加平台,利于集中管理。

3.6.2 新增子平台

点击父级模块的名称,上方显示"新增子平台",输入平台名称和域名地址,选择<是否开启>,默认< 新开页面>按钮打开,点击<保存>,新增子平台成功。

上方导航栏新增该子平台,返回启动页,父级模块出现新增的子平台。

安恒信

ACR 2017 11				41	
- anna	* ##77b				
######################################	(2600)				
2/2810	(ming.)				
#1/##### #1/7#F#	140.000				
dare to	-8556	N.			
INTER-COM					
eduttere	-				
**************************************	Part of the local division of the local divi	**			
 setartile 					
• (Ridetti)					
· 2017-0000					

3.6.3 编辑子平台

点击子平台的名称,上方显示编辑子平台,显示历史的平台名称和域名地址,根据需求修改平台名称 和域名地址,选择是否开启,点击<保存>。

若编辑了名称菜单中该子平台的名称就会改变。上方导航栏该子平台的名称也发生了变化。返回启动 页,父级模块下的该子平台的名称也发生变化,若修改了域名,则点击之后跳转的页面也会发生变化。编 辑页面如图所示。

AICSO IREE	879)		1942	50118	1117	807-1	61020	ii iin D
E.B.	常性							0
- P			##Y##					
	######################################	8	17444	******				
	101867-0		- 2019 1044	NUMBER OF THE OFFICE AND ADDRESS OF THE OWNER.	namiadrostas citado de			
	#5.070710E		- 942	(a) (b) (b) (b) (b)	F # # #			
	Tribate		. 8270	(CD)				
	entitetticie.		- 11/2.8	00				
÷	2308407*0 Http://			B(7 8.2				
1.00								
	North							



3.6.4 删除子平台

点击子平台右侧的<删除>按钮,跳出提示,点击<确定>,菜单中该子平台就会被删除。上方导航栏该 子平台也会被删除。返回启动页,父级模块下的该子平台也被删除了。

A*CSO inggigra	1799	unes.	410.004	9.4000	REAL	43-929	0 +++ B
新聞会かれ ・ (1985) ・ (1		100 / 100 		er er er		(4	a.)
1996-6122000 9426-51200 9426-51200 9426-51200 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 9426-5120 940-5120 940-5120 940-5120 940-5120 940-5120 940-5120 940-5120 940-5120 940-5120 940-5120 940-5120 940-5120 940-5120 940-5120 940-5120 940-5120 940-5120 940-5120 940-5120 940-5120 940-5100 940-5120 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-5100 940-51000 940-5000 940-5000 940-5000 940-5000 940-5000 940-5000 940-5000 940-5000 940-5000 940-5000 940-5000 940-5000 940-5000 940-5000 940-5000 940-5000 940-5000 940-5000 940-5000 940-5000 940-500000000000000000000000000000000000		- RETER () 				
			(17.5.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1	LA-18-2 (1)			

3.6.5 新增彩虹标签

配置子平台可以添加彩虹团队标签,添加完成后显示在启动台和导航栏的子平台菜单中。

	1000	2.940	5279	*107	842-1	11525	0.171 8
新聞 目特性							
 .0000 .00000 .0000000 .00000000 .00000000 .000000000 .000000000 .0000000000 .0000000000000 .000000000000000000000000000000000000	1.5	00027712 - 10-200 (001 - 002000 (001 - 002000 (001 - 002000 (001) - 002000 (001) - 002000 (001) - 00200	en regi res registrat at serie reginer. Ref (en) (en) (en)	PSilacedat Bit) (R), All A			



子平台配置完成后,进入 OS 启动台,鼠标移至上方导航栏,会显示彩虹团队的名称,同时下拉框内显示对应的子平台。



3.7 配置管理

配置管理中可以配置 logo、修改平台名称和修改水印。

A*CSO	-	and and a second second	10000	0400	100.000	DAD4	80105	17229	0.100 0
111000									1.000
	entre	É.						-	
	**				9N	whete		14.7	
	1	age of the second secon	Family 102010	2012/act/16/a/1110	Formation	102-21.0(1)	19624		
	1	10-101	*=170484	Pip .	1400	100000	yute	-	
	1		00R53700		1000	and which is	12.51	-	
	25	A stressed as	1000		SEA494	3829-30.01-21			
	5	4.500.500			#8934	2010/01/01	10.11	-	
		10.4134	147.0			1025-01-01	3424	-	
	Ť	or present	-		- CONTRACTOR	10-10-0	17.41	-	
	10	or parts	wga 116.2637.08	60.0	and pression	125 11 11 1	10.34	-	
	*	wijne - 171,1871	100pt (102) (102) (102)	2	equal prize	1021-27.3k m	07.60		
		-	eredation		unrest.	2025-06-02-08	in in	100	



3.8 角色管理

在角色管理页面,选中角色后,选择右侧的菜单权限,点击<保存>。

通过该设置功能,可以给不同的用户组设置不同的平台访问权限。

A 8 C 50 服用安全运营中心	10.00.00.00	现象的目	10000	20020	养猪营工用	10.10.1010101	0.164	8 .	Ð
-	opadmin						8.0		
- apachine - unerphysic	2.053								
(complete)					14	88 .	W		
gerentituse skultustren		2010年 第三元年期代報号台 第三元元第第号台 副政策第号台 副政策第号台 副政治(第三号台) 期間合「周辺集団号台 期号合 第三年号 第三年号 第三年号 第三年号 副市(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本台(第三年号) 日本(第三年号) 日本(第三年号) 日本(第三年号) 日本(第三年号) 日本(第三年号) 日本(第三年号) 日本(第三年号) 日本(第三年号) 日本(第三年号) 日本(第三年号) 日本(第三年号) 日本(第三年号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三号) 日本(第三) 日本(第三号) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日本(第三) 日(第三) 日本(第三) 日本(第三) 日(第三) 日本(第三) 日本(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第三) 日(第 (1) 日(第 (1) 日([] (1) (1) 日							

3.9 审计日志

可以查看安全运营中心,安全大数据分析模块,资产弱点管理模块的相关日志信息。

安全运营中心根据平台模块分为运营支撑系统、安全事件管理系统、安全服务管理系统、情报威胁运营系统,同时可以按照操作类型、操作人和时间范围对日志进行筛选、查询。

点击<导出全部>, 默认导出近6个月的日志文件,也可经过筛选后导出结果。

注:取用户名 keycloak 中属性的 fullname;大数据分析模块中 system 命名为系统账号;弱点模块 opadmin 命名为审计账号、openUser 命名为系统账号。

ASCSO	安全运营	防御管理学台	6001	1990	40.518	10 Kitor	80.00	$M = \mathcal{M}(M, \mathbb{R})$	0.000	
	电计算机							10.1		
		10/281542	S-807889							
	COMP U	12:00.00		BINE SHARES		BILA.	ingeningen anderen ander			
	6058									
								Mall I		
	.95	MOH4		MILA.	3847	16/45	ing .			
	8	212-05-04-06-05-05-05		annext A	10 39 87 288		-Was / 11 21 198 21 19	disang manan.		
	3	and the second s		ananna.	19/40.00 100	2.0	max 113 20 108 500			
	3	221024044		1004	10 20 11 281	3.0	Here 112 20 104 50 51	(Institution)		
	8	mpaintern or e	6	-1212	412111204	4.7	1004-11120-104-50F			
	1	2010/01/01/01		48.00	412.17.8.4	2.4				
	÷	217-10-04 10 21 21		1522	10.01 #1.221		Web 171 20 108 201			
	5	determination of		0.014	the state day		mperied by which he has	distance.		

3.10 授权信息

授权信息里可以更新授权证书,新安装平台或者证书到期后需要在此更新网络防御运营管理平台的

平台证书。授权后才能正常使用平台功能。superadmin、opadmin 可以对授权信息进行操作。



3.11 待办任务

点击右侧<待办任务>按钮,侧抽屉展示代办任务,还可以跳转到平台执行任务。

待办任务列表项可以查看工作流实例的节点数据,包含工作流名称、所属项目名称、任务类型、任 务开始时间等。



待办列表设置滑动分页,1页10条。



点击<工作流名称>, 弹窗展示工作流详情查看页。



点击<立即处理>按钮:

"安全服务"任务(状态为进行中)跳转至安全服务管理模块 - 工作台;

杭州安恒信息技术股份有限公司
AICS	o							A STRATE	0.000
O BENIER	19 ft	H1 - 37m							
		8425		1111118		2768		8301-6	
	-	371		367.00)	111	28	182.000	0
	1	and a second				1. And 1.		and an	
	-	10.0415							
NDE.		-	(then		YORE	Medicate R		**	
eterrite.		99000114		iá i		301111-0-021111-0		matrixin .	
196		BARTIN	4.00		ADD NAMES DOT	2011 (F-30-3021 (F-30		1.000	
-		10.0110	100		1279	101101-01-021-021-01		800,0.034	
-		-802104	840			3027-07-24-0027-07-07		12768	
	1	MM01129	400		0.110	2011-01-01-01-01-01		#1705.W-	
		#640779	A1112		10.0010	2011/01/01/01/01		14110101000000000	
		Mart11	A1110		10.8574	1011-01-01-0021-01-00		80.448	
		(Busility)	A010		+4.8919	305-01 m and an an		440-	0
		mailte	Acres		PERCENT	1011-01-00-0021-01-00		384-	0
		(Marrise)			HOMBOUR	380.010-80.0130		586*	

"安全事件"任务跳转至安全事件管理模块 - 事件列表 - 研判 / 处置。

A8CS0			h events	0.000
528418# 1 1	and inclusion of the			_
	Tester			_
with a	812.8			
91160	strate sweetcol	#H4 (17)		
enale -				
12041	Break and a second s	\$142 11\$ M		
	BARD	#**E21		
81078B	THE RELATES			
anoes.	68-00-001 - 011			
1.000	T. I DEPTHE PERSONNELLER.	THE PERSON NEEDED AND ADDRESS AND ADDRESS ADDR	Construction and an other states	
NUMBER OF				_
-				
-	81123			
	1. 20 Mr.			
-	and and the	The Avenue construction of the	~ .	
				-
		and and constant fragments in the		- 0

杭州安恒信息技术股份有限公司

🖲 安恒信息



4 工作流

4.1 扫描类工作流

扫描类工作流主要包括主机漏扫、web 漏扫、基线核查。



4.1.1 新增扫描任务

在安全服务管理模块的项目管理中,选择项目进入到项目详情。

点击<工作计划>,新增"主机漏扫"任务。

			通知社 55				× .			_
4869			12867		*175 85		100			-11
######################################	日本		W-01000000000	10.00	·····································	r:				124
			· (E8:64)		Name of Concession, Name of Street, or other	BOODELOCK	85. T			
10421	ADDA:	10100	00.10000		104/V040	2NAMES	444	经常状态		191
	march		+ 任無端期			no Arsta		(Deet)		-
and topics	1017	STR.	description in		4020121	+046710		1000		-
and-	3829	87308				* 20081A		(free)		
	marrie .					2.0	E .9.	() see a		-
0.001	2007	it-failer		2.000	3003003	2410	100	10HE	28	
BERRY .	Wet .	1000					KEX	(100)	200	-
ARTICAL REAL PROPERTY AND INC.	Madette	MALE NO.	12月6日11日	28	PERSONAL PROPERTY.	9.628	60X	(ant)	75	-
NGA PER CO	III III III III	THEFT				*01	412	(Arts)	28	-
	marer		94			4008	400	(Second)	10	-
Redeal	Marris .					4078	400	(1997)	18	
								-	1	1 % 10.0

4.1.2 解析方式确认

在安全服务管理模块,工作台页面的待办事项中点击<解析方式确认>。

杭州安恒信息技术股份有限公司

AICS	o							年 長渡田村地	8. @ant
<u>\$28888</u>	甲台	20 · 162							
Iba		BIN SH		2.01140		10.418		ROOM	
10112				2777729711		the state			
	5	371	9	369//75	0	111	35	182/000	0
NATE		DATE: N		1.000				10000	
EI6101	1.5								
9.21.987	5	話の書店							
H-LODIE -		285年	0888		1185	第1832月1		1.90	
201013	1.0	Bidores.	TRACTO		10000	2821-00-04-2221-00-04		101010	
oune.		Mid:129	1215677		\$208	2521-06-64 (621-89-64		Statistics.	
10KER	1	Wildon zw	weighters	INEX.		2821-07-30-2827-877-80		0000000	
antite		19100121	(eper-		REPORT AND A COMPANY OF A DESCRIPTION OF	201-01-05-2021-07-01			
10000		Bightipo.	100		Correct Correct	20147-29-20147-0		ROW FOR DRAW	0
		#100729	(041		REALTH SALANDONE)	2021-07-29-2022-07-21		1.000 H	-

选择漏洞扫描类型时,点击<新建扫描任务>,点击<提交>。

AICS	ю			5.050948	0.007
***	8 4 8	and a provide a manifold with			
100					
NOTE:	10	解析方式增认			
TURNE	18		·		
1000001	6		40ergater#		
3.05(10)54	e.		marcare m		
Invite	6		WARSHINE -		
14/011-11					
nextire .					
LINCTON	12				
677588	54				
THURSDAY	14				
*******	12				-
8:2540					0

4.1.2.1 发起扫描任务

选择<新建扫描任务>后提交,在待办事项中点击<发起扫描任务>。

得力事所				
动日日称	任务纪律	1743865	预计超止时间	84
3804072+	土机制石田中	生机能动力器	2021-08-04-2021-08-04	ALCO PROVIDE AL
10520729	安全归政任务	#1913B	2021-00-04-2021-00-04	MATHER M
M620725	weight an electronic at	webi展/355篇	2021-07-30-2021-07-30	AMONTO NOTICE IN CONTRACTOR OF
10 20729	(MRR)	周期(十年) 系统学校的现在分 位语	2021-07-29-2021-07-31	signitar
1020729	ENKRYL	後1223第	2021-07-29-2021-07-31	nekszyszaka 🙆

。 安恒信息



输入扫描目标,选择扫描模板 (默认选中"默认模板"),系统开始扫描任务。

Specify With With Parket Interface	1. Oam
TAL BRUTINE TALIA BRUTINE TALIA BRUTINE TALIAN SALIAN	
1. Notice:: 2. All failers 2. All failers 2. All failers 3. All failers	
2.71 TERNA + GB A,W: 1.71 TERNA + GB A,W: <td></td>	
Initian • Exelute 0	
ANTER - CERTIFIC - CER	
CARTAR - FARME VILLEN	
20732 - ULOR 2010 	
1111 Hold Barriel Ba	
-1679	
210/200730700	-
E-INFRAGENCI-I-INFRA	0
带现111	

4.1.2.2 定时扫描

在<新建扫描任务>之后,用户可以选择扫描任务发起的时间,如果勾选<立即执行>则该任务将会立即执行; 若选择指定时间,则该任务仍处于扫描状态,可在工作台处查看。

《项目名称:	Bullans.		
* 春户名称:			
•任务名称:	10月入		
• 扫描目版 ①:	10.20.57.69		
但時機断:	款 小编码		
执行时间:	2022-02-14 14:00:00	曲	() (如何)内行



4.1.2.3 扫描器扫描

	O I∓tt	0 13(43) 810 - 1.414 - 188945	* 205468	68Y
ING BUSTRE INVE		ENRYA		
10-1000 10-1000 10-1000			••	
NATE:		. 138	正在扫描 manufacture	
94138. 04138	6			
2750112	5		•	0

4.1.2.4 导入扫描器报告

在解析方式确认页面选择<导入扫描器报告>,点击<提交>。

A (CSO 安全服务管理平)	INTER CRIMINE I MIRECUMUL	4 设计部外地址	0.887
This mentum Training Training Training Training	解析方式选择 * 点在展示了每年节 - 点在展示了每年节 - 点在展示了每年节 - 点在展示了每年节 - 点在展示了每年节 - 点在展示了每年节		
			0

在待办事项中点击<导入扫描器报告>。



待办事项

项目名称	任务名称	计规则型	预计标准时间	198475
Mitto728	主和漏行任务	主机周日社業	2021-00-04-2021-00-04	中人自認認得苦
第1月0729	主机副口证于外	主机潮行社園	2021-08-04-2621-08-04	13Maak (3Ma



根据对应文件类型上传对应的扫描报告。

項目名称;	DusVMITE	
合同编号:	自动已经	
客户名称:	就是你的客户全部	
扫描器报告		
扫描器:	安极期重进程安全评估-主机扫描-单机器(XML)	1
	安恒明鉴远程安全评估-主机扫描-单机版(XML)	
资产信息	绿盟远程安全评估(XML)	
资产信息	绿盟远程安全评估(XML) NESSUS-主机扫描(CSV)	

4.1.3 资产确认

点击待办任务中的<资产确认&责任人指定>,跳转页面后,展示该资产所属责任人和漏洞处理人,点 击<更改处理人>,选择后点击<确定>。

O CREATIVITI	 Drivel / Brielandinase 			
后产带以来社民人物	æ	在另外要人		NEDMANN
S 1.04%	1740 C		 and the	-917
11.000	NAMES AND	1308A: 0000		all Broks
		adM.		

选中资产,点击<提交>,完成资产确认。



AICS	o							4 675		
安全服务管理	I¥台	#) 2/4	11. 12.41	5.00(2, A) (802)						
									-	
#0 11 8	1.0	进产	8认奏责任/	、指定				100000	EAC.	
10100	-		99	87-68	45	genein.	BRA.	91		
111000100			- 617	AND MADO INCASE	HENREDUTO		16.05.79	.96	REALA	
201820									· [] =	
20111100										
101111										
BATTR.	12									
LINE R	14									
\$17.58	1									
with the	14									
\$2.000	1									
0.000										2
								114		

4.1.4 责任人处置

点击代办任务的<责任人处置>,进入责任人处置界面。

A*CS0	er		ALC: 7						3	
A A BOOT BUILT		Done - Ma								
100										
BOOTTON .		任人批測								(A818)
Init	-	18.0	21-24	他**地图	15.830	ROUGH	307915	JEFIELS.	810	385
TUMPIN		<u>v</u>	INCREASE THE REAL PROPERTY OF	100,168,21,178		10041001-00238 20204-0018- 10518	-	OperASIA (OperASI) Server 5-		-
1.0110008										-m-
101000										
760911.91										
and it.	-									
conter :	÷.									
0.0138										
++0200	-									
*******	-									~
	2									0
										tion icom inter

点击<处置>,选择处置结果<整改/搁置/误报>:

- 选择"整改",处置状态变为"待验证";
- 选择"搁置"或"误报",处置状态变为"待审批"。



处置说明为必填项,填写的处置说明将会在项目经理评审阶段的已选漏洞列表内展现,填写相应信息

后, 点击<确定>。

	12.W.		. 8			
胜任人处置 (14)	- YENDAM	840			3.5	and the second
a W	* 從團說明日	NA AN		ili jene L.		18
	1					

4.1.5 项目经理评审

责任人处置提交后,进入项目经理评审阶段。

- 选择"整改"的漏洞:验证期间状态为"验证中",验证完成后状态变更为"已修复"或"未修复",
 若漏洞仍为"未修复",则进入漏洞复测流程,回到责任人处置阶段;
- 选择"搁置"或"误报"的漏洞:处置状态变为"搁置"或"误报"。

A*CSO								-14	A Martine of the	Onze
安全服务管理平台	0.0 / 10000 / 0.000000									
	and as they arrested to									
-	项目经理评审								0.8111	
LASIN	·宋产有能	107163	enne .	香菇人	#06.0	MARKEN.	SPECE	805		19/5
3.0000.00	0 m.w.m.m.26	152, 562, 37, 171		和意中	CyumikSH 田士田 詳知(14)、2018 1599年	-	Open104 (Open800 Secure 5.)	110		-
24014646								818	(III) a	8.0
201000										
HARING (
Austra -										
tilittin -										
2010 ·										
eenne -										
\$E\$\$213# ·										-
										0
									10.04	an

杭州安恒信息技术股份有限公司



点击<审核>,选择审核结果<通过/不通过>,填写必填项处置说明。

单个审核时,显示该漏洞的详细信息(漏洞名称、漏洞等级、处置结果、处置说明、责任人);批量审 核时,显示被选中的多个漏洞的详细信息。

A*CSO								- 180	Over Over
SHERTER	Str. Daile - Million								
	BERRAW Bran Monarity	815 - 64018 - 02626	781 81			×	and the local pro-	100 100 100 100 100	
		- Phote Repo	ne l						
		RIGHT	A1164	1.000	1.858	MiLA.			
		Operative and Recive-anni 112116	-	**	1	8.27			
		_	_	_	_	82 83			
									0
								0.00	iners and

4.1.6 结果查看

进入工作列表-我的任务,点击<结果查看>。

AICSO									14 JA	READS	Ont
R全服务管理平	er.	REAL PROPERTY AND									20010
TANK											
ALC: THE A	-	UNCE: DO.		2004-0040	10.0		GR 创造	2014			
LALINE	-	integer and									
INDUST											
2010/08/98		兰布古林	2058	1982	12-00-2114-002-00	1.984	SHIMP) A	92		911	
THURSDAY		100001036	HELECTRA	AND DOM:	2021-08-64	889	85819	10.110	110		
and the second	- 11	.E/00110-9	3682774	3100532.0	200-68-04	887	1587	1000	1998	-	
102(1.1)		warmen w	105424/23	\$2811M	30/1-06-04	0.27.9	35.82.9	19.814	79.96		
uniter.		(EDWID)	1000729	\$6-0.50,90000005	1011-07-29	NOT.	487	-	110	1.015	
16210		16(85)	matrice.	9.2128	301-17-29	1107	687		-		
er mil	-	15803	Matuta	1001110-0487300000011000	3507-07-29	50.00	8.809	-	18		
ente:		(UNIT)	Madorize	1000	1021-07-29	822	10.017	(+)+	an.		
-		(89393)	1040174	计算道系统数	300.47.38	647	8.67	-	1948		-
100	2	00100	10002738	计算法规则	30(1-07-0)	1.2.5	15.874	1000	10.05		0
		1011112	1000723	PERMIT	3225.477.00	10.00	487	-	28	-	



点击<结果查看>,页面跳转至 VM 弱点管理平台-工单管理-该任务的工单详情信息。

4.2 渗透类流程

渗透类流程包括渗透测试、代码审计。



4.2.1 添加计划

选择计划类型为"渗透测试处置"。



5311±1										
2793 8	_		播加计称				- 38	_	_	_
8404 mar							and the second second			
	1110		* 15(5)-15(4)		+ 计 祖國聖					-
AVE - 25	DAMA 1		all and the second second		SHOW HERE					
			* 任務会社		+ 動程人					
1926	100.00	21220030	3092-101208		1967-00/5A		MA.	GRUE.	-	6
6	1962111	0-1010	+ (14) 8(25					2008		200
AND A PERSON (Here	anno.	8842012				10 C	(SHE)	**	849
1948-	ातमा	107304						010		300 C
9883)	10041111	APREND				0.18	12	(Dec.)		Bie .
a mure	THE	R-SHER		177	NO. Kenn	100	800	100	88	-
BP25RA	100	229-21-				400	452	(mex)		221
COLUMN TO A	- Bed I II	station for the local	STRONG	- 24	ACCOUNTS.	443	4425	(ROE)		824
IN THE REAL PROPERTY AND INCOME.	Barre	STREAM OF STREAM		10	anarests -	210	410.	(10)		Sie.
Differences.	Matte	III. OR ADDR	aler 1			200	***		**	100
and the second se	384011	m-100				800	822	THE .	- 48	334
								4115 (T)	1 + 1 - U	1.100

4.2.2 选择资产

渗透类流程的资产选择为"应用资产"。可针对资产名称、类型、域名、业务系统、资产标签、资产责任人进行应用资产的筛选、查询操作,选择资产后,点击<提交>。

-	17.							
ńsłę			8-92 414			26		
RITIN	0.00		#*#B (444			APRIA MAR		
	2765	2792	8762	NAM .	4754	#IIA	8*52	240105
	101104,015	10.5.2.28	900	1.8			913	3825-16-27 12:4837
	MAG ACC 210	1652-00	wee	- 4			1018	2010/1-10127-1244-57
	ALLEST_WIN	10.0.0.0	week.	306			903	2021-10-27 12 AUT
	HILLIN, WIE	16.2.2.36	W18	- 12			345	2011-10-27 12-46-37
	NISTER AND	10.1.1.10	1953	- A			100	3121-10-27 CAALUT
	111.1.15, 1618	10.2.2.00	1978	10			1012	2021 - HILLST 1344427
	WW.WILLIN	10.52.00	WE				-	2011-01-27-13-04-07
	TELLAL WIR	10.5.1.44	WHE	14			1018	100110-01110-0011
	115.627,WHE	19.3.210	wo	508			1413	anarchi ari spandri
	VII. LAL MYR	75,520	1499				112	2021 IN \$1 1244.21
							ana (ii):	

4.2.3 导入漏洞

漏洞详情涉及资产列表和漏洞列表,点击<导入漏洞>,进行漏洞文件上传,若无模板则点击<下载模



板>后填写上传。

AIC50		and these states						-	ARCTAL CART
THE			BERRY A.			38			
an Links		ARRINE.	-2818		1883/5	Villes.			
10110	e.	C. HORE.					7855		310000
300000		11 H(1) H(301, H00-			10.00	10		1411	221-10-14 122-10-14
27019999								#18	(I) use
		Company of Company							
		Contraction of the second s							
									0.000
	-	21. AD51: AD54	(#795)	MAXA	30028		1945	- 83	18 .
	×								
	÷								0
11110	2								
									8.0

点击<导入>,导入漏洞成功。

点击<导入报告>,导入报告成功。点击<提交>。

WEB.
WEB
WEB
· 🛐 - 415

4.2.4 资产确定

点击<更改处理人>,选择后,点击<提交>。



输送减速加入非	WGE:	with the later of		BREAKSAN.
1.0450	Area.	and the second sec	C CREAK	(81)
1 ()	102223.049	+08A [Fault		TR. BALES
1 a.	110000.000	404	4481	NR (RADEA)
1 (B)	THEORY AND	28	9.8. NO.	NN (MINER)
х (к	20008		848	HALL BOOKS
1.00	ARE AN AVAILABLE		8428	WE CHARGE

4.2.5 责任人处置

进入责任人处置阶段,点击<处置>,选择处置类型为<已修复/未修复>。

- 选择"已修复",状态变更为"已修复";
- 选择"未修复",状态变更为"未修复";

A/CSO												-
安全部的和原平的	ŧ		-		1				-			
		供住人的	al P			# ###	etal.		×	Services	-	(144) (144)
		10.000	-		-	0	作業		-	-	144	-
		10.00	183	-	-	08658	HORIDAN	marganet propriet	- 1			1.00
		14 ST	1001		1.00	-	minute	maximum protonet	-			-
	1											
	1											
												6
											and a	in the second

4.2.6 项目经理评审

进入项目经理评审阶段,点击<审核>,选择审核类型<未修复/已修复>

- 选择"已修复",状态变更为"已修复";
- 选择"未修复", 状态变更为"未修复", 该阶段若状态为"未修复", 则进入漏洞复测流程, 未修



复漏洞重新进入责任人处置阶段。

A-CSO		a statute () and
2010 2010 2010 2010 2010 2010 2010 2010	-	
		A18 (11) (188)
11111		
		0

4.2.7 结果查看

流程结束后,进入工作计划-我的任务,点击操作列下的<结果查看>。

AICSO								14 M	RENDE	Oat
全線的管理平台	22. (DOIL) NO									2010
hak										
ताल -	UNKE IN-		1.0	1010		GR6	£ 5.11			
- 181	intentar and								ALC: NO	
Interests										
TOTOTAL	E#88	20158	11122	拉希利400%	1.984	DRM/IA	82		9/14	
The second second	HERMORY	HUDDE	FERRENT	3001-08-64	887	15.879		100	-	
11111111	HERRICH	36007/18	HERROR	300 48-04	0.87	1589	1000	0.00		
10)(I.M	VICE IN LOUGH	195422/28	涂铝树式社内	30/1-66-64	829	35.824	100	7158		٦
atas -	TORINE	100007	26801年	2021-00-04	NCT.	487		215	1.075	
1918 -	EXAMINEN	matrice	STORTIST.	2021-08-04	147	687		-		
- 141	ATTACHEM	Babito	21001010	3037-00-04	529	8.879	(beet)	18	1.1.2.8	
die -	业出行通行的	Multirian	##59#	2021-08-04	827	10.077	(4)(4)	100		
- 100	16001	10421774	888/18/98/2980000-00	303-47-28	547	887	-	210		
	1880)	10002125	5.011M	3047-477-29	1000	15.87#	10000	10.05		0
	10017	1000701	Statistics and a statistical statistics of the state of t	10. 11. 11. 11. 11. 11. 11. 11. 11. 11.	201	487	10.000	20	1000	

页面跳转至 VM 弱点管理平台的任务管理-渗透测试-任务详情。

杭州安恒信息技术股份有限公司

6 DAS-VM	* miller *	GARE	. 17755				-						180		0.441.555
• 11/1 WW -	onthe court and	10. MR												_	
80.0					80	17.40x11905-1446-1	148-4082-0	Alac world							
8552	and and														
8*98	acc-na														111
UNER -	****	31.62	-101		****	mean.	-	1.66	14	400 401	140			**	
CHATE	0.04420_40	100	40.03.44	200 ;			1.01	1.4	1.		141				
limat:	1011						-		_						- ¥
	410.1.00											10	- 1997	48.1	
	3074														
	APR		ales. (re	- 1010-0				100			(inter-			1.0	
		ée) (
	1.000	-	-												
		-		and the second		A*100		0.000		work.	- 84	en .		-	
						2,50									

4.3 通告类流程

通报类流程包括外部通报预警。



4.3.1 添加计划

选择计划类型为"外部通报预警"。

			LOT N						
					Contractor 1		-		
IN MAR. NO.	CRAFT.		A	tal-di	UNITED FOR STREET				
			1.8.94		18944				
199	01110	1000			dan tan t		20	8845	
		areas a	10.000					100	
distant di		1999	depart following					Cher.	
-	1.00	1100						dia.	12
	1.000	and the state				10.01	100	100	47 54
	127.	arease.		-	1000011	410	440		28. 85
Sec.	1.00					***		100	48.44
	Aure		age a			853	101		48 84
1. 11 E	1000	CREWENCE :				*1 	102	late.	12 21
BATHLE DATE OF THE OWNER	Barth	and the Real Property lies, th	8			400	*//=		40 00
-	-	area.			and the second s	were a	-		
								www.dth	



4.3.2 选择资产

外部通报预警的资产选择分为"主机资产"和"应用资产"。可根据资产 IP、类型、标签、业务系统、 应用、系统版本、资产责任人等进行主机资产筛选,选择资产后,点击<提交>。

±6,0/H	2月前午							
10 ⁴ 10			1745 (1088S		
E*88	ant.		2.4			6404		
NUCS.			#P#GA: ====					
	8-68	2×4	8***2	jačne:	2.65M	851	87462	Links
	190343132.250	(4) 10(21.22	215	1 C		Aut200	111)	2021 (2-63-152049)
	1020020.25	18-00-01-010	1910			ACHT -	(92)	2021 St-42 W-2059
	1902-008-312190-0246	(Au) Austication	2.05			AUTO	18.85	max on 26 example.
	10.1.3.2.20%	16.2.1.2	385	181			出95	3021-30-2711-96-46
	10.1.2.1.0.2010	18.1.2 128	31.0				3.85	2011 NOT COMM
	10.1.111.2245	10.0.000	2.65			#71m	10.95	2021-0219-100824
	10.0.012.005	10.0.0.010	245				18%	2021-0119-020024
	101.0171_005	48.8.4.10*	(2.9).				105	#54637 R118-15%
	10.1.1.10.20%	(0.07.026)	215				111)	20071-31178-1238-214
	115210.28	1012240	311				3.81	(007) 10 19 10 million
							(#10.6 · [1])	1 K.1 - II > 108/8

4.3.3 上传外部文件

填写相关信息,并上传附件,点击<提交>。

安全服务管理平台 : 150	II - Dentris - Beenhamer	
ING		
HILDE .	上传外部文件&编写相关信息	
1000 -	- 担关位用	
TRANSFERR.	in diaminant	
Initem.		
270104686	129	
10201131		
NATE -	T. Tames	
contra -		
44138 ·	<u>11.4</u> 0.	8
#4308 -		
*****		0

4.3.4 责任人指定

点击<更改处理人>,选择责任人后,选中资产,点击<提交>。

	CONTRACTO	I I THIRD I REMARKAN						862
<u></u> 第/中幕	间认备处理人工	RE .					alexener.	
TR/4-	6597							
	*0	d*68	55	24935	#12.4.	MHOLE.	211	
	1.4	THE PROPERTY AND	100.100.21.02		ALSE	0115		BUTCHEA.
	3	16.56.51.200_20%	10.00414.000		Addate .		-	BAYER-
							816	1

4.3.5 责任人处置

点击<处置>,选择<未排查/已排查/未涉及>,点击<提交>。

	11.00		×		
的任人社會	184	8	10		882.0
INST OVALUE	1.0				
KR* smar		- Epold + 100			
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-			ENILE	344
	10			2.00	10.
			8.8		



4.4 云 EDR 告警工作流



在安全事件管理模块,配置管理-管理流程绑定页面,绑定新的管理流程,依次输入研判、T1 处置和 T2 处置人员所在钉钉群的 webhook、sign 和对应人员的手机号。

									NINTERNI I
REAL	м		883.	manent	1	#ISRN		80	
WINDOWS			***	301100-001411029		8	RYPER	-	-
CIADEVINE.	jungeWebbunds	Rige) (agi dispaktori/valit/ard/acoit_late	1597	2011/06/10 1710/24		8	al sector	NE	-
	Lebertupe	INCREASES AN							
	1.1gePasse.	10240418000							
	handlerWebburk	why the department of the second s							
	heiderlige	978-9244468819778-0296619767							
	broleftene (1559318003							
	hermologie (Mercele)	Approvage displatic error whether of lacence, betw							
	handlinkplatifign	973-00-4449-001512/94(101964)36782							
	handler/Agail-Product	152844 HALLO							

在事件管理-事件监控-提交事件页面中,选择管理流程名称为"云 EDR 告警分析处置测试",选择项 目名称、事件来源、事件标签和告警时间,填写事件名称,点击<提交>。

4提交				
	· ##59409:	ant Alignetic mail		
	100568-	CLASS OF BRIDE		
	- #11610	10408060#		
	- 81575.8	1.Rov	a salest	
	- 8446/5	web.ob.03/170724898	and the second se	
	- #115.00	8 XIN () 801 () 942 () 853 ()		
	- 100010	2022-09-13 15.0034 27		
	наеф	10.0000/0000000000000000000000000000000		
	RMETO	MACONSTRUCTION AND INC.		
	0.420194	8 7 == == ==		6

事件提交后,发送钉钉消息至研判群,并@对应的研判人员。



若事件研判有效,进入T1处置阶段;若事件研判无效,则进入误报列表。

HD#				20
	2011(+4+10 =1(4)) 🛇	NUME INCLUSION INCLUSION (INCLUSION)		atten
	2011/01/01/01/01	AND REAL ANALONATION () (INTRO)		- 201
ų.				
	- 894623	* + 102		
	1919 B	E Suga	NENE	
	#19501	8 I = = = =		

事件研判有效后,发送钉钉消息至 T1 处置群,并@对应的 T1 处置人员。



若事件 T1 处置为"已解决",则事件归档;

若事件 T1 处置为"未解决",则进入 T2 专家处置阶段。

PHILE				d.
380.00		NUT WITH ALS WITH THE REAL OF THE SECOND	1.00	6
30((++)		(age : and a first a the second second second second	. viic	
307144-1	0	INTEL BOOKSTOL HERBOLISSONDER (INCOME	0110	6
2011-04-1		AVT BID: ANDDRETBIADCR (Contain)	1.000	6
	1 (1.0010.00	CERN W AND		
	10083	BENR Y		6
	0.0070	6 / = = = G		-
		DO. HOMPOMIEL		

事件 T1 处置为"未解决"后,发送钉钉消息至 T2 处置群,并@对应的 T2 处置专家,由 T2 专家处置

后事件归档。

à	内部评审机器人	查机器人	
	测试钉钉消息 事件来源:长考 事件标签:web 攻击IP: 受影响IP:	息提醒 SWAF oshell后门攻击事件	
	事件等级:高炽 告聲时间:8/1 告警详情:1、 界。2、攻击制 攻击的汇总载 明:攻击的汇总载 明:攻击的汇总载 日志的截图,一 件结果:该事件 需要T2 全事件	1/21,9:45 AM 监控设备位置:网络边界/地市到总部边 每件简图:攻击汇总的截图,如多种类型 图,包含告警日志条数。3、攻击事件证 事件的详细日志截图,能证明攻击成功的 最好包含筛选语句在截图中。4、攻击事 牛攻击成功/失败。 专家协助 @马建锋 请尽快处置 查看安	

。 安恒信息



4.5 港中旅工作流

4.5.1 敏感信息发现与排查



在安全服务管理模块的工作计划-任务列表内添加计划,选择计划类型为"敏感信息发现与排查",填

写相应信息后点击<确定>。

添加计划		Х
* 项目名称	* 计划类型	
输入项目名称可选择项目,可多选	流程归档 / 敏感信息发现与排查	\sim
* 任务名称	* 执行人	
请输入任务名称	请输入执行人	
* 任务周期		
请选择周期类型		
	取泸	当 提交

上传文件&填写信息,上传附件、填写情况概述和敏感数量,点击<提交>。

- Weider Nitzlanderen	
T Tame	
- WARD	
and the second	
- Unicensia	

填写处理结果时,填写无需处置数量、整改结果、整改数量,勾选是否完成:

若完成,则进入下一个节点,项目经理审核;

若未完成,则进入循环,重新填写处理结果至完成。

🖸 administration - Intern		BET-
编写处理站表现		
	- Balling-United	
	T Turkin	
	ARE A DESCRIPTION OF THE ADDRESS OF	
	Dettes	
	- 12128/2	
	- iplice	
	SALADAR.	
	- STDIA	
	BARE	G

项目经理审核,不能对信息进行修改,填写审核意见后,选择是否通过:

若通过,则流程结束;



😑 🛛 sisantaryo 🔹 Ikuw		8971
	in the literature	
	BARREN STATISTICS	
	PROVIDE A CONTRACTOR OF THE OWNER	
	101703	
	15-34	
	Bright	
	新式的基	
	hinnen and hi	
	14992 2014 - 2017	
	#040 T	0
	E.S. E.S.	



4.5.2 互联网资产发现与管理



在安全服务管理模块的工作计划-工作计划列表内添加计划,选择计划类型为"互联网资产发现与管

理",填写相应信息后点击<确定>。

		1831014	ti .							
PROFE THE PROFE					400000		100			
		1.000	and the second second second		AND	topol.				
										1
943	100.000	(Index)	e Alexand		BUDA,		100	lines (6
		section light					6	[399]		-
RRAND RR		(445) ····	-					(Dec)		-
mai-	82	11-22					i.	and i	-	-
1000 C	-					8.4	100	THE OWNER WATCHING	-	-
1000	- 100	R-AMER		1947	STATE H	1828	216	THE R.		-
mana -	391						(448)	Dest.		-
motore E	800 11	ARCHARDS.	π	44	STATISTICS.	808	800		-	800
Charge and Long	BALL	104115		28	and the second second	***		(week)	-	ante.
residences.	and the second	COLUMN TWO IS NOT			INCOMPTO	82.0	100	1997	-	-
MIREN C	000011					602	ALC: N	[2008]	(88)	-
								Maine STATE	3 4 4 - 14	

第一个上传文件&填写信息,上传附件、填写情况概述后,点击<提交>。

上传文件 & 编写信息			
	- 30407-84		
	4.2000		
	THE PARTY AND ADDRESS OF AL		
	and a second		
		-	

第二个上传文件&填写信息,上传附件、填写情况概述和资产数量后,点击<提交>。

杭州安恒信息技术股份有限公司

- 335H-2750HB	
4 1000	
LARGE THTELER DEPENDENCE IN AN	
- W1962	
anali	
- 0794	
1°	
- 101ML-10	
1 Liters 78	
- S294273###H82	
911012	

填写处理结果时,填写无需处置数量、整改结果、整改数量,勾选是否完成:

若完成,则进入下一个节点,项目经理审核;

若未完成,则进入循环,重新填写处理结果至完成。

C STREAM STREAM		
	ROM	
	 丙基基本 <!--</td--><td></td>	
	- 02019 (7*102) #0.6(2)	
	1 8764	
	1	
	- 92/85	
	* 82.447	
	- Alderian	
	8584	6
	6.8 C.N.	

项目经理审核,不能对信息进行修改,填写审核意见后,选择是否通过:

若通过,则流程结束;

若不通过,则重新回到填写处理结果的节点,直至审核通过。

0		A87
	A after 78	
	ADVARTED AT MUS	
	1748	
	8708	
	第 月1日年	
	10-010	
	- 81282	
	at .	
	RANCO S	
	87 S.A.	

4.5.3 钓鱼邮件测试



在安全服务管理模块的工作计划-工作计划列表内添加计划,选择计划类型为"钓鱼邮件测试",填写

相应信息后点击<确定>。

🛛 segenne 👘 :	anne dene									
列表	le le		38.440+36				1	1.1		
			(WINHT RD)							
			· #868		· IFTINS					-
1945 2 49 MIN	Carse :		NO. A DECEMBER OF DESIGNATION OF DESIGNATIONO	. 104-6	102011/828614182					1
			- 注册 能物		• 纳行人					
ENAN:	6248	Home:	862 (DE CR		2002/07/5-0		48.A	GMME	100	•3
	2004111	877388	• 私用運輸				0	1000		200
AND REAL PROPERTY.		2784	annead				÷.	1940		-
MAR-		2-00						1000	-	-
1181	(Belly)	175300				8.94	ER.	294	20	-
1100	1001	Water and		24	West West (***	-	1997	**	-
1-28.83	9221	ARRA.			100000	24.0	-	(the second		324
	Marrie	Ani DAT	COLUMN TWO IS NOT	1.000	Internation .	202	550	(100)		250
rezhia er sente 💶	855111	Harwitter				825	420	(mare)	-	-
ATMAINTMAN AND A	BARTON	1011383000	alan i	- 101		A82 (4000	(Beer)	- 98	-
and an article of the second se	1.0000000	and an other little		1.00		10000	Concerned in the	(Internal)	1.00.00	Sector 1



第一个上传文件&填写信息,上传附件、填写情况概述后,点击<提交>。

- 10 ARV/WALKERS		
4.30000		
- MOUNTA		
444-40-444		
	1778 av.	
	- BLANDWALLINCON - L. ANNANA - ANNAL - MANNAL - MANN	

第二个上传文件&填写信息,上传附件、填写情况概述、涉及人员数量、上钩人员数量后,点击<提交>。

- provinces	
A attain	
- gentral all the set of the set	
* \$2,426	
- 190 MRB	
1.818790-03000	
Litter 18	
- 914/07/06/2017/094-5462 WYSEL	
(11) V.	

项目经理审核,不能对信息进行修改,填写审核意见后,选择是否通过:

若通过,则流程结束;

若不通过,则重新回到第二个上传文件&填写信息的节点,直至审核通过。

🛛 Simotheyis 🔰 Inum		Maren 2
	32.34800 MB	
	COROSINI, WITH WITH LA	
	104	
	The second s	
	Class 1	
		-
	HU人用ma	
	上的人生物量	
	- exert	
	nciazi E	0

4.5.4 安全应急演练



在安全服务管理模块的工作计划-工作计划列表内添加计划,选择计划类型为"安全应急演练",填写

-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1	101110 / 100000								
		_	18.000±141				×		
34		_	a minimum and an		(Laborer)		10.0		
and Area	there is a second s		al antened manager	0.6	BREEKS/ STRUCTURE				COLUMN STATE
			- (1861)		18/74				
	No.41	prints .	md-10000		age_4.00(1.4)		MA.	1200.02	80
	Martin .	8-74LUM	-128.48				17.00	(9944)	
ana kalendi T	3660 (19540.	angel limbers				6	1000	10.00
	101	0.00						2000	ALM
	201011	0.000				0.10		I DATE:	89
		8-70018		599	.8429309.	8478	400	1000	80.00
10		10.000				80.0	410	12/22	
	THAT IS	ARCIT OF	Internet and	391	-712.512.0	2.63	150	THE OWNER	** **
-	Marry	(SEMIRE)				800	810	TAXABLE INC.	22 324
SPRESSION.	8011	orr.setter	See .			253	2410	(ALC: NOTION OF	12 -

相应信息后点击<确定>。



第一个上传文件&填写信息,上传附件、填写情况概述后,点击<提交>。

O STROUGHT TH		
上侍文件 & 编写信息		
	- SHERES	
	-d. Anten	
	- August	
	PR- 1992	
	A	

第二个上传文件&填写信息,上传附件、填写情况概述后,点击<提交>。

上传文件 & 項写信息		
	- 048690	
	4. 21899	
	LANSE THREE DEPOSITION OF AN	
	· 12*24.00*0402	
	day processing	
	- LEWART	
	4.1thmy VW	
	CHRANTWISH	
	#18065	

项目经理审核,不能对信息进行修改,填写审核意见后,选择是否通过:

若通过,则流程结束;

若不通过,则重新回到第二个上传文件&填写信息的节点,直至审核通过。

目经理审核		
	17540414044	
	- manual	
	- 258440	
	12.2000 TB	
	(historie)	
	analog .	
	- DRIMANT	
	2.2000 VE	
	nóisc B	6

4.5.5 玄武盾监测告警分析与处置



在安全服务管理模块的工作计划-工作计划列表内添加计划,选择计划类型为"玄武盾监测告警分析与

O Someran	-DHITLY GAMOR.									
列表	Her Ma	. Le	imico+40				4	1 1		
800- mar			Second of							
			- 油田式町		+ 1713M2					
	(inter-		4	10446	0.0000100000000000000000000000000000000	Netal				
			* (<u>188</u> 49)		- MITA					
ERMAN	(10049)	1000	discounter and		1063,81714		19.3.	ante		a.
10	MACH	W-FURNE	+ (<u>1</u> 14)(N (M)					(Dere.)		
gik a constants	100	SHEEK.	diamani di					(Case of a		-
		1.100						(Dave		-
and a	Reim	annena				4.16	8.0	1000	**	-
CONT.		5-7008		1.11	And Advent	45.0	858	(Sector		-
b*2881		2841		1.11		812	AND	(marked	25	-
	1000	month in the second	No.	25	Distantia	212	-	(and the second		-
	Desarry	STREET, B.		34	34230,44	***				-

处置",填写相应信息后点击<确定>。

上传文件&填写信息,上传附件、填写事件数量、处置数量、误报数量和情况概述后,点击<提交>。

杭州安恒信息技术股份有限公司

守旧信

- INSTRUCTION OF BRIDE	
J. J. Linker	
CONTRACTOR AND ADDRESS OF A DECEMBER OF A DE	
· Pros	
- (CRUS)	
- 40 VAL2	
res temp	

项目经理审核,不能对信息进行修改,填写审核意见后,选择是否通过:

若通过,则流程结束;

若不通过,则重新回到上传文件&填写信息的节点,直至审核通过。

- TAXABANAN		
(2.588) 16		
MER .		
8540	17	0
	an an	

4.6 安全运维工作流

4.6.1 安全设备及平台巡检





在安全服务管理模块,在安全运维阶段添加建立"安全设备及平台巡检"计划类型的计划。

359U-8			18201-05						
							100		
			100000		+1:5145				-
ABACE 28 BE BALLS	CODR .		A1101 1010 1010	0.40	1000010000000	-SN			
			103840		+ (821A)				
10047	20.04	PORS	10000, 1 - 12, 40 - 41 (10)		100.1 (0.7.1.)		110	isten	MIT:
1	100011	-	11210100					1 per l	82 200
ARRIVER.	940	20444	ASSESSME					(mark)	25 20-
404m	1.1915	R-90						(ever)	es av-
	marry.	areas a				8 m		int.	-
281	1000	arrand.	64	Sec.	And the second s	8478		Contract of Contra	88 59
RPARAS.	Net	-				8125	225	18965	44 24
ARCHINES C	- 1940/1		INSTRUCT		20000344			INCOL	100.000
Carlos Carlos	States 1	TENTER		17.		412	***	(April	-
and designation of the local division of the	degrand.	ter, sale	atte			802	813	100	25 900
AMONTO:	100211	-				800	200	Time (85 8 0

计划添加成功之后, 录入巡检记录, 选择设备状态为"正常"或"异常", 输入备注并上传附件, 点击

<提交>流程结束。

😑 🖸 Asmudaka i Tumu		687-
录入巡检记录		
	5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 50000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5000 - 5	
	- 800 - 1 Califo - 1 Califo	

杭州安恒信息技术股份有限公司



4.6.2 安全设备及平台维护记录



在安全服务管理模块,在安全运维阶段建立"安全设备及平台维护记录"计划类型的计划。

69%表			#20+0							
			- and the second s				-			
			ALTERNATIONAL TES		FITTING .			-		
					ALCS ALSS ALLS	- inter-		-		
			10000		(BALA)					
INCO	#2 EX	111540	1000-1 (100-0-00		001471		100	129-012		
	10000	A-1000	GRAM						88.00	
COLUMN AND ADDRESS	1111		date from the					The second se	10 10	
Sear-	Mari -							100	82. 50	
	Max 111	arrested to				8.00		and the second second	22.00	
	mit	Arrest Street	2	(94)	Address of the	CROW	100	1000	22.00	
ATLEN.	1111	4885		22.0	Television (410	862		88 80	
CO research	-	and be	COLUMN TWO IS NOT		percente.	84.0	850	100		
Dis-th	Mag 111	. ridialette			analysis of the	200	***	Sec.		
TROUGHDORNESS	MALTI	COLUMN ST	44			100	100	(and the	2.0	
89-87V)	10000111	1.000				100	101	1000	88 80	
								wine of the		

计划添加成功之后,录入升级记录,填写设备名称、维护内容并上传附件,点击<提交>后流程结束。

e 11	Mar-
ance	
mulana	
- 10PV/d	
The second secon	
- 898	
A 1.10000	
	6.A
	+H - BECG - BE-VA - BE-VA - BE- - BE-

杭州安恒信息技术股份有限公司



4.6.3 安全设备及平台策略调优



在安全服务管理模块,在安全运维阶段建立"安全设备及平台策略调优"计划类型的计划。

	nito / Enna		والصححة تتعرف المحازد			ويتحجب للطام			
勞列表	1.1.		(\$10+4)	- 14	19.1		- <u>-</u>		
			Analysis.				and it		
den au air i	-		A Annettafan III-		+1045 #208/#2080708885				and the
		1.000	1.任用有印		- 18/7./		100		
GRAD	10111	mains.	444.1.0.000		AUG. 1. AUT 1.		10.A.	127012	87
3	REALING	3-1202	+ 1241 MINS				1.	and a local division of the local division o	22.00
ERATINES.		2031	#1000000					1000	22 80
andr.		11-210							
ORRECT	204111	-				30.00		(Inter	100 000
		1-20.00		187		-	-	(Dec.	-
aneses.		-			and April		***	1000	22. 80
ABLINGED TO	-	3815.65	COLUMN THE OWNER		Including	-	800	Are	20 80.
	Manual V	nerging #		100	and a second second		-	10000	-
	Magrill.	TO CRAMON .			20200311	200	8416		
and the second	MATT	327808			ISCONT!	100	*65	THERE	22. 80
								A 100 1 11 1	A REAL PROPERTY.

计划添加成功之后,录入策略优化记录,填写设备名称、策略名称、策略内容、源地址、目标地址、

条件、备注和上传附件,策略优化时间和策略生效时间默认为当日,可重新选择,点击<提交>后流程结束。
	W195	
大策略使化记录		
ST STREEP IN COURSE		
	- 128-E.M	
	184-1954	
	- 300-cm	
	AL-1814	
	- Mathiag	
	Aug. Statest	
	· Statutes	
	1000 F 100 F 10	
	- MM(+1)	
	NY CRUZ	
	 More a source 	
	3001-09-17	
	- Mag	
	data-prose	
	+ 628-401	
	20-1	
	- 94	
	dillo 3 H	
	-51	
	((8512	
	4 L1009	1.00

4.6.4 安全设备基础信息收集



在安全服务管理模块,在安全运维阶段建立"安全设备基础信息收集"计划类型的计划。



			(\$11.1+10)						
and set a					() () () () () () () () () ()		10.00		
10-8-22 A/74 A	34.4		1.0000000000000000000000000000000000000	100	COMP.	- 290			
			10880		- IN/57.				
-		ineres .	1000, 1 (1 (0 mills)		and dorts.		ATTA	12,004,000	100
	10000		- 42.404.48				01	(INNE)	100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (10) (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (100 (10) (10) (
(0.1)-mailed	ंत्रस	488.	0.0.0000				0.2	200.	10.00
and the second se	10.0						1	ALC: NO.	88 . 898
		271000				8.8		Saf.	-
inte la companya de l	1441	arrante.	-	.0	DEDITION	400		and the	100
5881	1991	104.0		(14)	10000001	(100)	(4005))	1004	and the second
	3960111	WHICH BE THE	LITERATION	1.44	month.	1808	(449)	and the second s	
meren in	merri	FORENER			and the second second	85/2	-	100	-
Station of the local division of	Martin	Luo mano	1818		and the second	100	410	Charlen .	80, 201
10000 C	BARTIN			4.0			4425		100 000

计划添加成功之后,录入信息,录入设备名称、设备访问地址、设备型号、设备安装日期(默认当日)客户信息,输入备注,上传附件,点击<提交>后流程结束

4.6.5 安全设备及平台故障报告



在安全服务管理模块,在安全运维阶段建立"安全设备及平台故障报告"计划类型的计划。



ALC: NO.									
2771-8			181411-10				×		
LAN IN							ALC: NO.		
			- 4884		- 开的编辑				-
tare + sa nor			W. CHARLEN MARK	10.00	安全設備:安全設備混开作	NUCLEOR IN			a series
			- 任務改務		* 旗行入				
UA4M.	225.0.0	testing.	1041/25110		UNICARITA.		124	to all stores	and the second s
	marith .	arrive and	- (10.40)					11000	10.000
0.68.0.000		OWNER.	812223					100MC	20.00
an er-	1117	areas.						244	25 20
2.81	marrs)	ar stand				5.0		100	
10 Mar.	11.0	ar-idana.		1.1.00	and the second s	100	105	100	
1740 K.	1115	OREA.			BEARS IN	300	8.04	Distance of the local	
AUR 14 A 1911	magers (ARCS NO.	476912 (124	2010/00 Mil	800	402		1001100
	DECTY	-		21		260	863	1000	88 88
JIS-SEALSTREE.	Matrix	Cit pana	atem.		ALL DISTANCE AND DESCRIPTION OF	100	1100	1 Marcal	28. 200
ana ana	Martin	-			and a state of the	Atte	100	1000	-

录入信息,录入产品编号、产品名称、产品地址、故障描述,上传附件,点击<提交>后流程结束。

a view		
東入語母		
	14 BAR	
	(Max 1948)	
		4
	1750h	
	48177558	
	market and the second sec	
	- 2003g	
	re-inva	
		£1
	1929	
	57 55	
	Control (Control (Contro) (Control (Contro) (Control (Contro) (Con	

4.6.6 安全工作报备



管理员和 OPadmin 进入 os 启动页,点击右上角编辑工作流,进入工作流页面。选择 A006_安全工作报 备流程的.bpmn,点击编辑,点击工作流的第一步,设置//环境变量

def reviewUser = "计划添加人的手机号"

execution.setVariable('reviewUser', reviewUser)后保存。



编辑完成之后点击<部署>,点击二次确认部署弹窗<确定>。



在安全服务管理模块,在安全运维阶段建立"安全工作报备"计划类型的计划。



О создания	NAL OF STREET, STREET, ST.								+715
任勢列表			t de la de		1.1		1.1		
			- 第350(1H)				× .		
			- 病務老均		· vramed				
THE R. D. MIN 1	(1997)		WARDOWSLAUGHT.	018	REDA/REINES				and the second
			+ (2888)		* #JEA				
mes	-	ALC: N OF ALL PROPERTY AND A	and its an		departs.		154.		
	maria	8172218	- (2.8.368)					2000	910 B16
	1000		antitionet					100	
1000	1007	2-10						(max)	20 00-
1995	(Western)	-				8.10	10.00	I DIRECT	AM
RE-	THEY	No. of Lot, No.		15	manual re	100	840	1000	
84065.	1.000				and a state of the	+111	802	2000	22 80.
anatara ana	Regist	NAME OF BRIDE	INVER-		and the second s	***	100	1940	
	86411	HIGHING			and 100/11	800	100	Land.	0.0 000
	S MARTIN	- 200,000	6×			3995	313	(March)	
Margarit.	Meaning .	-			maximum ere	100	w00		22 21
									1.4.1 - 11.1 (HAR)

填写工作报备,时间默认当天可自行修改,输入内容、涉及网元、影响范围、操作人姓名、添加说

明, 上传附件之后点击<提交>

向工作物香		
	144	
	and an	
	148	
	1400	
	- AUX	
	I DATE	
	and a state of the	
		2
	- BRX	
	88-81	
	1.00	
	10.02	
	194 -	
	4.2開発	
	Toronta and a second se	
		() () () () () () () () () ()

流程进入审批工作报备,勾选是否同意,填写审批意见后,点击<提交>;若审批不同意将重新填写 工作报备直至审批同意。

NULT UNDER		
	-	
	eten.	
	aving	
	and Control of the control of the	
	1.014	
	The second se	
	8758	
	web.	
	allo and a	C

审批同意之后,完成工程施工。勾选是否完成,上传"拨测证明"附件后点击<提交>;

Service		
U-EIH-MI		

	54 C	
	units .	
	1412	
	and an end of the second second second	
	TOTAL N	
	ers 1	
	17mi	
	18804	
	4.2494	
	848C	

工程施工完成之后由项目经理复核结果。勾选是否复核通过,填写复核意见之后点击<提交>;若复

核不通过将在工程施工出处重新上传拨测证明完成工程施工直至复核通过。复核通过之后流程结束。

		1.4.5
and a		
-		
-		
17		
1 mm 1		
Contract in the second s		
95-14-00		
-		
100		
17775 18. 0-10		
	100 B	

4.7 周期计划

4.7.1 安全告警监控数据录入工作流



在安全服务管理模块,建立"安全告警监控数据录入"计划类型的周期计划。

1917-06			38.00 Hit		× ·		
ARRA DEC.							
10. 2 10 Ave	(10.0		IM VARE FOR FOR THE FORM	ebite.			-
(A 21)	1000	CHOME:	LANSTER PARTNER OF STREET		4.6	0.010	(MARK)
	-	acres in	448-07em48-1222014	10875-506700 KSW20071908.		1000	10 M
and opposite	100	URBA.			_		20. 00.
and the second se	Trail.	2-20	12247	11100		1000	
an)	-		ALCONTRACTORS (1998)	ANELINA / REPORT AND A PARTY OF A			
#541			- (E#@#	《神法人			
		1000	and Critical and	PALMON.			12.00
-1		1000	- (ER-988)	· MRFmmtR		Contract of the local division of the local	
CONTRACTOR CONTRACTOR	and in the second secon	ARC: U.A.	-80	annin 0		and the second	20 20
1. A		1200011030	wanter.	- Branching (197		(1444)	112 010
BIORISEH CARE			81	- Accession range		ACT.	10.00
(Dec)	Sec. 1	2-22	1.12				
		0.002.00	-824				

录入告警数据时,填写设备名称,告警数量和备注,其中记录时间默认值为当日,可重新选择时间,

点击<提交>后流程结束

😑 🛛 0.0800200700 / 20	STAR.		
录入告誓数据			
	- 2868		
	- 598		
	- (1991)200 2001-00-11		
	- Bit million		
		#2 N3	
			0

4.8 情报转事件工作流





在威胁信息共享模块,情报管理-情报列表页面中,选择一条情报,点击<转事件排查>,安全事件管理 模块的监控组成员在"待排查列表"中,选择该条事件进行排查,选择项目后,输入其他字段信息,点击 <提交>,事件创建完成,进入待研判状态。如果点击<误报>,则该事件进入到误报列表,工作流结束。

\∛CSO	BARRY BARRY BARD		
2全事件管理平台	事件提交		
ene 🖂			
minant	+ 1020 454b		
	+ 30-12-81,001	Microsoft Exchange Dever2018/11200/11200	
2590	- 814.2	TOP	
-		104	T MINNER
NO.11		1.07	
WHERE WE	* #11-021	#8 * #2 +0 10	
和田村市.	* 5(\$1)41	2027-04-20 09:20:83	
****	TE SPORTAL STRONG	W-Addistanting - T+WE	
20.00			
NHOR .	常新的内容者心和此前在心:	RIGELLER RITER	
815¥11		8 / = = =	
1911		Microsoft Exchange Tenver(1)(PCIGR)/TIER	
19788			
			- Ca
	2件:	上 上傳文內	
	自由 同於開始	Willison	
AICSO NERRINE	antes de	LAND MILLS	
			(abias)
			100 F 110
			manual a
	1	As As	The second secon
	/ .		anti-outra (manufacture) have
	200		
			Second 7 Description of the des
			advoca
		Plant V	
			101417 (MIRLDOW) FAM
	-		
			107907 (200000) 10800000
			A-0
			Toract (1) million in a second

研判组成员在待办任务的待认领列表新增研判任务,或者直接在事件管理平台的研判列表中选择该事



件,点击<研判>,进入事件平台进行研判操作,研判完成后待处置列表新增事件。

处置组成员在待办任务的待认领列表新增处置任务,或者直接在事件管理平台的处置列表中选择该事件,点击<处置>,进入事件平台进行处置操作。处置完成后已处置列表新增事件,工作流结束,结束后事件平台生成报告。

ASCSO MRERIEREO	129418	0990	100-100	5,637	80.000	117221 0 EF 0 E
						ntes
		.1	1 -		A .	94819 A
	100		A C	24	ABCC	insert (manipulation of ballion of
		O	MAT		120	
		-	C.			10-017 (#08000000) r##+F
		*1.48				
	-				*	TOPHT? LINNING CONTENSION
		-		2		
			-	/		1000007 (2498002 (2804960)
						Andres (1998)
						TOTAT? INVESTIGATION .

AICSO	un:		2
aa -	0	BAR (BODIER TEAC) INTERVIEW	Proc.
en eta l			
resid.			
18			
allong -		ruttat. Die ville	
÷ -		(1888) (1995)	a min
		owner B 1 = = D	
		18 C	



A®CS0				1 818217 () mit
安全争的管理中台	8-83 (0103) #89M			
-				
anes -		and the second second		
Alles -	-	Same .	singarii	91
10100	2005	TRACKS.	897-00.00 (TA16)	
assettes -	1000	amagin	age-solar tracket	190 Sam
awere	##820010am	N8104*15574025	and the second second	te es
	2007	234258	2210.0276144	
	+=20	annain.	202-00-00 (# 1000 F	Tel Cam
	+588	10412	and the second second	190 - 190
	2485	1241201	111-10-10 TEL:	1981 (1989)
	+====	1000050	202-00-00 1120-00	Tel an
	+588	104120	221-02-06-01-024	0
	2005	1.541294	auguran na riakowi	10.000

🖲 安恒信息



4.8.1 AiLPHA 告警转事件



AiLPHA 告警转事件工作流

AiLPHA 推送数据到安全运营平台后,事件管理平台监控组用户在"待排查列表"中,选择该条事件进行排查,选择项目后,输入其他字段信息,点击提交,事件创建完成,进入待研判状态。如果点击误报,则该事件进入到误报列表,工作流结束。

事件平台研判者角色的用户在待办任务的待认领中选择"AILPHA 指派了【网络防御运营管理平台】 的去事件平台研判的任务",并在事件平台进行研判。



事件平台处置者角色的用户在待办任务的待认领中选择"AILPHA 指派了【网络防御运营管理平台】 的去事件平台处置的任务",并在事件平台进行处置。



4.8.2 EDR 告警转事件工作流



EDR 推送告警后,事件平台监控组成员直接在"待排查列表"中,选择该条事件进行排查,选择项目 后,输入其他字段信息,点击提交,事件创建完成,进入待研判状态。如果点击误报,则该事件进入到误 报列表,工作流结束。研判和处置流程与"情报转事件"和"AILPHA 告警转事件"相似。



4.8.3 新系统上线评估



在 keyclock 平台进行用户配置。

注: 需要新增三个用户: 项目负责人、客户B、工程师;

A [®] CSO 安全运营	平台					4 Adres -
Acia e	用户					
with the second s						
V main	TOTAL TRACTAL	6 second				 anter anteri
10.000		181-10	0.790	 	80	- Local D
A Braile	10000 Tel. error. (al.) 4.1	ethe, illustration			3000	 849
AL 440						
E						
2 HE						
**						
(1) AP						
1.000						
= **						
- 10 MA						
TR: MAL						



添加用户, 输入用户手机号;

		AP 1 SURP			
	ALLE				
····································	100 C	物加州中			
····································	T Design				
A Arasettel A Arasettel <	0.000	1987			
AN	A NYMES	18/16/1	10200420070	输入手机号	
	= **				
Image: Construction Image: Construction					
	E 16/8/8	119			
and and waterstand 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	- 44	34.			
A M A THEND CO B M* A THEND CO O AB A THEND CO	-	m-antri	100		
	3.8		and the second sec		
O RM CREMPTOR OF 0 Data TO RA READING OF 0 C TO RA READING OF 0 C TO RA READING OF 0 C		A Parried U	1.1.1.1.1		
	0.000	68899-60.0	States,		
	0.00	1000	88-1		
	(1996)		1173 mm		
	(1) (44)		Based		

用户添加后,需要配置2个属性:fullname与phone;

fullname:项目负责人、工程师、客户 B;

phone:手机号码;

ASCSO 安全运营	平台		4
Ase +	m* - Manaza		
	13750708726 =		
1 milt	HE RS THE ADDRESS IN THE ADD BEEDFARES	8	
	(av	Table .	21
A. 87-9456	Share	10 ¹ 2	
0.48	per-	1010-000	
			disc.
E 1979-9			
4.44	100 100 I		
100			
1.00			
2 MA			
12 mm			





管理员在安全服务管理模块的工作计划配置模块,在实施阶段与规划阶段,新增"系统上线评估"任

务类型;

A8CS0				N LINE NO.	0.08
安全服务管理平台	83. 2000 - 2000BR				
ini - donie -	自定义工作计划类型				
Investe -	12917-88	2,360,65-454012	nati		
200 martine	• HELITHERE	- 注除年間	No.1578		
atorigi an	NYTH TO A	- 工作品名称	NUMBER BRANCH		
BATTE -	10.913M	- 111:0000	839,8,002	11	
osate -	在市场代表评估		RETAINTS MELTIN THINK PERFITS AN		
0.7462	009.116/742				
unitar	12/01/H		4.4 S		
1000L -	* NORTH				-
aurat -	ROULDERTS EDECH				0
and a	NORTH NO.				

注: 工作流编号来自"网络防御运营管理平台-编辑工作流-工作流列表-查看单条工作流-编号";





由项目负责人在安全服务管理模块,新建项目,并且新建项目后,需要添加成员工程师与客户B;

注: 在添加用户前, 工程师与客户 B 需要登录过安全服务管理模块

由项目负责人在项目管理-项目列表-文档管理-规划阶段-新系统上线评估,上传默认资产信息模板;

THE CONTRACT OFFICE					3	CREME	() ex
	=x11;m			×.			
SHE DELINE INST		O THEM	() into				
-		<u>a</u>					
	「二件実育」	#IRALIAIPS					
			8				
1000		****	ALM. BOOHLIN-TON D	2041			
111.00 Karte		ADDARD AND AND AND			. 29	ora 10	
-		1 3********				-	
177	815	ing. A set		-		100	
				1			•
	-						

文档上传成功后,右键"检查",点击 Network,刷新 (ctrl+R)界面,点击 page 查看 url 中的值 "/minioaicso/..../xlsx";

注:此值复制后,删除此文档;



AICS0	11.1111.2MB			(visite) (to	 Interests Cont Interests Cont	de Sanata Network • ■2 Ø (3) enertrop □ Desler • 2 ± Ø
16	2000				A I I A Ch ing Meth	e fort Doc W5 Masker Otar C Hasblockshookin
- 100					C Boowillegasts	
and the second s	ente sate a		-	metrorems	200 mai 400 mai 6	05 mi 000 res 1088 mi 1200 mi 1400 mi 1600 m
22000	1000					
Lense -				and the second second		
10*63	278. 00-	##A: 1961.	Tage over 1		have	· Handett Presser Weiperson Schutzer ·
- 1947	1110 1879	1000	201 a 10 10 10 10	29406	C second	<pre>v(imb+) 2004 duta: (records) [a=], total: i), message</pre>
-		man(F)	AX+PUTURU.		1 twe	wista: (tecords: [,-], tatal: 1]
- 100	248	■#31030	4341-48	87	tree	*0: (id: 104, name: "8)"01.0.00.0000.alms", or1:
liver -	1070-0400-0400-04	357926(A)	Cate-5	-	L[pape:	1dt 196
- 2404		FIRIT	Can+F			Later "Weith Later St.
and -		ARBITC),		PLA LET HAR		will "Attorney on 18100019/5144, to 4534244844 0007548811 010
steen -		Н леленить	#1			Total: 1
New -		副由中交 (第件)	ch			1000 Co. 100 C
-		REAL TRANSPORT	C10+0			
-		NUTRING .	Emelistrei	. 0	3725 maint: 14740/2020	
-					1 Conside	×

由项目负责人将 url 的值, 复制到工作流第一步"上传资产信息收集 Excel 文件-表单-

assetTemplet_uploadFile"中的默认值;



工作流用户任务的详情-代理人处,进行用户配置;

每个用户任务现在分配人是写死的,根据实际情况配置,本流程有3个角色,修改截图中的手机号即可;

输入<mark>\${system}:处理任务者的手机号码</mark>,如下图所示,每一个用户任务处都需要添加;



(1) 项目负责人:



(2) 工程师:



(3) 客户 B:





用户添加成功后,点击发布;



工作流发布后,在工作计划列表,选择此具体项目与任务类型,并填写相关内容后,点击<确认>,(也可以在项目管理-项目列表-工作计划-添加计划,选择任务类型"新系统上线评估",并且填写相关信息,点击<确认>后),则触发此工作流;



O COMPANY	zmirki X Ademak									****
任勢利表	1.1		1010-01		-1- <u>1</u> -1-	4	-			
week (-			
	(16.8		#1000	1419	100109-04220296					Aurts
1			(E84b)		18/54					
68.40	38.0423	11540	3 9981-039-039		IIII AARAA .		PEA.	ALL MALLER TO	81	
1.0	- BL2111	8-78.08	+ ((m.20)					1998		
1013.000 Http://doi.org/1011	1.041	10.00	SIND GR					1000		
Arrite-	THE	1100						(Tex.)	-	
1001	Statist A	477000				8.11		100		
1.20	1 August	areas a	1	1.64	annyarre .	458	410	1000		
areas.	1000	49.41		Are :		ACE.	1005	10000	88.40	
KORLA MEN Y	MAZINI .	ARM NO.	INARHA)		100030444	810	468	1000		
All and the second second	- Marre	NEWCAR		20.	2000	905	400	ALC: NO	88 300	
	- MARRIE A	- DOLLARD	20			812		Chinese,	22 23	
and down	Sec. 111	2708				10.0	-	1000		

指派到的具体用户,当此任务之间的任务完成时,就会在待办任务处接收到待办任务;





4.9 安全服务工作流

4.9.1 渗透测试服务



在安全服务管理模块,在安全服务阶段添加建立"渗透测试服务"计划类型的计划。

Ф снания	SHOUL MARKE								
务利表			, da d		1.1		1 . C		
Hards I was			10.031140				A DESCRIPTION OF		
Case -			- (010 am)		10-0285				
and the Party of the	100.0		ALCOHOL: UNK	759A	·····································				
			10888		+ Brit A		-		
	22.64		8812325		and states		44.	1975	. 87
	MACHIN	3-10.00	GREEN					-Base	20 20
288-1482	1967	ARRI	0.00110						-0.0 1.00
and *	1.11							1000	88.89
time .	(Maging	2-1223				10.00		DATE:	20 20
	191	ar-land	2	10	" and have	8108	100		22 40
BPLES.	1.000	49.61					-	(internal)	22 00
REPERSONAL CONTRACTOR	Mac100	1000103-004	interes)		10000000	8.08	1000	and a	20 80
	- HELEYAR	() PREPARE				857	10000	1000	310 400
atarasseries.	Barry	Dorigination	-814	47		8.02	410	1000	8.8 80
Address of the Owner	and the	-				8102	848		22 20
								Anis (I)	1 + 1 - 11 1 HAR .

计划添加成功之后,在工作台待办事项中上传渗透测试报告的附件,输入备注,点击<提交>,提交 成功之后流程结束。

C	可豆	信息
	DAS-SECUR	ity geog

化建造制成用品		
	-1468	
	1.108H	
	184. - Maria and	
		87

4.9.2 WEB 漏洞扫描服务



在安全服务管理模块,在安全服务阶段添加建立"WEB漏洞扫描服务"计划类型的计划。

			182821110							
		_	- 225-242		100002		-			
nen i en alte i i	(100 m)		W. Statements	10.03	eter/duyman	OBER -				-
			- 440 M PE		- miss,		-			
11 A.M.	(REAN)	101042	1000/1/12210-000		MINI MICH.		ier.		1.1.1	11 C
		(arrested	1 15.20 MINE					(000)	5.MR	-
R.R. Arrenter	1000		e-Ratrise					((SMC)		-
aler 1		0.488						100		-
M-	3880111	Arrithman and				8.8		1986		-
		473488		1.494	Includes.	310	100	(Dire)		
-188A	(111)	0.0.0.1			2010/01/1	400	300	(000)		100
10.0 K (0.0 K (0	situirre	SELLE SE	and the second s	- 88	TTO AND INC.	100	100	(bers)	-	-
Ewanes 🔛	992111	COALLE.					400	(2011)		
BALLBRAN HUNDS.	3802111	OCADE	10.1			210.	100	1994	22	-
nde-to-	000111	5A-1016		1004		320	910	10000		810
								with the state	1 4 4 4	a line

计划添加成功之后,在工作台待办事项中上传 web 漏洞扫描报告的附件,输入备注,点击<提交>,



提交成功之后流程结束。

hwtME同口遗经也		
	· 1408	
	1. 2 Miles	
	PR-0.1	

4.9.3 主机漏洞扫描服务



在安全服务管理模块,在安全服务阶段添加建立"主机漏洞扫描服务"计划类型的计划。

	_	3311	181						
este and					111171-001				
	-	- 40	10.000000000000000000000000000000000000	10.	*14085 ※北京各/二三、145868				
		- ()**	s#		*8/TA				
CR. MIN	and the second	HANKS.			888, 1, 825 A		e.,	- TERMONE	1011-
	metty	APPENDE - 1287	441					(1996)	
(C.A.) and (C.A.)	1997	DEAL NO.	enn					1000.	
teler-	THE	01909						1000	-
B A	Marris .	and the second				12.00	-		-
ali i		an-riterion		. 14	PAGE MARK		8.6.8		-
CTERRY.	105.0	1000 C		2.38	2022/06/1	(868.)	1010	(999)	(100.000.)
	matter				100.004	410	8408	(MPR)	-
Statement and	marri	CONTRACTOR .			and the second second		800	And.	-
Manager and Party of Street, or other	Matti	TRO-MARK		10	manager.	-	948	1000	
autors.	matth	0.105			100000-0	-	820	19441	100.000
								LINE PRO	1912 - Dia 1912



生影調測的自動解告			
	1.2 ⁴ 90		
	1.1000		
	182		
	48CH2		
		8.0 8.0	
	March 1	82 84	

4.9.4 基线核查扫描服务



在安全服务管理模块,在安全服务阶段添加建立"基线核查扫描服务"计划类型的计划。



计划添加成功之后,在工作台待办事项中上传基线核查扫描报告的附件,输入备注,点击<提交>,

提交成功之后流程结束。

-2.968		
A 2000		
841401		
	100 A.	
	88 B.A.	

4.9.5 弱口令扫描服务



在安全服务管理模块,在安全服务阶段添加建立"弱口令扫描服务"计划类型的计划。

杭州安恒信息技术股份有限公司



11110		_	MADD+90							_
							and a second			
CONTRACTOR DOCUMENTS	122		-386		- (+13#2)					-
tent a se anne s	C1008		A COLUMN TWO IS NOT		#####/(IIS,#C)+#	100-11				
			- (38-89)		+ BUTEA.					
CRAW.	20 M H	11045	and colors of the		(00,5)(27.5)		al A	iperta :	51	1 C
	MALLY .	0170310						288		-
ARR COMPANY		1000 C	0.40014				<u>c</u>	1000	100	80%
ARR-		8-95						254	-	min -
	matti					2.6	111	1004	-	asks (
	-	STREET.		5940	Hereit M.	882	-	(Dec.)	((ane)
P12551	THE .	4881		1.941				244		-
	manan	*****	*****		and the second	8005	205	(even		-
Table 17879	marris	HEATTHE		4.4		a and a second	4112	344	100	-
RIGHERSON AND A	matrix)	INCOME.		(44)	100000000000000000000000000000000000000		100	1004		3000 I
All and the second s	mates	21420		1941		(##28)	0.000	1000.0		NO.
								and the	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-

计划添加成功之后,在工作台待办事项中上传弱口令扫描报告的附件,输入备注,点击<提交>,提

交成功之后流程结束。

地球和中心地球出		
	- Tradition	
	1.1484	
	-81	
	40-41	

4.9.6 新系统上线安全评估服务





在安全服务管理模块,在安全服务阶段添加建立"新系统上线安全评估服务"计划类型的计划。

			(2211131						
6 % (057					C. LANSING				
	dina .		grant and a statement	112	THEFT / TOOL MARKS	Real-Case			-
			GREE		- 1012.5.				
A	and done	1042	ane-areas		americani, s		MA	marks	Case
	200111		- (24168)					1000	
N. 8 / / Proc. 810	100	100.00	10019				0.00	(Date)	-
112 ⁻¹		10.00						100	
194	mairie	are stated				2.2	-	1944	
ar (1000	armine.		414	202203(1)	100		1540	20.000
*4883	.)107.1	288.4			10000		10.00	1200.	100 001
ACCREMENT COL	Mail 11	ADD OVER	CRASHS .		and the second	855	848	(North	28 25
	marsi.	Chapter.				850	812		-
-Britsmannings	marrie .	Col. wated			Marriel 1	240	***	1000	23 100
REAL PROPERTY AND INCOME.	394101	311000			20100411	400	(400)	1000	100 000

计划添加成功之后上传新系统上线安全检查报告的附件,添加备注之后点击<提交>,提交成功之后

流程结束。

特别是现在是非常教育			
	and a second sec		
	(). Emp		
	- 44		
	1440-1461		
		10 m 1 m	

4.10 运营成熟度工作流



4.10.1 运营雷达评估



在安全服务管理模块,在运营成熟阶段添加建立"运营雷达评估"计划类型的计划。

O STRATE	HILLY C REMAIN								
务列表	<u>la de la c</u>	_	#10+10					de contra de la co	
CARGE STAT							1.00		
			· 2016-639		(interest				100000
TRUE & SH BARR 1	COLUMN COLUMN		6-20-0410	100	121031121222				and the second se
			100.00		1865.6				
	25.00	THRE	ana constrainte.		896-0014		ma.	104100	
	-	0-1008	- GRAN					(100	
\$1181-marks	1960		248UB					EDMAX.	
HHO?	1999							(1997)	10.00
1281	Marri	#-7811#				8.0		(1945)	FR FR
2.801	100	(0-70010)		<i>b</i> ,	2229864	895		Conv.	-
Deliver.		dentes.		1.0	manufactor -		100	(1962)	
AALLE MENT CO	100011	NUMPER OF			202000.	202		and a	98 8 8N
This is a list with the list	(82711)	(19440308			aniseties ((414)	22 24
ATRIAL COLORAD	Mag 144	-	10.0		2010/01/01	10.01.02		(MOR)	-

计划添加成功之后,输入雷达评估值,评估日期默认当天可自行修改,对安全运营、安全防护、暴露 面监测、威胁狩猎、应急响应进行评估。评估完成之后点击<提交>,流程结束。

注意:以上填数字:高级 (9~10)中级 (7~8)基础 (5~6)无效 (0~4)。高级:满足所有关键运营服务工作,能输出交付物;中级:满足最关键、中等关键的运营服务工作,能输出交付物;基础:只满足最关键的运营服务工作,能输出交付物; 无效:运营服务工作不能正常开展。

Contraction of the		-
	-P428	
	2014-01-00	
	1200	
	des-second	
	615P	
	and control of the second seco	
	441.00000	
	- altria	
	49.4898	
	- 5545	
	MELONAS .	
	24	
	a rest for a second sec	
	area a	

4.10.2 运营风险趋势



在安全服务管理模块,在运营成熟阶段添加建立"运营风险趋势"计划类型的计划。

的列表									
		_	18726240				-		
		_	-4880		- 110902				
SHARE REP. MAR 13	CHER		-	1000	22020-2120320-0	· · · · ·			- Barr
			10880		* p (B.A.				
Cheff.	(Calebra)	STERS.	100.000		Republic A		100	Shrip	
	And it is		- () (0.000					(Base)	
	1000	AMMA.	0.88129					1996	
MARCH .		(10.000))						Dett	
100	Marrie	or the second				10.0		(PARL)	
440	7822		1	54	(and the set	100	93.2	1000	
872851		area.			Description of a	100	810	(Married)	
	ADD:111	300,00,000	and the state of t	(344)	0.00000044	848	ALC:	CRAWLE .	10.00
HOLEH RE CO	0.00011	CONTRACTOR:			(manual)	100	8108	1999	1990 (B.M.
or Residences and	Barry		EA.	1777	Anna and a	800	*12	CANADA.	22 22
and the	Section.					100	****		22 23

杭州安恒信息技术股份有限公司



计划添加成功之后,填写每月风险趋势值。填写完成之后点击<提交>,流程结束。

ninesenin		
	- 4428	
	400-10-00	
	100002	
	am1.071200	

4.11 资产管理工作流

4.11.1 资产业务准入



管理员和 OPadmin 进入 os 启动页,点击右上角编辑工作流,进入工作流页面。选择业务准入流程的.bpmn,点击编辑,点击工作流的第一步,设置//环境变量,//设置安全管理员信息

设置'securityAdminId','ssmp:安全管理员的手机号,'securityAdminName','安全管理员姓名',点击部署, 二次弹窗确认之后,流程部署完成。





部署完成之后,点击安全服务管理模块,由需求人在任务列表中建立"业务准入"计划类型的计

划。

O SEMMINI II C	outer) another								
例表:					and the grant of the		- <u>1</u>	1	
			ann a				1		-1
	-		- UNAB		<11585 (11585)(1153823時)(1584	D			THEORY.
			- 108.058		- 昭谷人				
an a sea	4200	trunds.	204-122-010		(0021)0111		24	10405	3819
	(80011)		- (三谷 町町					(100.00)	20 000
ALC: NUMBER		HIGH.	11/640-1.8					(2007)	28.00
and the second se	1.000	1-10					- C.	1000	88 80
m4	maili					8.71	-	Carry .	
	1000		à	1.0	342 March 1	810		1998	2.8 10
-sea-	1000	STAL.		66		210	288	1000	MM (1000
ancie antes e 🛄	0.00000	Concerne	HERE BOARD		#252200 ·	WORL:	107		25.00
	0.0000111	THE OWNER WATCH					410	ingen.	10.00
Anterestates.	(9602111	cort, indete	-	17	and the second second	802	802	(merry)	20.01
and the second second				Ut		-	802	COME;	28 20

在工作台中的待办事项点击<创建申请>,进入申请新增资产页面。点击左侧列表右上角<+新增>,可 选择新增主机资产或新增应用资产。选择需要新增的资产类型,填写相关资产的信息,点击<确定>。



In the section of the			
1 94101-0001/F			
▲ 资产则表		💼 0-71+15	
		1 BW	
	arrests arrange, system	and when a starter matter	
		-62	
		241.110	
	6.10.0		
	#100+01	AV40 0.000 1.000 0.000	
	新增主机资产		×
	· 资产名称;	 : 西产责任人; 	
	 · 面产名称; · 面10入内司 	 资产量任人: (市)市内の 	
	 · 唐产名称; (副Q人内印) 	 资产重任人; 资选程内资 	
	 · 查产名称: · 面前(人)内部 · 业务系统名称: 	 资产重任人: 资选作内容 业务系统关制: 	
	· 查产名称: 图10入内码 · 业务系统名称: 通告保内有	 ・査产責任人: ・並务系統关目: ・ ・ ・	
	 · 查产名称: · 业务系统名称: · 通告保内的 · 伊地址: 	 ・ 留产重任人: ・ 並务系統笑知: ・ 近务系統笑知:	
	 · 查产名称: (面成入内间 · 业务系统名称: 请告诉内消 · P地址: · mx入内市 	 ・歯产重任人: ・並与系統英語: ・並与系統英語: ・適合応内容 ・適口: ・協口: もんのなどのなる目を加入下一个範囲 	
	 · 查产名称: (例6入片四) · 业务系统名称: 请告保户前 · 护地址: · 护地址: 	 · 置产重任人: ・並勞系統英語: ・並勞系統英語: ・適告時内容 ・適告時内容 ・適告時内容 ・適告時内容 ・適告時内容 ・適告時内容 ・ ・適告時内容 ・ ・	
	 · 查产名称: (例60人内容) · 业务系统名称: 请告母内育 · 护地址: : 请给人内容 · 设备类型: 	 一部产量任人: 第進即内容 ・业务系統英語: ・ 強気系統英語: ・ 適応: ・ 適応: ・ 適応: ・ 適応: ・ 適合型号: 	
	 · 查产名称: (面成入内码 · 业务系统名称: 请告保内消 · 护地址: 请张入内容 · 设备类型: · 遗告类型: 	 ・ 菌产量任人: ・ 並勞系統笑知: ・ 並勞系統笑知: ・ 満日: ・ 満日: ・ 満日: ・ 満日: ・ 満日: ・ 送各型号: ・ 送各型号: ・ 送各型号: ・ 送給型号: ・ 	
	 · 查产名称: · 业务系统名称: · 通告保内指 · 护地址: · 游输入内容 · 设备类型: · 通告师内容 · 语代系统: 	 ・ 唐产書任人: ・ 道秀系統英語: ・ 並秀系統英語: ・ 靖古洋内雷 ・ 靖山: ・ 靖山: ・ 靖山: ・ 靖山: ・ 遠子郎号: ・ 道子郎号: ・ 道子町号: 	
	 · 查产名称: (面較入內面 · 业务系统名称: (面当你內面 · 伊地址: (請較入內容 · 设备类型: (前出則內容 · 握作系统: · 输入内面后用由国生缺入下一个标签 	 ・ 唐产勇任人: ・ 由方系統英語: ・ 业方系統英語: ・ 満口: ・ 第二: ・ 第二: ・ 後名型号: ・ 造留厂句: ・ 设备厂句: ・ 遺留厂句: 	
	 · 資产名称: · 业务系统名称: · 清告保有許 · 伊地址: · 清告保有許 · 伊地址: · 清告保有許 · 设备接型: · 请告供告告 · 操作系统: · 输入与成后供告信年龄入下一个秘密 	 ・ 歯产量低入: ・ 业务系统关制:	
	 · 資产名称: · 业务系统名称: · 清告保有許 · 伊地址: · 伊地址: · 谢娘入汽音 · 设备类型: · 遗告操型: · 遗告操题: · 遗告操题: · 遗告操题: · 遗告操题: · 遗告并否在访问控制: 	 ・ 唐产垂任人: ・ 由产垂任人: ・ 由市田内内 ・ 小男系統笑知: ・ 第四: ・ 第四: ・ 第四: ・ 第四: ・ 後者型号: ・ 设备工写: ・ 设备工写: ・ 设备工写: ・ 设备工写: ・ 提番在线: 	
	 · 資产名称: · 业务系统名称: · 通告保内有 · 伊地址: · 伊地址: · 總依人內容 · 資格樂型: · 通告保内容 · 資格樂型: · 通告保内容 · 場件系统: · 場合系统: 	 ・ 唐产垂任人: ・ 由产垂任人: ・ 由予系統英語: ・ 地劳系統英語: ・ 靖田: ・ 靖田: ・ 埼山: ・ 御田: ・ 御	
	 · 資产名称: · 业务系統名称: · 市場公司有 · 伊地址: · 伊地址: · 滑級人内容 · 设备类型: · 過告申告 · 過告 · 當注: 	 ・ 唐产垂任人: ・ 由方系統关題: ・ 山方系統关題: ・ 靖西洋内府 ・ 靖田二: ・ 靖山二: ・ 岐音山二: ・ 岐山二: ・	
	 · 資产名称: · 业务系统名称: · 清告保有許 · 伊地祉: · 伊地祉: · 清告保有許 · 设备类型: · 通告保有許 · 设备类型: · 通告保有許 · 操作系统: · 小方式后后用注册主题》入下一个秘密 · 是百存在访问控制: · 备注: · 微达、 	 ・ 唐产垂任人: ・ 班劳系統关題: ・ 班劳系統关題: ・ 靖市洋内府 ・ 靖市二: ・ 靖市二: ・ 靖市二: ・ 靖市二: ・ 後者型号: ・ 设备型号: ・ 设备工号: ・ 设备工号: ・ 设备工号: ・ 设备工号: ・ 没备工号: ・ 没备工号: ・ 没备工号: ・ 没备工号: ・ 没备工号: ・ 提高在块: ・ 量 () 否 	
	 · 資产名称: · 业务系统名称: · 清告保有符 · 伊地址: · 清告保有符 · 设备类型: · 通告供表表: · 操作系统: · 输入内容后后当主题入下一个秘密 · 是否存在访问控制: · 备注: · 请职入内容 	 ・ 置产重任人: ・ 近方系統关目: ・ 近方系統关目: ・ 靖立洋内西 ・ 靖二: ・ 靖二: ・ 徐二: ・ 後者型号: ・ 読者型号: ・ 読者型型号: ・ 読者型型号: ・ 読者型号: ・ 読者型号: ・ 読者型号: ・ 読者型号: ・ 読者型型号: ・ 読者型号: ・ 読者型号: ・ 読者型号: ・ 読者型号: ・ 読者型号: ・ 読者型型号: ・	
	 · 查产名称: · 业务系统名称: · 油务系统名称: · 通告保有符 · 伊地址: · 谢敏入内容 · 设备类型: · 遗告类型: · 是吉存在访问控制: · 是吉存在访问控制: · 备注: · 请收入疗费 	 ・唐产重任人: ・由注目内町 (*) ・业务系統类印: ・資告符内市 (*) ・適口: ・協口: ・協口: ・協力に応応の市田年輸入下一个毎回 ・设备工事: ・设备工事: ・資告工味: ・提告在味: ・ 重 (*) 否 	
	 ・ 資产名称: ・ 业务系统名称: ・ 市場は合作者 ・ 伊地址: ・ 滑橋人内容 ・ 漫作系统: ・ 操作系统: ・ 地方用成后用由同年総入下一个核型 ・ 是否存在访问控制: 〇 二章 〇 否 ・ 备注: ・ 清除入内容 	 ・ 唐产書任人: ・ 班劳系統类部: ・ 第五称内容 ・ 端口: ・ 総合型号: ・ 総合型号:<td></td>	
	 ・ 歯产名称: ・ 业务系統名称: ・ 市地址: ・ 清助人内容 ・ 遺告供型: ・ 遺告供型: ・ 遺告供型: ・ 遺告供型: ・ 遺告供系统: ・ 操作系统: ・ 是否存在访问控制: ・ 是否存在访问控制: ・ 看注: ・ 備除人内容 	 ・ 唐产書任人: ・ 班劳系統笑明: ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	

"资产省称"	* 资产责任人:	
诸仙入内育	资选程内容	N
* 业务系统名称:	• 业务系统类别:	
透過排列時	~ 婚退理内容	
· 域名/URL:	• 阿站名称:	
雪喻人内容	清输入内容	
\$ 软件名称:	* 软件版本:	
唐输入内容	调输入内容	
是否存在访问控制;	* 是否在线:	
	0 単 0 吉	
- 是否阿站备室:		
0 是 0 百		
•备注:		
接触入内容		

填写完相应资产信息之后,左侧列表展示新增的资产数据。再填写申请详情,搜索选择部门负责 人,输入备注点击<提交>,弹出资产提交成功的提示。

资产提交成功之后,由部门负责人进入工作台审批报备的资产,可以查看所申请的资产列表数据。 选择审批意见<通过>或<不通过>,输入备注,点击<确定>。若部门负责人审批通过,则进入下一阶段由 安全管理员审批;若部门负责人审批不通过,则退回到申请阶段,由申请人重新填写并提交。

部门负责人审批通过之后,由安全管理员审批,可查看申请资产的详情。选择审批意见<通过>或<不通过>,输入备注,点击<确定>。若安全管理员审批通过,则申请的资产会录入DAS-VM弱点管理平台中,并生成文档,该文档需要进入我的任务中查看任务详情处下载,流程结束;若安全管理员审批不通过,则退回到申请阶段,由申请人重新填写并提交,部门负责人重新审批。

安恒信



O DAB-VM	-	n Contempor		1.000	-						THE ST. CONTRACTOR
. 3275	1.000	10.000									
artar-											
178*	91.50	10.010	879	-		e**	a		- 80-	dan cart	
a const	124.60	10000	- 1898HA	11111		1.010		14	< 184-	00.000	
a berthe	-										
	-										
		8718	879	8*22	120.2	****	8789.1	8742		A HEREN	80
		25.8*	100 TO 10 TO 10	sta		RECEIPTER	***				
		AND	100.002.0.7	519.	. 4	Repaired.	***	1.0		4	
		400.0	144 144 141	110	14	beyreast.	***				
		10210025	100,000,000	eets.	4	1011	108				
DAS-VM		in n conta		THEFT.		a tonic					100-01 1 120-0020
	and has	del caravierti	Contraction Sources	Service III	A CONTRACTOR OF	1270100					Market of March 199
 9-9795 	5768.1	Calify Street									
14530%	1 area		1745			1.44				-	
GROP .	1000										
(0.11.00.00)	3748	100000		1000.00		· · · ·	84 88				
4.8*51	-										
0.000											
	-	8748	APPER	8-12	140	PATR .	3402	a.m.		THEFT	315
	-	1 (202-	The large balls control .	10	1.1	ALL STREET	*11				11 11 11
		 	W-40-40-11;	104	2.4	ACCREATE					
		 Arrowings 	THEN PAYHS AND LOW, SHIEL	025	14	ACLESSES.	855				
		all us address	750 /101 114 3 K 248809-	1000	162	1000-100	1.10				
O without	-018	2010.0200694			28.0	1	1000	areanna an	22 1		1.0
							1-1-		-		
							14				
		Constant and	Anna Consecutor -					-			
umbre		Manager	in management						1		
2-12		100.000	10.00								
24.27		10000	The second second								G
					140	H THEF	1122610				
BAR BAS			and the second second			8	1042				

												.25	10.0					ant :						391	
													KOPA IN				3	11.10.77					-[76 8	3
	-	-	-		-		-						titule - h	-						- 24			-æ	• •	e. Al
2.80 1.98 7.803 No	1.1	(4) 	2 **						н С- 5 Р	19.8	hinar,	ž.	11.11			£13	87 111-0		H 夜		1 (1) 1 (1) 1 (1) 1 (1)	NRN NRN	8428E - 43 - 49 -	27 199220 1 84	P
arra ere	1 12.110 13.110	E LAAN PRN IN ZIL M	0 #11 80	1 84.42	antes antes a	6 5133 0124		1 18539 1844	1 101510 101525	874 6088	42,45 32	M MALER	91115 2.1.0	ERAR BR COAR	* 5.0 8.0 8.0 8.0 8.0 8.0 8.0 8.0 8.0 8.0 8	0 2144	*****	3 2+23	1 8484	0 666.08 2000043	1 N.) 10800	N 1731 843	43	\$111. (MAR)	
		an talk									rebéte	a titrij			SPC 8					-					

BARMIN



4.11.2 资产变更报备工作流



管理员和 OPadmin 进入 os 启动页,点击右上角编辑工作流,进入工作流页面。选择资产变更报备流程的.bpmn,点击编辑,点击工作流的第一步,设置//环境变量,//设置安全管理员信息

设置'securityAdminId','ssmp:安全管理员的手机号, 'securityAdminName','安全管理员姓名'后保存。


部署完成之后,点击安全服务管理模块,由需求人在任务列表中建立"资产变更"计划类型的计

刬。

添加计划		Х
* 项目名称	* 计划类型	
输入项目名称可选择项目,可多选	湖州移动测试流程 / 资产变更 🛛 🗸 🗸	
* 任务名称	* 执行人	
请输入任务名称	请输入执行人	
* 任务周期		
非周期任务 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>		
	取消	提交

计划创建成功之后,在工作台的待办事项处,点击<创建申请>。进入申请资产变更报备流程处,资 产列表分为主机资产和应用资产两个 tab 页,展示申请人名下的资产信息,分别为资产序号、资产名称、 资产类型标签、资产责任人、IP/字段、是否在线、是否存在访问控制、操作项下的<变更>和<查

杭州安恒信息技术股份有限公司



看>icon。

(1) 变更主机资产

点击需要变更信息的主机资产后的<变更>icon,进入变更主机资产详情页,修改需要变更的信息。点击确定之后,在列表处该条被修改的资产名称被高亮显示,点击<查看>,可查看具体被变更的信息,且被修改的字段会高亮显示。

· 推广省称:	• 通广黄征人	
	260	
业和意味的市	- 2-8 KiEWB	
用此上后系统律师	 Orma 	
1780	0286	
10.20156.68	One	
	白星市高	
已备供意	這注筆時	
25.0	· 368	
densie:	+ 28FR	
line (and second	来臣	
SEPRIMANN.	- 858:8	
8 a () a	8 # C #	
· W(生)		
	电关键 人名英格兰克 化乙烯酸	



透	产列表							
dat."	E-800*							
**	8780	a-#8	第四十 章 15人	#/#E	市地	WHEN	1819	
141	ODDAIL MORE AND	12.00	*01	10.20.114.69	Ж.		22	-
194	1.4 Alwayson	(1880)	463	3020.007.0		а.	68	-
121	±1388/96361	196	***	1020.107.02			22	28
ΰΰ	(omtail)	1000	8428	3333	=			
						171.2	10.8	- 104

资产证明			X
0304±8lqm4			
A BYREA REP. C	個個性的 2022-03-04 16:53-10		
把户关型 :	金明系統649:	业务系统关键	
385	用点业分析和成效用	1.3m Mrt	
PRIME	2842	运搬型号:	
10.20.156-60	#\$1#	201-62	
設備厂商	是否在地	重百件在成初日年:	
9 H	8	8	
INCO:	國作業的		
39.	lines emblore		
WE:			
	通用的な有事は実施にた公案はなみ门戸案	an.	

(2) 变更应用资产

点击需要变更信息的应用资产后的<变更>icon,进入变更应用资产详情页,修改需要变更的信息。点击确定之后,在列表处该条被修改的资产名称被高亮显示,点击<查看>,可查看具体被变更的信息,且被修改的字段会高亮显示。

×
* 窗产责任人:
893 ·
*业务系统类型:
アーカ公果病
• 网站名称:
www.3%ig0307.com
* 软件版本:
001
* 是否在线:
① 型 〇 否



变更资产信息完成之后,填写申请详情,搜索选择部门负责人和输入备注,点击提交之后确认二次 弹窗,提示资产变更报备提交成功。

提交成功之后,进入资产变更报备审批流程,列表展示被变更过的资产详情,由部门负责人选择审 批意见<通过>和<不通过>,输入备注,点击<确定>。若部门负责人审批通过,则进入下一阶段由安全管 理员审批;若部门负责人审批不通过,则退回到资产变更报备阶段,被变更的资产不保存,由申请人重 新填写并提交。



部门负责人审批通过之后,由安全管理员审批,可查看被变更资产的详情。选择审批意见<通过>或< 不通过>,输入备注,点击<确定>。若安全管理员审批通过,则变更的资产会在DAS-VM弱点管理平台 上同步修改,并生成文档,该文档需要进入我的任务中查看任务详情处下载,流程结束;若安全管理员 审批不通过,则退回到变更申请阶段,被变更的资产不保存,由申请人重新填写并提交,部门负责人重 新审批。

and the second second					_				
30.0						- 9105			
and a						8146	and the second second	8793	
100 m						1.11	17.0	APPA, 10.0110.00	
-			-		11.000	10100.1	100	10000	
- 1 C - 1	And and					1.0001701			
And Co.						- 9195			
	-					17811-		attille concerne	
		100	8722	1000				art	
		1.000			- Annalise and a	10000	design of the second		
	a hanne i	- al an inclusion			And Description in which the	8718			
	- Miller	1.000			-	1HIRKS			
	1 2010/00		4497		1000	40.1	A PRESS OF REAL PROPERTY.	TRANSPORTER TO A	
	-				-	-			
					Accessory.	- #038			
		And And And And			-	80 0		875.0 913A	
						-			
						mile			
2.000-14F	* 4110 - 111	a ang a pa	a a.1		*	8-14			
	and and the					- 101			
					1.0	9760, Q	deserve.	ansa	
						1942. 1		served on conversion	
100						2712	-	24890	
H	-								
100	Read of Lot of L	-	1000	100		- 9108			
		and and	200		Anna and	1100 B		PEAK ON-STR	
		Annual Street or other	_			atte a	and Revelation	#1. mm1	
	-	and the second sec				1000			
	1				Section and	1940		6409	
	julio-tu	-			annane a	1010062			
			1.000			80. 0	- Auguster etternet - ette	ett. 41.14	
	I DOCUMENT	- Announcements	- 199			0			
	and the second second	The Constant of the				< 1818.			
	-		1.77		-	10134	101148 108	r	an.
	-	-			and i	-	and Ballion		**
						(149 + H		1.1.1	100
					and the second s				

											HU1088/1	and the state of the	el-terri						1.00	e e		0 X
1	H		-	-		-		Q menu														ALME:
1	XX	1	1918			11	1 - 10		IT DO	100	#10		10	1	0. 1	-	1	nichti -	27	P		-
4	1.25	ieni Ieni		k (ar ei 112	- 0-	4. 1	1.10		Ban	an -	B. 1997	12.2	settic.	25 80	are a	6A 1888	the g	1 30 10 -	MIPROR.	WINKSON T		
	EME		2		- 10		1	3(97	nt.	-	87			Ric.		*7.8	10	222	618			-
jA3			1.5	$\sim f$	1630(1)	97																
1		4		N.S.	p	1.0	3.	1.2.		1	- da	18-	inter-	- 57	all a	. e.,		0	11.3.1		Ť	U.F
ŝ	报告行	ħ.	第22月間 1/語書台	PRM	80	保老典型	是合存至	日気湯市 約11条単	说著广展	· (2층)(8	操作系统	· 是自有 WEB等重	制品加加	网络老袍	是在力性	41	情况,机信 - 采和	※吉華保	20MB	欧件毛衔	软件原本	报费用
2	3.16			30.20.198	-73		4		金幣	101-68	Walk wind					11户系统	用过业务	i				202205
	王时			10151/395 301.13.6			*	WEB				景	301 12.6	100 con		办公系统		1	用	验疗者用1	001	302303
8																						
ŝ																						
1																						

4.11.3 资产退网工作流



管理员和 OPadmin 进入 os 启动页,点击右上角编辑工作流,进入工作流页面。选择资产退网流程 的.bpmn,点击编辑,点击工作流的第一步,设置//环境变量,//设置安全管理员信息

设置'securityAdminId','ssmp:安全管理员的手机号, 'securityAdminName','安全管理员姓名'后保存。



部署完成之后,点击安全服务管理模块,由需求人在任务列表中建立"资产删除"计划类型的计

划。

添加计划		×
* 项目名称 输入项目名称可选择项目,可多选	* 计划类型 湖州移动测试流程 / 资产删除 V	
* 任务名称	* 执行人	
请输入任务名称 *任务周期	请 搁入执行入	
非周期任务 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>		
	取消	提交

计划添加成功之后,工作台处点击<创建申请>,进入申请资产退网流程处。资产列表分为主机资产和应用资产两个 tab 页,展示申请人名下的资产信息,分别为资产序号、资产名称、资产类型标签、资产责任人、IP/字段、是否在线、是否存在访问控制、操作项下的<查看>icon。

杭州安恒信息技术股份有限公司



选中要删除的资产,主机资产和应用资产需要分别选择,请不要遗漏。选择完成之后填写申请详 情,搜索选择部门责任人,输入备注,点击提交,二次弹窗确认之后,弹出提示资产退网提交成功。

提交成功之后,进入资产退网审批流程,列表展示提交退网的资产详情,由部门负责人选择审批意 见<通过>和<不通过>,输入备注,点击<确定>。若部门负责人审批通过,则进入下一阶段由安全管理员 审批;若部门负责人审批不通过,则退回到资产退网申请阶段,由申请人重新填写并提交。

部门负责人审批通过之后,由安全管理员审批,可查看提交退网的资产详情。选择审批意见<通过> 或<不通过>,输入备注,点击<确定>。若安全管理员审批通过,则提交退网的资产会在 DAS-VM 弱点管 理平台上同步删除,并生成文档,该文档需要进入我的任务中查看任务详情处下载,流程结束;若安全 管理员审批不通过,则退回到退网申请阶段,由申请人重新填写并提交,部门负责人重新审批。

-	-		RA.	-	RH.	-	-	-	-	0.	mane											100	194	100 A	A.m.
Ê	1.1		m			-	11 - 1	C. 6	一個	= 4	be -	12 10 20	(i)	10	+	1	2		6- (b)	1 2	morei -	AT.	Q		
NN	10	101		1 4 -		٥.	<u>A</u> -	ŧ.	- 18	= 18	1.11	Elent	80 -	47 - 3/ 4	1.4	24982	業用 単行 務務式 -	CENTRE I	IEA BER	mit.	HR-	8,9080	RECORD		
1	199					κ.				1	时东方	d.	- 1	6.9			11 H		10,725			601			
à1			15	×	fr	Million	5																		
Æ	A.	1	×.	č		D	E				i.J		1.1				. M	1. N.	0	. p.	Q			Ť.	UT
1	「行音」	1	10歳百日	6 公用/码 9 把增加	194	捕兵	服务#	t.	是洛存在 话间拉制	· 一個供) 前況:	保务 各型	设备厂商	设备型制	1 维作系统	是否有 WEB得慮	域名/同面 地址	网站名称	是否为(京永任	(信息系统 条制)	- 信単規様 約和	是街等保	是咨问站	软件名称	拉件成单	报备日
2	#12			333	8				西	主机		亲国	XH-1	winttows						测试业务	ŝ.				81230
	808			https://	W140				唐						41	https://ww w.test.com	testiume			浙试业务 百律停汗					202203
		1																							



4.11.4 资产风险自查工作流



管理员和 OPadmin 进入 os 启动页,点击右上角编辑工作流,进入工作流页面。选择风险自查流程的.bpmn,点击编辑,点击工作流的第一步,设置//环境变量,//设置安全管理员信息

设置'securityAdminId','ssmp:安全管理员的手机号, 'securityAdminName','安全管理员姓名'后保存。



部署完成之后, 点击安全服务管理模块, 由需求人在任务列表中建立"资产风险自查"计划类型的



计划。

					1. 1. 1.					
列表			18101+31					1 1		
							and the second			
Ma B at Mile C	84.0		WARDON CONTRACTOR	04.6	· 计如何推动的 (另外网	2012				
			- URDE		* 845A					
man .	20140	101945	100,011 (0.00)		398.4.6/14		et.4.	(SHAD)	100	ŧ.
	384133	arrante	- (E8)408					1299		-
Real Property lies	清明:	0.000.	addited					1000	2882))
195	(1197) ((10,000))					-	1000		-
ma -	more	8				8:10	15 2	1000	-	-
14.7	100	Re-THERE			BELOWATE .	9428	8475	and a	-	-
10081		46.83				A122	450	1000		-
manager a manager and a manager	Inches of	Read to out	ALCONOME.		(The second state	853	853	Sec.	-	-
iter an 💼	matter	PERSONAL PROPERTY AND			Harman and the literature of t	-	2012	1000		-
COLORADOR DATE:	386011	- DOLWERS	-		and the second s	Water	8252	(Alter)		- /
AND CONTRACTOR OF CONTRACTOR O	38400	(areas) (400	Act	(max)		-

计划添加成功之后,工作台处点击<创建申请>,进入申请风险自查流程处。资产列表分为主机资产和应用资产两个 tab 页,展示申请人名下的资产信息,分别为资产名称、资产类型标签、资产责任人、IP/ 字段、是否在线、是否存在访问控制、操作项下的<查看>icon。

选中需要扫描的资产,输入备注,点击<提交>。二次弹窗确认之后,进入扫描页面,可返回工作台 等待扫描完成。



在工作台处点击<获取扫描结果>,若扫描失败,则流程直接结束。



若扫描完成,则可以点击创建工单,继续流程。

<申请风险自查流程	4. 9. 9	1. 1. 1.	A. K.	E L
-9				
		•		
		扫描完成		
		MILL #19		

点击<创建工单>,若被扫描的资产不存在漏洞,则提示"工单创建失败,无漏洞生成"进入安全管理员 审核流程。左侧展示漏洞列表,右侧展示申请详情的被扫描资产数和漏洞数。



🗧 🕑 semnita	i zwiel/s	CONTRACTOR OF CONTRACTOR	10 m							8855 ·-
< 风险自由流程器	國政結果审批									
📥 अव्ययम							10000	E fristume anna	NOVE.	1.681/289
li ases	8101	REAR	8469	P.186	2484	8845	89	82 1022		
			1					- 安全教師成業調整核		
								- 6 15 (1996) - 1995		
								-		
										0

安全管理员输入备注,点击<提交>,则流程结束,任务已完成。

若被扫描的资产存在未修复的漏洞,提示"创建并下发工单成功",则进入反馈整改结果流程。左侧漏洞 列表展示漏洞名称、漏洞等级、漏洞描述、资产名称、IP/域名、业务系统、处置结果、操作列的处置 icon,表头上方有批量处置功能。右侧展示右申请详情的被扫描资产数和漏洞数。

Θ	\$53885MIN	1. 2010/00	C BERRENALDA								
4	麗起刘表							(10.0)	10 DAHA Amet	RNEE.	1.441-888
	1000 C	-	and a	****	9/8E	2/886	51,005,00	1817		52	
	1014101-00%	-	OperAtel Open-	1030110246	10.20.21,00	01138	(New)	128	REPERT		
	Carriel MR.	-	OperStit Oper_	1022110,495	11211106	101+52		18	C Land		
	iperioritit.	-	family Spec-	11.201716.205	-1120.030	Net the			- 65		
	Operated BBR.	•	OperStill Stepes.	10,01110,485	162657.86	101138	***	410	106-110F		
	Specific BB -	-	Operation Street.	National Action	10000	101.154	++2	-	88 8.8		
	Second States	•	OperStill Opera-	1020106205	1010106	0113	New C	100			
	OWNERS.		CHRISTIA.	NUCCESSARY	HALTSN	0115		48			
	Successfill.		and the providence of the second	0000636	mat Pay	MALE N	+**				
	10-87 MBT.	-	urier##DAtes.	ALCONTAL AND	10.20.5736	1011130		hese.			
							E COL	- irs/m -			0

对漏洞进行处置,选择处置结果"整改""搁置""误报",填写处置建议。当处置结果为"整改"时,漏 洞状态变为待验证,当处置结果为"搁置"和"误报",漏洞状态变为搁置和误报。填写备注,点击<提



交>。进入安全管理员漏洞审核流程,对整改的待验证的漏洞进行复测,点击复测列表可以查看任务状态。若漏洞已修复,漏洞状态从待验证变为已修复,则审核提交后流程结束;若复测该漏洞未修复,漏 洞状态从待验证变为待修复,则审核提交后回退至反馈结果整改处,重新处置待修复的漏洞。

对搁置和误报的漏洞进行审核,选择审核结果"通过"和"不通过",通过的处置结果则提交后流程结束。若未通过则回退至反馈结果整改处,重新处置漏洞。

4 1	相同列表							-818	I	1 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	#10.8	- 16. 168
	ANO1		8764	e*sk	#/HZ	27165	心器放弃	1817	•			
	Gertlin Mitte		Operation (Operation	0.003734.445	10.0017.00	151.+36	++=	-		PARAMETER		
	0+0198	-	Operation (Operation	10.01.07.00, ±41	0003786	40.134		1.0				
	(antited).	-	Operation (Operation	10.2117 (41.225)	10203736	3107.33		105		The state of the second	Risel.	
	the life fills.	-	Operative (Operation	10.00196.28%	10.2037.00	werds.	-	- 1		1	,	
	(perfect 038).	-	OpenSH (Open-	10203736.285	10.0037-00	391738		1.4				
	Dwith the	-	Operative communication	REPORTED AN	11.01.07.00	-	ia.	1.04				
	circlare.		OFBBOSIS.	10.002199,4895	16263720	300030		(1,1)		NO SCHOOL		
	turnide.	=	annonie.	0.0310.003	10.20.07.88	1071.136	14	1.10		March Artis		
	STREEMENT.	-		11205730,3685	95255746	627.136	24	1.4				4

所有漏洞都处置审核完成之后, 输入备注, 点击<提交>, 风险自查流程结束。若存在复测未完成或未处

置完成的漏洞将无法提交。

KEINSSTATERIE		•	Canada Ma	中,將東部的漏洞,无	注档学工业)		11	
		1					📙 申请详情	
						ALC: NO.	资产数量	满则数量:
RHRS	# # \$#	IP/158	业务系统	現代に白	1819		1 御住:	9
Open658 (Open.,	10.20.57,66,主机	10,70,57,86	10000038	[.10962.]	100	2 .	风险自由方程	
Oper55H (Open.,	10.20.57.86,#85	10.20.57.86	城市大湖	48	110			
Open55M (Open.	10.2037.86, 384	10.20.57.06	城市大路	81	1010	##	長行教室:	建同时是
OpenISH (Open	10.20.57.86_主机	10.28.57.0E	城市大阪	相由	111	言句	1	3
OpenSSH (Open.,	10.20.57.86_#8%	10,20,57,96	城市大部	***	100		22	

