企业安全建设分享

--综合基准安全检测

程 冲
金山集团

北京 珠海 成都 大连 深圳 日本 马来西亚

目录

目录

- 背景介绍
  - 网络安全风险
  - 基础建设条件
  - 物力人力资源

目录

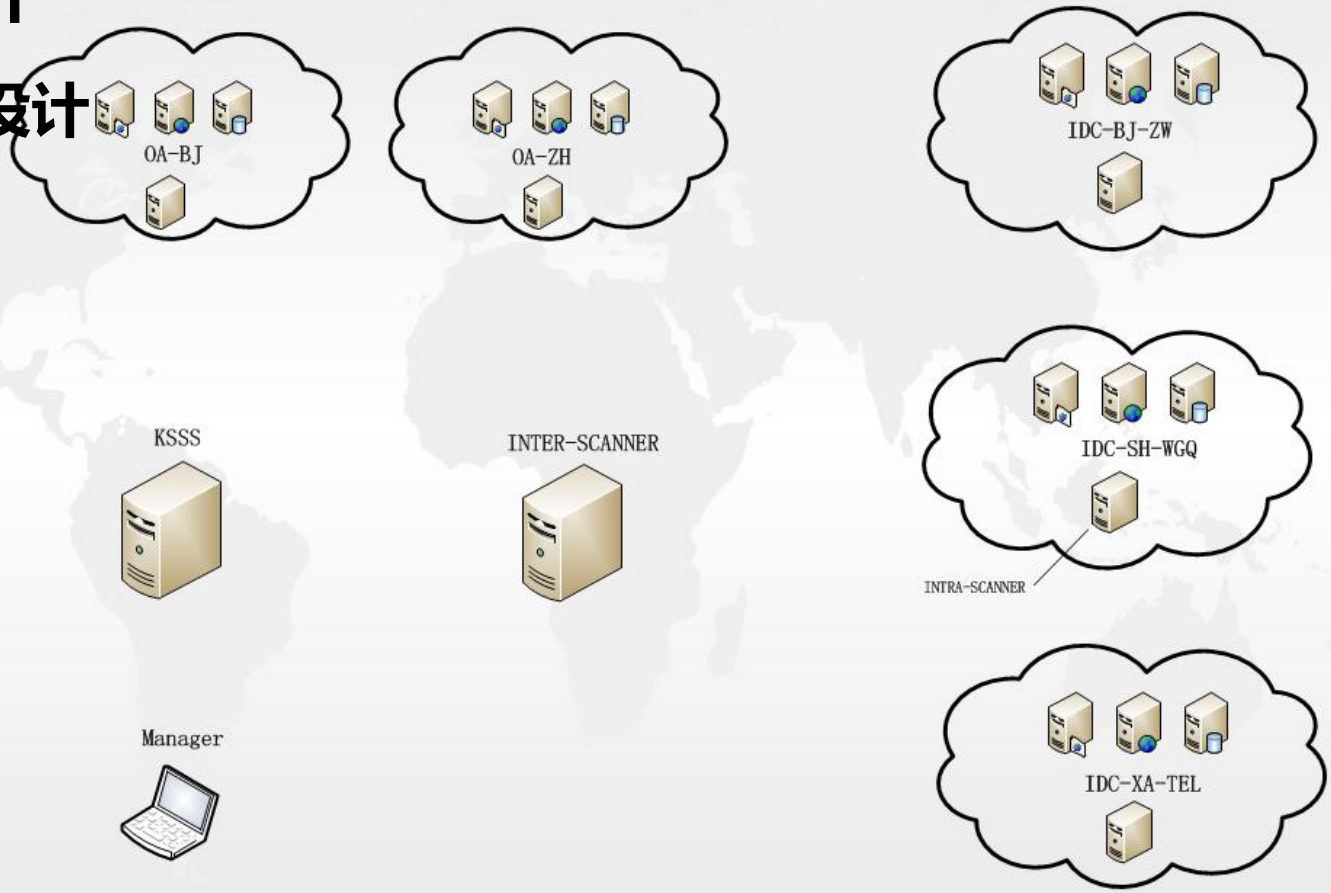
- 需求分析
  - 开放端口监控
  - 对外服务建档
  - 基础安全检查
  - 自动化流程化

目录

- 系统设计
  - 架构设计
  - 通信流程
  - 功能模块
  - 其它思考

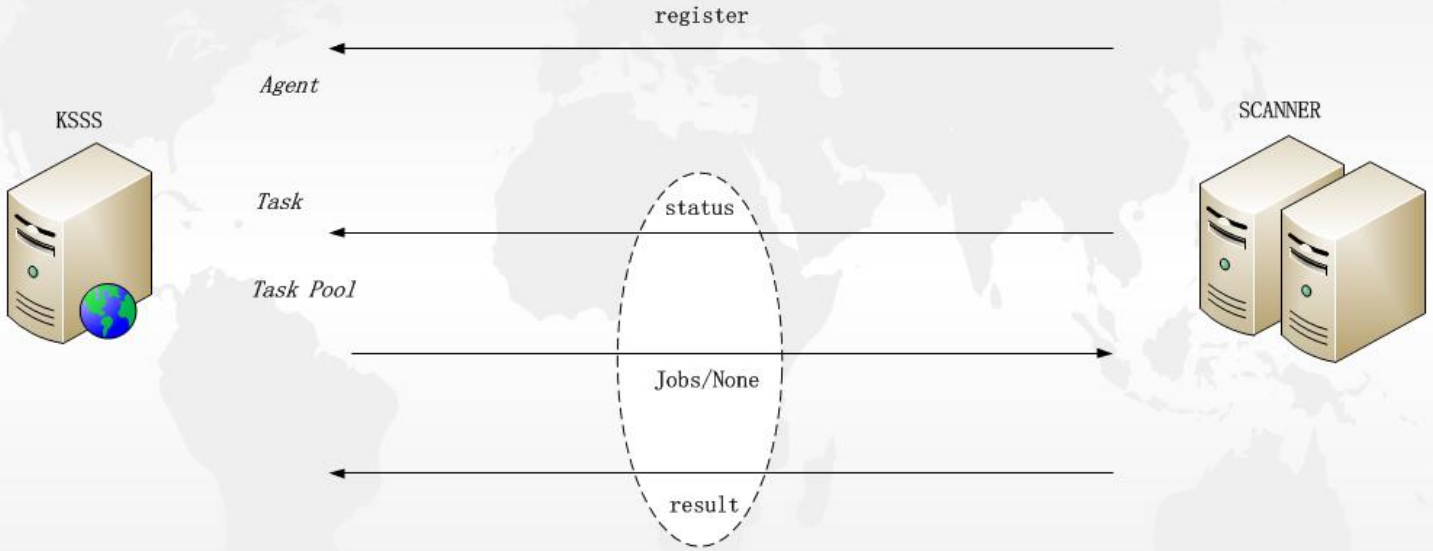
目录

- 系统设计
  - 架构设计



目录

- 系统设计
  - 通信流程



目录

- 系统设计
  - 功能模块
    - 对外开放端口扫描
    - 应用服务版本搜集
    - 网站威胁后台检测
    - 常规应用密码猜解
    - 业务端口服务建档

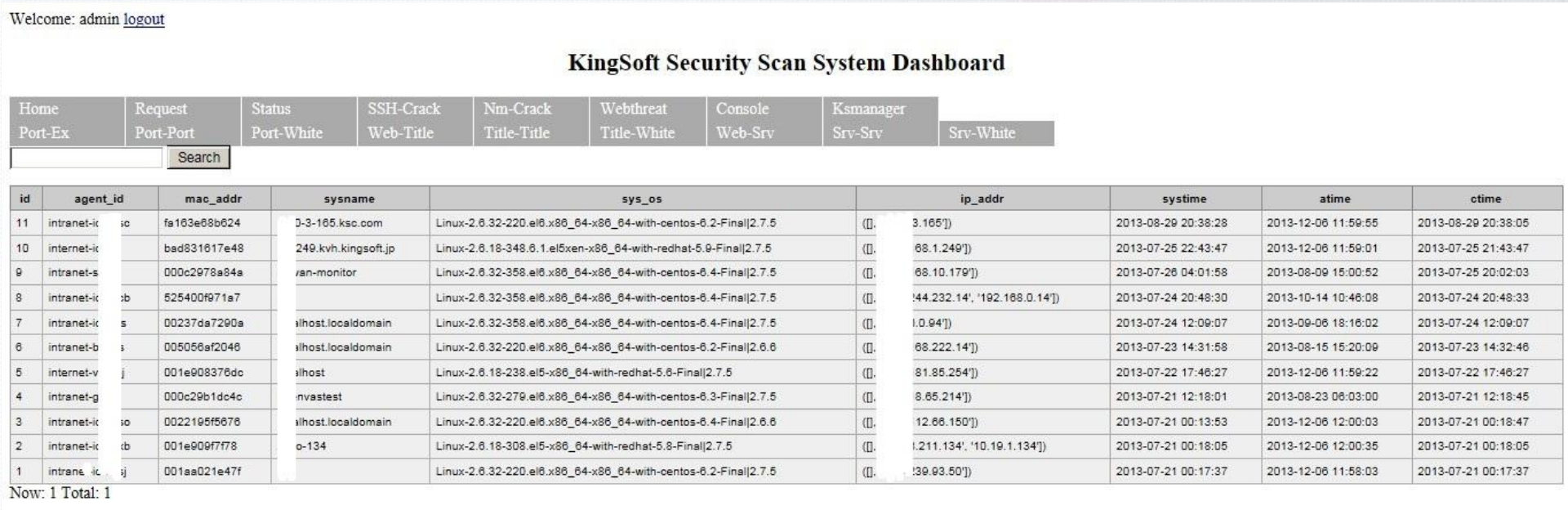
目录

目录

- 效果演示
  - 安全扫描系统节点
  - 业务端口服务建档
  - 网站威胁后台检测
  - 常规应用密码猜解
  - 任务集中管理界面

目录

- 效果演示
  - 安全扫描系统节点



Welcome: admin logout

KingSoft Security Scan System Dashboard

Home | Request | Status | SSH-Crack | Nm-Crack | Webthreat | Console | Ksmanager
Port-Ex | Port-Port | Port-White | Web-Title | Title-Title | Title-White | Web-Srv | Srv-Srv | Srv-White

Search

id	agent_id	mac_addr	sysname	sys_os	ip_addr	systime	atime	ctime
11	intranet-ic sc	fa163e68b624	0-3-165.ksc.com	Linux-2.6.32-220.el6.x86_64-x86_64-with-centos-6.2-Final|2.7.5	([]. 3.165'])	2013-08-29 20:38:28	2013-12-06 11:59:55	2013-08-29 20:38:05
10	internet-ic	bad831617e48	249.kvh.kingsoft.jp	Linux-2.6.18-348.6.1.el5xen-x86_64-with-redhat-5.9-Final|2.7.5	([]. 68.1.249'])	2013-07-25 22:43:47	2013-12-06 11:59:01	2013-07-25 21:43:47
9	intranet-s	000c2978a84a	van-monitor	Linux-2.6.32-358.el6.x86_64-x86_64-with-centos-6.4-Final|2.7.5	([]. 68.10.179'])	2013-07-26 04:01:58	2013-08-09 15:00:52	2013-07-25 20:02:03
8	intranet-ic cb	525400f971a7		Linux-2.6.32-358.el6.x86_64-x86_64-with-centos-6.4-Final|2.7.5	([]. 44.232.14', '192.168.0.14'])	2013-07-24 20:48:30	2013-10-14 10:46:08	2013-07-24 20:48:33
7	intranet-ic s	00237da7290a	alhost.localdomain	Linux-2.6.32-358.el6.x86_64-x86_64-with-centos-6.4-Final|2.7.5	([]. 0.94'])	2013-07-24 12:09:07	2013-09-06 18:16:02	2013-07-24 12:09:07
6	intranet-b s	005056af2046	alhost.localdomain	Linux-2.6.32-220.el6.x86_64-x86_64-with-centos-6.2-Final|2.6.6	([]. 68.222.14'])	2013-07-23 14:31:58	2013-08-15 15:20:09	2013-07-23 14:32:46
5	internet-v j	001e908376dc	alhost	Linux-2.6.18-238.el5-x86_64-with-redhat-5.6-Final|2.7.5	([]. 81.85.254'])	2013-07-22 17:46:27	2013-12-06 11:59:22	2013-07-22 17:46:27
4	intranet-g	000c29b1dc4c	nvastest	Linux-2.6.32-279.el6.x86_64-x86_64-with-centos-6.3-Final|2.7.5	([]. 8.65.214'])	2013-07-21 12:18:01	2013-08-23 06:03:00	2013-07-21 12:18:45
3	intranet-ic so	0022195f5676	alhost.localdomain	Linux-2.6.32-220.el6.x86_64-x86_64-with-centos-6.4-Final|2.6.6	([]. 12.66.150'])	2013-07-21 00:13:53	2013-12-06 12:00:03	2013-07-21 00:18:47
2	intranet-ic cb	001e909f7f78	o-134	Linux-2.6.18-308.el5-x86_64-with-redhat-5.8-Final|2.7.5	([]. 1.211.134', '10.19.1.134'])	2013-07-21 00:18:05	2013-12-06 12:00:35	2013-07-21 00:18:05
1	intrane ic sj	001aa021e47f		Linux-2.6.32-220.el6.x86_64-x86_64-with-centos-6.2-Final|2.7.5	([]. 39.93.50'])	2013-07-21 00:17:37	2013-12-06 11:58:03	2013-07-21 00:17:37

Now: 1 Total: 1

目录

效果演示

业务端口服务建档

id	agent_id	bu_name	host	port	name	product	version	extrainfo	systime	ctime	desc	admin	Action
6698	internet-vps-bj	b_kis_id	.46.35	80	http	nginx	1.0.11	n/a	2013-12-05 13:10:11	2013-12-05 13:10:12	infoc	周	
6899	internet-vps-bj	b_kis_id	.146.104	80	http	n/a	n/a	n/a	2013-12-05 13:17:18	2013-12-05 13:17:18	infoc	周	
6880	internet-vps-bj	b_kis_id	.146.105	80	http	n/a	n/a	n/a	2013-12-05 13:17:18	2013-12-05 13:17:18	infoc	周	
6710	internet-vps-bj	b_kis_id	53.37	80	http	Apache httpd	2.2.9	(Unix) DAV/2	2013-12-05 13:15:36	2013-12-05 13:15:37	样本交换	周	
6879	internet-vps-bj	b_kis_id	.146.103	80	http	n/a	n/a	n/a	2013-12-05 13:17:18	2013-12-05 13:17:18	infoc	周	
6874	internet-vps-bj	b_kis_id	.146.107	80	http	n/a	n/a	n/a	2013-12-05 13:17:18	2013-12-05 13:17:18	infoc	周	
6897	internet-vps-bj	b_kis_id	.146.155	80	http	n/a	n/a	n/a	2013-12-05 13:17:18	2013-12-05 13:17:18	infoc	周	
6909	internet-vps-bj	b_kis_id	.146.243	80	http	n/a	n/a	n/a	2013-12-05 13:17:18	2013-12-05 13:17:18	infoc	周	
7067	internet-vps-bj	b_xsj_id	.93.25	21	ftp	Serv-U ftpd	6.3	n/a	2013-12-05 14:55:29	2013-12-05 14:55:30	麻江仁[illegible]，需对外开放	周	
6290	internet-vps-bj	b_kis_id	.68.103	8080	http	Apache Tomcat/Coyote JSP engine	1.1	n/a	2013-12-05 12:55:19	2013-12-05 12:55:20	卫士开源社区	周	
6289	internet-vps-bj	b_kis_id	.68.103	80	http	nginx	1.0.5	n/a	2013-12-05 12:55:19	2013-12-05 12:55:20	卫士开源社区	周	
6419	internet-vps-bj	b_kis_id	.93.53	8080	http	Apache Tomcat/Coyote JSP engine	1.1	n/a	2013-12-05 12:59:15	2013-12-05 12:59:15	手机毒霸	周	
6418	internet-vps-bj	b_kis_id	.93.53	80	http	n/a	n/a	n/a	2013-12-05 12:59:15	2013-12-05 12:59:15	手机毒霸	周	
6496	internet-vps-bj	b_kis_id	.93.139	8080	http-proxy	n/a	n/a	n/a	2013-12-05 12:59:15	2013-12-05 12:59:15	[illegible]	姚	
6181	internet-vps-bj	b_kis_id	.67.82	80	http	nginx	1.3.7	n/a	2013-12-05 12:49:23	2013-12-05 12:49:23	游戏中心	黄	
6179	internet-vps-bj	b_kis_id	.67.75	80	http	nginx	1.3.7	n/a	2013-12-05 12:49:23	2013-12-05 12:49:23	游戏中心	黄	
6913	internet-vps-bj	b_ksp_it	.106.5	25	smtp	Microsoft Exchange smtpd	n/a	n/a	2013-12-05 13:30:04	2013-12-05 13:30:05	邮件服务器	孔	
6926	internet-vps-bj	b_ksp_it	.176.248	443	http	Microsoft IIS httpd	7.0	n/a	2013-12-05 13:53:37	2013-12-05 13:53:38	北京邮箱服务OutLookWeb	孔	
6925	internet-vps-bj	b_ksp_it	.176.248	80	http	Microsoft IIS httpd	7.0	n/a	2013-12-05 13:53:37	2013-12-05 13:53:37	北京邮箱服务OutLookWeb	孔	
6929	internet-vps-bj	b_ksp_it_	.176.240	8080	http	IronPort AsyncOS http config	n/a	glass 1.0; Python 2.6.4	2013-12-05 13:53:37	2013-12-05 13:53:38	用于同事自行查看邮件隔离区	孔	

目录

效果演示

网站威胁后台检测

id	agent_id	bu_name	url	eurl	title	bytes	rnum	code	systime	ctime
811	ternet-vps-	b_kis_idc_	http:/ .93.53:80/test/	http: .93.53:80/test/	n/a	1498	0	200	2013-12-05 22:32:27	2013-12-05 22:32:27
812	ternet-vps-	b_kis_idc_	http:/ .93.53:80/test	http: .93.53/test/	n/a	1498	1	200	2013-12-05 22:32:27	2013-12-05 22:32:27
813	ternet-vps-	b_kis_idc_	http:/ .93.29:80/test.php	http: .93.29:80/test.php	n/a	131	0	200	2013-12-05 22:32:27	2013-12-05 22:32:27
814	ternet-vps-	b_kis_idc_	http:/ .93.60:80/admin/login	http: .93.60/admin/login/	n/a	66	1	200	2013-12-05 22:32:27	2013-12-05 22:32:27
815	ternet-vps-	b_kis_idc_	http:/ .93.111:80/test.php	http: .93.111:80/test.php	n/a	26	0	200	2013-12-05 22:32:27	2013-12-05 22:32:27
816	ternet-vps-	b_kis_idc_	http:/ .93.113:80/info.php	http: .93.113:80/info.php	n/a	0	0	200	2013-12-05 22:32:27	2013-12-05 22:32:27
817	ternet-vps-	b_kis_idc_	http:/ .93.152:80/install/	http: .93.152:80/install/	phpcms	262	0	200	2013-12-05 22:32:27	2013-12-05 22:32:27
818	ternet-vps-	b_kis_idc_	http:/ .93.152:80/install	http: .93.152/install/	phpcms	262	1	200	2013-12-05 22:32:27	2013-12-05 22:32:27
819	ternet-vps-	b_kis_idc_	http:/ .93.226:80/test	http: .93.226:80/test	n/a	0	0	200	2013-12-05 22:32:27	2013-12-05 22:32:27
820	ternet-vps-	b_kis_idc_	http:/ .93.227:80/test	http: .93.227:80/test	n/a	0	0	200	2013-12-05 22:32:27	2013-12-05 22:32:27
821	ternet-vps-	b_kis_idc_	http:/ .93.248:80/test.php	http: .93.248:80/test.php	n/a	132	0	200	2013-12-05 22:32:27	2013-12-05 22:32:27
822	ternet-vps-	b_kis_idc_	http:/ .93.218:80/pma/	http: .93.218:80/pma/	n/a	5095	0	200	2013-12-05 22:32:27	2013-12-05 22:32:27

目录

- 效果演示
  - 常规应用密码猜解

id	agent_id	bu_name	host_port	user_pwd	systime	ctime
185	intranet	lan_b_kis_	4:22	root 6	2013-07-02 22:10:06	2013-07-02 22:05:45
186	intranet	lan_b_kis_	06:22	root 6	2013-07-02 22:10:06	2013-07-02 22:05:45
187	intranet	lan_b_kis_	02:22	root 6	2013-07-02 22:10:06	2013-07-02 22:05:45
188	intranet	lan_b_kis_	9:22	root 6	2013-07-02 22:10:06	2013-07-02 22:05:45
189	intranet	lan_b_kis_	05:22	root 6	2013-07-02 22:10:06	2013-07-02 22:05:45
183	intranet	lan_b_kis_	7:22	root 6	2013-07-02 21:21:19	2013-07-02 21:17:07
184	intranet	lan_b_kis_	8:22	root 6	2013-07-02 21:21:19	2013-07-02 21:17:07
177	intranet j	lan_b_ksp :	36.84:22	root ft	2013-06-29 20:35:13	2013-06-29 20:35:13
178	intranet j	lan_b_ksp :	36.101:22	root 6	2013-06-29 20:35:13	2013-06-29 20:35:13
179	intranet j	lan_b_ksp :	36.76:22	root 6	2013-06-29 20:35:13	2013-06-29 20:35:13
180	intranet j	lan_b_ksp :	36.91:22	root 6	2013-06-29 20:35:13	2013-06-29 20:35:13
181	intranet j	lan_b_ksp :	36.109:22	root ft	2013-06-29 20:35:13	2013-06-29 20:35:13
182	intranet j	lan_b_ksp :	36.92:22	king 3456	2013-06-29 20:35:13	2013-06-29 20:35:13
167	intranet j	lan_b_ksp :	35.110:22	root 6	2013-06-29 19:57:08	2013-06-29 19:57:08

目录

- 效果演示
- 任务集中管理界面

Welcome: admin logout

KingSoft Security Scan System Manager

Home | CIDR | IDC | BU | Module | Port_Rule | Threat_Rule | NmCrack_Rule | BU_Admin | Task | Task_Pool | Ksdashboard
White_Port | Black_Port | White_Title | Black_Title | Black_Threat | White_Srv | Black_Nmap | SSH_User | SSH_Pwd | FTP_User | FTP_Pwd | Mysql_User | Mysql_Pwd

agent_id: intranet-idc-.. bu_name: b_kso_idc_ ctime: 2013-12-05 16:03:58 Search task_status: Todo cidr:

task_module: task_time: 2013-12-05 16:03:58 port_ex_time: 2013-12-05 16:03:58 utime: 2013-12-05 16:03:58 cycle_status: No cycle_period:

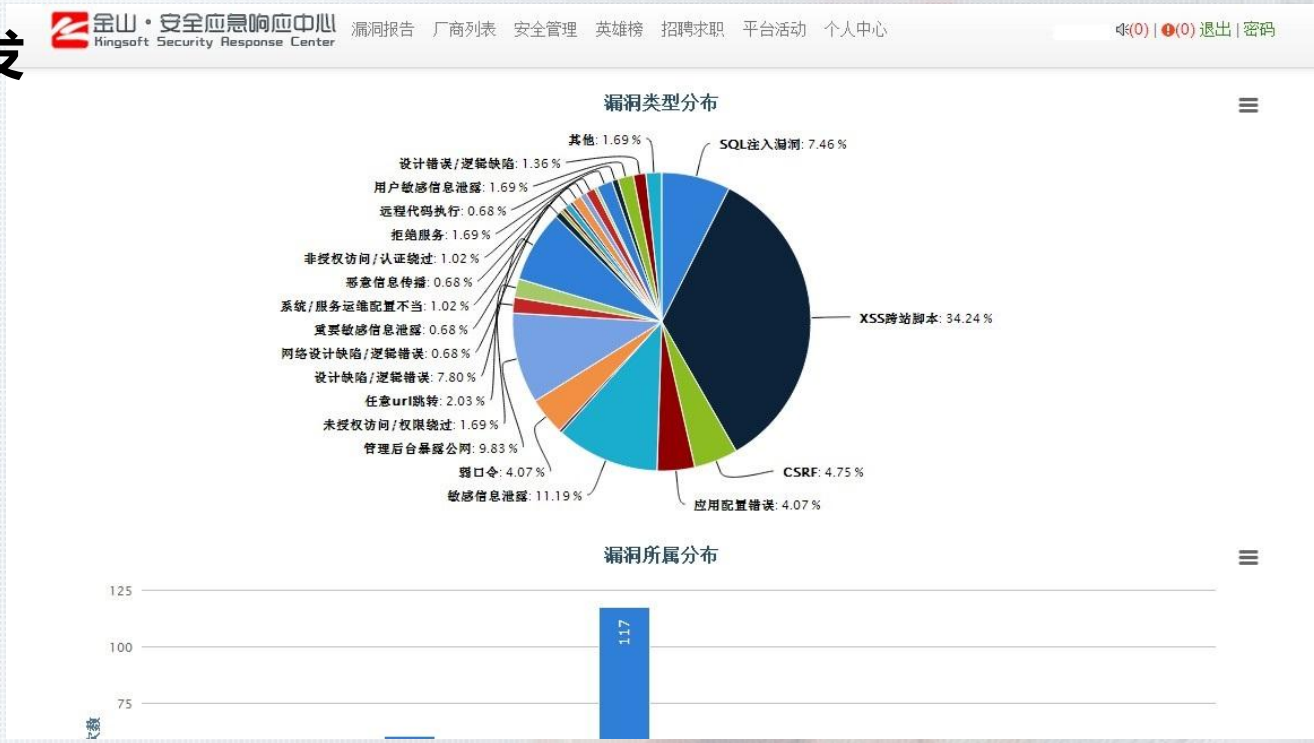
id	agent_id	bu_name	cidr	task_module	task_code	task_extra	task_time	port_ex_time	task_thread	black_status	task_status	cycle_period	cycle_status	task_desc	utime	ctime	Action
947	[redacted]	b_ksc_idc_	[redacted]61.0/24	kschk_port_ex	1	{'scan_port': 5L, 'scan_type': 1L}	2013-12-07 11:33:49	2013-12-06 11:33:49	30	Yes	Todo	24h	Yes		2013-12-06 11:33:49	2013-09-02 15:50:29	Encycle Disable
941	[redacted]	b_ksc_idc_	[redacted]61.0/24	kschk_web_title	2	{'scan_port': 1L, 'scan_type': 1L}	2013-12-07 09:09:54	2013-12-06 09:09:54	10	Yes	Todo	24h	Yes		2013-12-06 09:09:54	2013-09-02 15:39:43	Encycle Disable
940	[redacted]	b_ksc_idc_	[redacted]61.0/24	kschk_web_threat	3	{'scan_port': 1L, 'scan_type': 1L}	2013-12-06 19:21:19	2013-12-05 19:21:19	20	Yes	Todo	24h	Yes		2013-12-05 19:21:19	2013-09-02 15:39:33	Encycle Disable
938	[redacted]	b_xsj_idc_	[redacted]5.0/26	kschk_web_threat	3	{'scan_port': 1L, 'scan_type': 1L}	2013-12-07 09:15:40	2013-12-06 09:15:40	20	Yes	Todo	24h	Yes		2013-12-06 09:15:40	2013-08-09 10:32:06	Encycle Disable
937	[redacted]	b_xsj_idc_	[redacted]5.0/26	kschk_web_title	2	{'scan_port': 1L, 'scan_type': 1L}	2013-12-07 09:14:39	2013-12-06 09:14:39	20	Yes	Todo	24h	Yes		2013-12-06 09:14:39	2013-08-09 10:31:59	Encycle Disable
936	[redacted]	b_xsj_idc_	[redacted]5.0/26	kschk_port_ex	1	{'scan_port': 1L, 'scan_type': 1L}	2013-12-07 09:10:55	2013-12-06 09:10:55	50	Yes	Todo	24h	Yes		2013-12-06 09:10:55	2013-08-09 10:31:44	Encycle Disable
213	[redacted]	b_ksc_idc_	[redacted]9.76.0/24	kschk_port_ex	1	{'scan_port': 5L, 'scan_type': 1L}	2013-12-07 11:37:17	2013-12-06 11:37:17	50	Yes	Todo	24h	Yes		2013-12-06 11:37:17	2013-07-24 18:00:00	Encycle Disable
214	[redacted]	b_ksc_idc_	[redacted]9.75.0/26	kschk_port_ex	1	{'scan_port': 5L, 'scan_type': 1L}	2013-12-07 11:40:14	2013-12-06 11:40:14	50	Yes	Todo	24h	Yes		2013-12-06 11:40:14	2013-07-24 18:00:00	Encycle Disable

目录

- 下步计划
  - 与KSRC数据交互
  - 丰富基准安全检测
  - 单项深入安全检测

目录

- 下步计划
  - 与KSRC数据交互
    - 漏洞自动提交
    - 临时任务下发



目录

- 下步计划
  - 丰富基准安全检测
    - 应用探测与建档
      - whatweb
    - 针对性安全检测
      - bugscan

目录

- 下步计划
  - 单项深入安全检测
    - Web自动深入安全检测
    - 与系统安全扫描器对接

谢谢大家

chengchong@kingsoft.com
weibo：金山程冲