网络安全仿真验证环境建设及平台工具研发-电力工控自动化攻击验证工具项目概要设计方案功能比对偏差表

可研批复内容		软件需求内容		概要设计方案				说明
一级功能	二级功能	一级功能	二级功能	一级功能编号	一级功能	二级功能编号	二级功能	
	ARP欺骗嗅探攻击		ARP欺骗嗅探攻击	ECS01-MC01	网络层漏洞利用	ECS01-MC01-01	ARP欺骗嗅探攻击	
	DDOS轰炸攻击		DDOS轰炸攻击			ECS01-MC01-02	DDOS轰炸攻击	
	Smurf 攻击		Smurf 攻击			ECS01-MC01-03	Smurf 攻击	
	TCP SYN 泛洪攻击		TCP SYN 泛洪攻击			ECS01-MC01-04	TCP SYN 泛洪攻击	
	MAC 泛洪攻击漏洞利用信息查询		MAC 泛洪攻击漏洞利用信息查询			ECS01-MC01-05	MAC 泛洪攻击漏洞利用信息查询	
	http重定向攻击漏洞利用信息查询		http重定向攻击漏洞利用信息查询			ECS01-MC01-06	http重定向攻击漏洞利用信息查询	
	STP 重定向攻击							删除功能
	IP 重定向		IP 重定向			ECS01-MC01-07	IP 重定向	
	UDP泛洪攻击		UDP泛洪攻击			ECS01-MC01-08	UDP泛洪攻击	
	Land攻击漏洞利用信息查询		Land攻击漏洞利用信息查询			ECS01-MC01-09	Land攻击漏洞利用信息查询	
	Fraggle攻击漏洞利用信息查询		Fraggle攻击漏洞利用信息查询			ECS01-MC01-10	Fraggle攻击漏洞利用信息查询	
	DNS高速缓存污染					ECS01-MC01-11	DNS高速缓存污染信息查询	
	Rsync服务漏洞利用信息查询		Rsync服务漏洞利用信息查询	ECS01-MC02	端口服务漏洞攻击利用	ECS01-MC02-01	Rsync服务漏洞利用信息查询	
	支持Smb服务漏洞利用信息查询		支持Smb服务漏洞利用信息查询			ECS01-MC02-02	支持Smb服务漏洞利用信息查询	
	NFS服务漏洞利用信息查询		NFS服务漏洞利用信息查询			ECS01-MC02-03	NFS服务漏洞利用信息查询	
	Samba服务漏洞利用信息查询		Samba服务漏洞利用信息查询			ECS01-MC02-04	Samba服务漏洞利用信息查询	
	LDAP协议漏洞利用信息查询		LDAP协议漏洞利用信息查询			ECS01-MC02-05	LDAP协议漏洞利用信息查询	
	Pcanywhere服务漏洞利用					ECS01-MC02-06	Pcanywhere服务漏洞利用信息查询	
	ftp服务漏洞利用信息查询		ftp服务漏洞利用信息查询			ECS01-MC02-07	ftp服务漏洞利用信息查询	
	SSH服务漏洞利用信息查询		SSH服务漏洞利用信息查询			ECS01-MC02-08	SSH服务漏洞利用信息查询	
	Telnet服务漏洞利用信息查询		Telnet服务漏洞利用信息查询			ECS01-MC02-09	Telnet服务漏洞利用信息查询	
	Windows远程连接漏洞利用信息查询		Windows远程连接漏洞利用信息查询			ECS01-MC02-10	Windows远程连接漏洞利用信息查询	
	VNC服务漏洞利用漏洞利用信息查询		VNC服务漏洞利用漏洞利用信息查询			ECS01-MC02-11	VNC服务漏洞利用漏洞利用信息查询	
	IIS服务漏洞利用信息查询		IIS服务漏洞利用信息查询			ECS01-MC02-12	IIS服务漏洞利用信息查询	
	Tomcat/Nginx漏洞利用信息查询		Tomcat/Nginx漏洞利用信息查询			ECS01-MC02-13	Tomcat/Nginx漏洞利用信息查询	
	WebLogic漏洞利用信息查询		WebLogic漏洞利用信息查询			ECS01-MC02-14	WebLogic漏洞利用信息查询	
	Jboss漏洞利用信息查询		Jboss漏洞利用信息查询			ECS01-MC02-15	Jboss漏洞利用信息查询	
	Websphere漏洞利用信息查询		Websphere漏洞利用信息查询			ECS01-MC02-16	Websphere漏洞利用信息查询	
	GlassFish漏洞利用					ECS01-MC02-17	GlassFish漏洞利用信息查询	
	Jenkins漏洞利用信息查询		Jenkins漏洞利用信息查询			ECS01-MC02-18	Jenkins漏洞利用信息查询	
	Resin漏洞利用信息查询		Resin漏洞利用信息查询			ECS01-MC02-19	Resin漏洞利用信息查询	
	Jetty漏洞利用信息查询		Jetty漏洞利用信息查询			ECS01-MC02-20	Jetty漏洞利用信息查询	
	Lotus漏洞利用信息查询		Lotus漏洞利用信息查询			ECS01-MC02-21	Lotus漏洞利用信息查询	
	SQL-Server数据库漏洞利用信息查询		SQL-Server数据库漏洞利用信息查询			ECS01-MC02-22	SQL-Server数据库漏洞利用信息查询	
	MySQL数据库漏洞利用信息查询		MySQL数据库漏洞利用信息查询			ECS01-MC02-23	MySQL数据库漏洞利用信息查询	
	Oracle数据库漏洞利用信息查询		Oracle数据库漏洞利用信息查询			ECS01-MC02-24	Oracle数据库漏洞利用信息查询	
	PostgreSQL数据库漏洞利用信息查询		PostgreSQL数据库漏洞利用信息查询			ECS01-MC02-25	PostgreSQL数据库漏洞利用信息查询	
	MongoDB数据库漏洞利用信息查询		MongoDB数据库漏洞利用信息查询			ECS01-MC02-26	MongoDB数据库漏洞利用信息查询	
	Redis数据库漏洞利用信息查询		Redis数据库漏洞利用信息查询			ECS01-MC02-27	Redis数据库漏洞利用信息查询	
	Sybase数据库漏洞利用信息查询		Sybase数据库漏洞利用信息查询			ECS01-MC02-28	Sybase数据库漏洞利用信息查询	
	DB2数据库漏洞利用信息查询		DB2数据库漏洞利用信息查询			ECS01-MC02-29	DB2数据库漏洞利用信息查询	
	SMTP协议漏洞利用信息查询		SMTP协议漏洞利用信息查询			ECS01-MC02-30	SMTP协议漏洞利用信息查询	
	POP3协议漏洞利用信息查询		POP3协议漏洞利用信息查询			ECS01-MC02-31	POP3协议漏洞利用信息查询	
	IMAP协议漏洞利用信息查询		IMAP协议漏洞利用信息查询			ECS01-MC02-32	IMAP协议漏洞利用信息查询	
	DNS服务漏洞利用信息查询		DNS服务漏洞利用信息查询			ECS01-MC02-33	DNS服务漏洞利用信息查询	
	DHCP服务漏洞利用信息查询		DHCP服务漏洞利用信息查询			ECS01-MC02-34	DHCP服务漏洞利用信息查询	

迅捷PDF编辑器

	SNMP协议漏洞利用信息查询		SNMP协议漏洞利用信息查询			ECS01-MC02-35	SNMP协议漏洞利用信息查询	
	Hadoop文件服务漏洞利用信息查询		Hadoop文件服务漏洞利用信息查询			ECS01-MC02-36	Hadoop文件服务漏洞利用信息查询	
	Zookeeper服务漏洞利用信息查询		Zookeeper服务漏洞利用信息查询			ECS01-MC02-37	Zookeeper服务漏洞利用信息查询	
	Zabbix服务漏洞利用信息查询		Zabbix服务漏洞利用信息查询			ECS01-MC02-38	Zabbix服务漏洞利用信息查询	
	elasticsearch服务漏洞利用信息查询		elasticsearch服务漏洞利用信息查询			ECS01-MC02-39	elasticsearch服务漏洞利用信息查询	
	memcache服务漏洞利用信息查询		memcache服务漏洞利用信息查询			ECS01-MC02-40	memcache服务漏洞利用信息查询	
	Linux R服务漏洞利用							整合重复功能
	RMI漏洞利用					ECS01-MC02-41	**RMI漏洞利用信息查询**	
	Rsync服务漏洞利用信息查询		Rsync服务漏洞利用信息查询			ECS01-MC02-42	Rsync服务漏洞利用信息查询	
Web渗透攻击	Xss攻击信息查询	Web渗透攻击	Xss攻击信息查询	ECS01-MC03	Web渗透攻击	ECS01-MC03-01	Xss攻击信息查询	
	基于时间的sql注入攻击		基于时间的sql注入攻击			ECS01-MC03-02	基于时间的sql注入攻击**信息查询**	
	基于错误的sql注入攻击		基于错误的sql注入攻击			ECS01-MC03-03	基于错误的sql注入攻击**信息查询**	
	布尔型sql注入攻击		布尔型sql注入攻击			ECS01-MC03-04	布尔型sql注入攻击**信息查询**	
	Stack型sql注入攻击					ECS01-MC03-05	**Stack型sql注入攻击信息查询**	
	基于windows的命令执行攻击					ECS01-MC03-06	**利用windows的命令执行攻击的信息查询**	
	基于linux的命令执行攻击					ECS01-MC03-07	**利用linux的命令执行攻击的信息查询**	
	绕过前端js校验的文件上传攻击		绕过前端js校验的文件上传攻击			ECS01-MC03-08	绕过前端js校验的文件上传攻击	
	绕过后端文件名校验的文件上传攻击		绕过后端文件名校验的文件上传攻击			ECS01-MC03-09	绕过后端文件名校验的文件上传攻击	
	绕过后端文件类型校验的文件上传攻击		绕过后端文件类型校验的文件上传攻击			ECS01-MC03-10	绕过后端文件类型校验的文件上传攻击	
	绕过后端文件内容校验的文件上传攻击		绕过后端文件内容校验的文件上传攻击			ECS01-MC03-11	绕过后端文件内容校验的文件上传攻击	
Apt攻击	钓鱼邮件链接攻击	Apt攻击	钓鱼邮件链接攻击	ECS01-MC04	Apt攻击	ECS01-MC04-01	钓鱼邮件链接攻击	
	利用链接的显示与实际不同进行欺骗攻击		利用链接的显示与实际不同进行欺骗攻击			ECS01-MC04-02	利用链接的显示与实际不同进行欺骗攻击	
	利用近似URL来进行欺骗攻击		利用近似URL来进行欺骗攻击			ECS01-MC04-03	利用近似URL来进行欺骗攻击	
	伪造邮件发送方进行欺骗攻击		伪造邮件发送方进行欺骗攻击			ECS01-MC04-04	伪造邮件发送方进行欺骗攻击	
	利用子域名伪造邮件进行欺骗攻击		利用子域名伪造邮件进行欺骗攻击			ECS01-MC04-05	利用子域名伪造邮件进行欺骗攻击	
	报警类型的历史数据统计		报警类型的历史数据统计			ECS01-MC04-06	报警类型的历史数据统计	
系统管理	用户名和密码联合验证	系统管理	用户名和密码联合验证	ECS01-MC05	系统管理	ECS01-MC05-01	用户名和密码联合验证	
	登录失败尝试次数限制		登录失败尝试次数限制			ECS01-MC05-02	登录失败尝试次数限制	
	添加用户		添加用户			ECS01-MC05-03	添加用户	
	删除用户		删除用户			ECS01-MC05-04	删除用户	
	修改密码		修改密码			ECS01-MC05-05	修改密码	
	修改用户权限		修改用户权限			ECS01-MC05-06	修改用户权限	
	授权文件生成							删除功能
	授权文件导入							删除功能
	授权文件匹配							删除功能
	检测终端重启					ECS01-MC05-07	**检测终端上线状态**	
	检测终端关机		检测终端关机			ECS01-MC05-08	**检测终端离线状态**	
	检测终端自学习							
	调试开关开启与关闭					ECS01-MC05-09	**支持终端调试日志开关开启与关闭**	
	检测终端报警日志开关		检测终端报警日志开关			ECS01-MC05-10	**支持终端报警日志开关开启与关闭**	
系统配置	获取检测终端IP地址的配置信息	系统配置	获取检测终端IP地址的配置信息	ECS01-MC06	系统配置	ECS01-MC06-01	获取检测终端IP地址的配置信息	
	检测终端配置信息备份与恢复		检测终端配置信息备份与恢复			ECS01-MC06-02	检测终端配置信息备份与恢复	
	管理平台配置信息备份与恢复		管理平台配置信息备份与恢复			ECS01-MC06-03	管理平台配置信息备份与恢复	
	恢复出厂设置		恢复出厂设置			ECS01-MC06-04	恢复出厂设置	
总体情况：								

试读PDF结束

网络安全仿真验证环境建设及平台工具研发-电力工控入侵检测工具项目概要设计方案功能比对偏差表

可研批复内容		软件需求内容		概要设计方案				说明
一级功能	二级功能	一级功能	二级功能	一级功能编号	一级功能	二级功能编号	二级功能	
	网络适配器的获取	数据采集	网络适配器的获取	ECS03-MC01	数据采集	ECS03-MC01-01	网络适配器的获取	
			网络适配器的选择				~~网络适配器的选择~~	
	支持分布式流量镜像		支持分布式流量镜像			ECS03-MC01-02	支持分布式流量镜像	
			支持零拷贝网络抓包				~~支持零拷贝网络抓包~~	
	协议流量队列的构建	协议解析	协议流量队列的构建	ECS03-MC02	协议解析	ECS03-MC02-01	协议流量队列的构建	
			协议流量队列的维护				~~协议流量队列的维护~~	
	协议解析队列的构建		协议解析队列的构建			ECS03-MC02-02	协议解析队列的构建	
			协议解析队列的维护				~~协议解析队列的维护~~	
	通用五元组解析		通用五元组解析			ECS03-MC02-03	通用五元组解析	
	ICMP协议识别		ICMP协议识别			ECS03-MC02-04	ICMP协议识别	
	FTP协议识别		FTP协议识别			ECS03-MC02-05	FTP协议识别	
	SNMP协议识别		SNMP协议识别			ECS03-MC02-06	SNMP协议识别	
	自定义通用协议识别		自定义通用协议识别			ECS03-MC02-07	自定义通用协议识别	
	Modbus协议识别		Modbus协议识别			ECS03-MC02-08	Modbus协议识别	
	S7协议识别		S7协议识别			ECS03-MC02-09	S7协议识别	
	IEC104协议识别					ECS03-MC02-10	IEC104协议识别	
	DNP3协议识别		DNP3协议识别			ECS03-MC02-11	DNP3协议识别	
	OPC协议识别		OPC协议识别			ECS03-MC02-12	OPC协议识别	
	goose协议识别					ECS03-MC02-13	goose协议识别	
	mms协议识别					ECS03-MC02-14	mms协议识别	
	sv协议识别					ECS03-MC02-15	sv协议识别	
	FINS协议识别					ECS03-MC02-16	FINS协议识别	
	CIP协议识别					ECS03-MC02-17	CIP协议识别	
	BACnet协议识别					ECS03-MC02-18	BACnet协议识别	
	自定义工控协议识别					ECS03-MC02-19	自定义工控协议识别	
	Modbus协议深度解析（指令、地址		Modbus协议深度解析（			ECS03-MC02-20	Modbus协议深度解析（指令、地址、值域）	
	S7协议深度解析（指令、地址、值		S7协议深度解析（指令			ECS03-MC02-21	S7协议深度解析（指令、地址、值域）	
	DNP3协议深度解析（指令、地址、		DNP3协议深度解析（指			ECS03-MC02-22	DNP3协议深度解析（指令、地址、值域）	
	IEC104协议深度解析（指令地址值					ECS03-MC02-23	IEC104协议深度解析（指令地址值域）	
	goose协议深度解析（指令地址值域					ECS03-MC02-24	goose协议深度解析（指令地址值域）	
	mms协议深度解析（指令地址值域）					ECS03-MC02-25	mms协议深度解析（指令地址值域	
	sv协议深度解析（指令地址值域）					ECS03-MC02-26	sv协议深度解析（指令地址值域）	
	OPC协议深度解析（指令）		OPC协议深度解析（指令			ECS03-MC02-27	OPC协议深度解析（指令）	
		流量特征提取	流量周期特征值提取	~~ECS03-MC03~~	~~流量特征提取~~	~~ECS03-MC03-01~~	~~流量周期特征值提取~~	
			流量带宽特征值提取			~~ECS03-MC03-02~~	~~流量带宽特征值提取~~	
			流量会话时间间隔特征			~~ECS03-MC03-03~~	~~流量会话时间间隔特征提取~~	
			自定义流量特征提取			~~ECS03-MC03-04~~	~~自定义流量特征提取~~	
			网络会话的源、目的IP			~~ECS03-MC04-01~~	~~网络会话的源、目的IP特征值提取~~	

试读PDF请在线

数据采集		网络会话特征提取	网络会话的源、目的端	~~ECS03-MC04~~	~~网络会话特征提取~~	~~ECS03-MC04-02~~	~~网络会话的源、目的端口特征值提取~~
			网络会话的协议标识特			~~ECS03-MC04-03~~	~~网络会话的协议标识特征提取~~
			基于会话的工控网络拓			~~ECS03-MC04-04~~	~~基于会话的工控网络拓扑提取~~
			网络会话的自定义协议			~~ECS03-MC04-05~~	~~网络会话的自定义协议特征提取~~
		电网工控协议行为特征提取	电网工控协议指令特征	~~ECS03-MC05~~	~~电网工控协议行为特征提取~~	~~ECS03-MC05-01~~	~~电网工控协议指令特征提取~~
			电网工控协议行为数据			~~ECS03-MC05-02~~	~~电网工控协议行为数据地址值特征提取~~
			电网工控协议行为数据			~~ECS03-MC05-03~~	~~电网工控协议行为数据值特征提取~~
			电网工控协议自定义行			~~ECS03-MC05-04~~	~~电网工控协议自定义行为特征提取~~
		流量异常规则生成	流量周期范围规则生成	~~ECS03-MC06~~	~~流量异常规则生成~~	~~ECS03-MC06-01~~	~~流量周期范围规则生成~~
			流量带宽利用率规则生			~~ECS03-MC06-02~~	~~流量带宽利用率规则生成~~
			会话响应时长范围流量			~~ECS03-MC06-03~~	~~会话响应时长范围流量规则生成~~
			自定义流量统计规则生			~~ECS03-MC06-04~~	~~自定义流量统计规则生成~~
		网络异常会话规则生成	网络会话的合法资产规	~~ECS03-MC07~~	~~网络异常会话规则生成~~	~~ECS03-MC07-01~~	~~网络会话的合法资产规则生成~~
			网络会话的五元组特征			~~ECS03-MC07-02~~	~~网络会话的五元组特征协议规则生成~~
			网络会话的异常目的地			~~ECS03-MC07-03~~	~~网络会话的异常目的地址检测规则~~
			网络会话的异常源地址			~~ECS03-MC07-04~~	~~网络会话的异常源地址检测规则~~
			网络会话的自定义协议			~~ECS03-MC07-05~~	~~网络会话的自定义协议规则生成~~
		电网工控协议异常行为规则生成	电网工控协议的指令规	~~ECS03-MC08~~	~~电网工控协议异常行为规则生成~~	~~ECS03-MC08-01~~	~~电网工控协议的指令规则生成~~
			电网工控协议的行为数			~~ECS03-MC08-02~~	~~电网工控协议的行为数据地址访问限定规则~~
			电网工控协议的行为数			~~ECS03-MC08-03~~	~~电网工控协议的行为数据值阈限定规则生成~~
			电网工控协议的行为数			~~ECS03-MC08-04~~	~~电网工控协议的行为数据取值关系限定规则~~
			电网工控协议的关键事			~~ECS03-MC08-05~~	~~电网工控协议的关键事件规则生成~~
			电网工控协议的协议内			~~ECS03-MC08-06~~	~~电网工控协议的协议内容异常规则生成~~
			电网工控协议的协议格			~~ECS03-MC08-07~~	~~电网工控协议的协议格式异常规则生成~~
		攻击规则添加	添加SYN Flood攻击规	~~ECS03-MC09~~	~~攻击规则添加~~	~~ECS03-MC09-01~~	~~添加SYN Flood攻击规则~~
			添加IP分片攻击规则			~~ECS03-MC09-02~~	~~添加IP分片攻击规则~~
			添加ARP欺骗规则			~~ECS03-MC09-03~~	~~添加ARP欺骗规则~~
			添加超长数据包攻击检			~~ECS03-MC09-04~~	~~添加超长数据包攻击检测规则~~
			添加弱口令攻击规则			~~ECS03-MC09-05~~	~~添加弱口令攻击规则~~
			添加持续重放攻击检测			~~ECS03-MC09-06~~	~~添加持续重放攻击检测规则~~
			添加常见木马攻击检测			~~ECS03-MC09-07~~	~~添加常见木马攻击检测规则~~
			添加Tftp漏洞攻击检测			~~ECS03-MC09-08~~	~~添加Tftp漏洞攻击检测规则~~
			添加ICMP泛洪规则			~~ECS03-MC09-09~~	~~添加ICMP泛洪规则~~
			添加自定义工控攻击规			~~ECS03-MC09-10~~	~~添加自定义工控攻击规则~~
			添加已知PLC漏洞攻击规			~~ECS03-MC09-11~~	~~添加已知PLC漏洞攻击规则~~
			添加工控扫描脚本攻击			~~ECS03-MC09-12~~	~~添加工控扫描脚本攻击规则~~
			添加西门子蠕虫病毒攻			~~ECS03-MC09-13~~	~~添加西门子蠕虫病毒攻击规则~~
			规则库的构建			~~ECS03-MC10-01~~	~~规则库的构建~~
			规则文件的添加			~~ECS03-MC10-02~~	~~规则文件的添加~~
			规则文件的删除			~~ECS03-MC10-03~~	~~规则文件的删除~~
			规则文件的修改			~~ECS03-MC10-04~~	~~规则文件的修改~~
			规则文件的查找			~~ECS03-MC10-05~~	~~规则文件的查找~~

		规则文件的选择			~~ECS03-MC10-06~~	~~规则文件的选择~~	
	规则库	规则文件的下发	~~ECS03-MC10~~	~~规则库~~	~~ECS03-MC10-07~~	~~规则文件的下发~~	
		白名单规则格式的定义			~~ECS03-MC10-08~~	~~白名单规则格式的定义~~	
		白名单规则列表的构建			~~ECS03-MC10-09~~	~~白名单规则列表的构建~~	
		白名单规则的增删查			~~ECS03-MC10-10~~	~~白名单规则的增删查~~	
		黑名单规则格式的定义			~~ECS03-MC10-11~~	~~黑名单规则格式的定义~~	
		黑名单规则列表的构建			~~ECS03-MC10-12~~	~~黑名单规则列表的构建~~	
		黑名单规则的增删查			~~ECS03-MC10-13~~	~~黑名单规则的增删查~~	
		所有规则不匹配触发异				~~所有规则不匹配触发异常~~	
		异常状态推送				~~异常状态推送~~	
		异常目的地址检测规则				~~异常目的地址检测规则~~	
	支持基于tcp的私有工控协议				ECS03-MC03-01	**支持基于tcp的工控协议**	
	支持基于udp的私有工控协议				ECS03-MC03-02	**支持基于udp的工控协议**	
	流量特征提取				ECS03-MC03-03	**流量特征提取**	
	设备特征提取				ECS03-MC03-04	**设备特征提取**	
	异常源地址检测规则	异常源地址检测规则			ECS03-MC03-05	异常源地址检测规则	
		协议内容异常规则生成				~~协议内容异常规则生成~~	
		协议格式异常规则生成				~~协议格式异常规则生成~~	
	异常检测	行为数据地址访问限定	ECS03-MC03	异常检测		~~行为数据地址访问限定规则~~	
		行为数据值阈限定规则				~~行为数据值阈限定规则生成~~	
		行为数据取值关系限定				~~行为数据取值关系限定规则~~	
		关键事件规则生成				~~关键事件规则生成~~	
		流量周期范围规则生成				~~流量周期范围规则生成~~	
		流量带宽利用率规则生				~~流量带宽利用率规则生成~~	
	电网工控协议行为规则生成				ECS03-MC03-06	**电网工控协议行为规则生成**	
		会话响应时长范围规则				~~会话响应时长范围规则生成~~	
		非法资产检测				~~非法资产检测~~	
		异常数据包标记				~~异常数据包标记~~	
		任意规则匹配触发异常				~~任意规则匹配触发异常~~	
		异常状态推送				~~异常状态推送~~	
		SYN Flood攻击				~~SYN Flood攻击~~	
		IP分片攻击				~~IP分片攻击~~	
		ARP欺骗				~~ARP欺骗~~	
		超长数据包攻击检测				~~超长数据包攻击检测~~	
		弱口令攻击				~~弱口令攻击~~	
		持续重放攻击检测				~~持续重放攻击检测~~	
		常见木马攻击检测				~~常见木马攻击检测~~	
	通用攻击规则添加		ECS03-MC04	攻击检测	ECS03-MC04-01	**通用攻击规则添加**	
	工控攻击规则添加				ECS03-MC04-02	**工控攻击规则添加**	
		Tftp漏洞攻击检测				~~Tftp漏洞攻击检测~~	
		ICMP泛洪				~~ICMP泛洪~~	
	已知PLC漏洞攻击	已知PLC漏洞攻击			ECS03-MC04-03	已知PLC漏洞攻击	

远境PDF编辑器

			工控扫描脚本攻击				~~工控扫描脚本攻击~~	
			西门子蠕虫病毒攻击				~~西门子蠕虫病毒攻击~~	
	管理中心规则库管理					ECS03-MC04-04	**管理中心规则库管理**	
	终端规则文件管理					ECS03-MC04-05	**终端规则文件管理**	
	异常数据包标记		异常数据包标记			ECS03-MC04-06	异常数据包标记	
		检测算法	基于流量的异常检测算	~~ECS03-MC13~~	~~检测算法~~	~~ECS03-MC13-01~~	~~基于流量的异常检测算法~~	
			基于网络会话的异常检			~~ECS03-MC13-02~~	~~基于网络会话的异常检测算法~~	
			基于协议深度解析的异			~~ECS03-MC13-03~~	~~基于协议深度解析的异常检测算法~~	
			基于关键事件的异常检			~~ECS03-MC13-04~~	~~基于关键事件的异常检测算法~~	
			基于通用攻击的攻击检			~~ECS03-MC13-05~~	~~基于通用攻击的攻击检测算法~~	
			基于工控攻击的攻击检			~~ECS03-MC13-06~~	~~基于工控攻击的攻击检测算法~~	
			基于行为模型的异常检			~~ECS03-MC13-07~~	~~基于行为模型的异常检测方法~~	
		管理平台日志记录	日志记录格式定义	~~ECS03-MC14~~	~~管理平台日志记录~~	~~ECS03-MC14-01~~	~~日志记录格式定义~~	
			日志记录列表生成			~~ECS03-MC14-02~~	~~日志记录列表生成~~	
		检测终端日志记录	日志记录格式定义	~~ECS03-MC15~~	~~检测终端日志记录~~	~~ECS03-MC15-01~~	~~日志记录格式定义~~	
			系统状态信息采集			~~ECS03-MC15-02~~	~~系统状态信息采集~~	
			日志记录列表生成			~~ECS03-MC15-03~~	~~日志记录列表生成~~	
			日志记录列表上传			~~ECS03-MC15-04~~	~~日志记录列表上传~~	
		日志管理	日志记录的更新	~~ECS03-MC16~~	~~日志管理~~	~~ECS03-MC16-01~~	~~日志记录的更新~~	
			日志记录的备份			~~ECS03-MC16-02~~	~~日志记录的备份~~	
			日志记录的删除			~~ECS03-MC16-03~~	~~日志记录的删除~~	
			日志记录的查询			~~ECS03-MC16-04~~	~~日志记录的查询~~	
			日志记录的选择			~~ECS03-MC16-05~~	~~日志记录的选择~~	
		报警记录	报警格式定义	~~ECS03-MC17~~	~~报警记录~~	~~ECS03-MC17-01~~	~~报警格式定义~~	
			报警记录生成			~~ECS03-MC17-02~~	~~报警记录生成~~	
			报警记录上传			~~ECS03-MC17-03~~	~~报警记录上传~~	
		报警记录管理	报警记录的更新	~~ECS03-MC18~~	~~报警记录管理~~	~~ECS03-MC18-01~~	~~报警记录的更新~~	
			报警记录的备份			~~ECS03-MC18-02~~	~~报警记录的备份~~	
			报警记录的删除			~~ECS03-MC18-03~~	~~报警记录的删除~~	
			报警记录的查询			~~ECS03-MC18-04~~	~~报警记录的查询~~	
			报警记录的选择			~~ECS03-MC18-05~~	~~报警记录的选择~~	
		态势报告管理	报告文件的定义	~~ECS03-MC19~~	~~态势报告管理~~	~~ECS03-MC19-01~~	~~报告文件的定义~~	
			报告文件的选择			~~ECS03-MC19-02~~	~~报告文件的选择~~	
			读取报警日志数据			~~ECS03-MC19-03~~	~~读取报警日志数据~~	
			报告文件的生成			~~ECS03-MC19-04~~	~~报告文件的生成~~	
			报告文件的下载			~~ECS03-MC19-05~~	~~报告文件的下载~~	
特征提取			CPU使用率实时监控				~~CPU使用率实时监控~~	
			内存使用率实时监控				~~内存使用率实时监控~~	
			硬盘使用率监控				~~硬盘使用率监控~~	
			内存大小				~~内存大小~~	
			硬盘大小				~~硬盘大小~~	
			读取资产列表				~~读取资产列表~~	

迅捷PDF编辑器

			修改设备描述信息				~~修改设备描述信息~~
			绘制网络拓扑				~~绘制网络拓扑~~
			修改网络拓扑				~~修改网络拓扑~~
	全部告警总和历史趋势	可视化管理	全部告警总和历史趋势	ECS03-MC05	可视化管理	ECS03-MC05-01	全部告警总和历史趋势
	分报警类型的历史趋势		分报警类型的历史趋势			ECS03-MC05-02	分报警类型的历史趋势
	终端告警事件统计		终端告警事件统计			ECS03-MC05-03	终端告警事件统计
	同一终端不同报警类型的事件统计		同一终端不同报警类型			ECS03-MC05-04	同一终端不同报警类型的事件统计
	终端告警事件百分比统计		终端告警事件百分比统			ECS03-MC05-05	终端告警事件百分比统计
	同一终端不同报警类型的事件百分		同一终端不同报警类型			ECS03-MC05-06	同一终端不同报警类型的事件百分比统计
			分类读取日志数据				~~分类读取日志数据~~
	系统健康值计算		系统健康值计算			ECS03-MC05-07	系统健康值计算
			系统健康值展示				~~系统健康值展示~~
		系统管理	用户名和密码联合验证	ECS03-MC06	系统管理		~~用户名和密码联合验证~~
			登录次数限制				~~登录次数限制~~
			添加用户				~~添加用户~~
			删除用户				~~删除用户~~
			修改密码				~~修改密码~~
			修改用户权限				~~修改用户权限~~
			授权文件生成				~~授权文件生成~~
	授权文件导入		授权文件导入			ECS03-MC06-01	授权文件导入
			授权文件匹配				~~授权文件匹配~~
	检测终端重启		检测终端重启			ECS03-MC06-02	检测终端上线状态
	检测终端关机		检测终端关机			ECS03-MC06-03	检测终端离线状态
			检测终端自学习				~~检测终端自学习~~
			检测终端报警日志开关				~~检测终端报警日志开关~~
			调试开关开启与关闭				~~调试开关开启与关闭~~
	检测终端IP地址配置	系统配置	检测终端IP地址配置	ECS03-MC07	系统配置	ECS03-MC07-01	检测终端IP地址配置
	IP地址下发		IP地址下发			ECS03-MC07-02	IP地址下发
	手动时间同步		手动时间同步			ECS03-MC07-03	手动时间同步
	自动时间同步		自动时间同步			ECS03-MC07-04	自动时间同步
	检测终端配置备份与恢复		检测终端配置备份与恢			ECS03-MC07-05	检测终端配置备份与恢复
	管理平台配置备份与恢复		管理平台配置备份与恢			ECS03-MC07-06	管理平台配置备份与恢复
	恢复出厂设置		恢复出厂设置			ECS03-MC07-07	恢复出厂设置
	系统帮助		系统帮助			ECS03-MC07-08	系统帮助
	大数据指标计算					ECS03-MC08-01	**安全状态指标计算**
	计算数据流入量					ECS03-MC08-02	**计算数据流入量**
	计算安全事件的历史发生频率					ECS03-MC08-03	**计算安全事件的历史发生频率**
	特征分析					ECS03-MC08-04	**特征分析**
	泪滴攻击特征分析					ECS03-MC08-05	**泪滴攻击特征分析**
	UDP洪水攻击特征分析					ECS03-MC08-06	**UDP洪水攻击特征分析**
	SYN洪水攻击特征分析DNS高速缓存					ECS03-MC08-07	**SYN洪水攻击特征分析DNS高速缓存污染攻击**
	行为诊断					ECS03-MC08-08	**攻击行为诊断**

迅捷PDF编辑器

	泪滴攻击特征分析					ECS03-MC08-09	泪滴攻击特征分析	
	端口扫描攻击特征分析					ECS03-MC08-10	端口扫描攻击特征分析	
	反响映射攻击特征分析							
	DNS高速缓存污染攻击特征分析					ECS03-MC08-11	DNS高速缓存污染攻击特征分析	
	数据聚合					ECS03-MC08-12	数据聚合	
	数据关联					ECS03-MC08-13	数据关联	
	指标定义					ECS03-MC08-14	安全状态指标定义	
	“资产安全状态” 整个网络中的					ECS03-MC08-15	资产安全状态展示发现的漏洞数量和所处级别	
	各防护设备获得的报警类别及各类			ECS03-MC08	分析需求	ECS03-MC08-16	设备产生的报警类别及各类别报警的总数	
	各关键设备开放的端口总量					ECS03-MC08-17	各重要设备开放的端口总量	
	各重要设备所使用的 OS 以及提供					ECS03-MC08-18	获取各重要设备所使用的操作系统	
	计算指标权重					ECS03-MC08-19	设置安全状态指标权重	
	计算网络态势得分					ECS03-MC08-20	计算网络态势得分	
	网络安全预警					ECS03-MC08-21	网络安全告警	
	配置数据源					ECS03-MC08-22	配置数据源	
	计算网络态势结果					ECS03-MC08-23	评价网络态势结果	
	态势预警					ECS03-MC08-24	态势告警	
	告警分类统计					ECS03-MC08-25	告警分类统计	
	告警数量统计					ECS03-MC08-26	告警数量统计	
	支持图形化展示统计结果					ECS03-MC08-27	支持图形化展示告警统计结果	
	设备流量统计					ECS03-MC08-28	设备流量统计	
	支持图形化展示统计结果					ECS03-MC08-29	支持图形化展示设备流量统计结果	
	分组流量统计					ECS03-MC08-30	分组流量统计	
	对办公区流量统计与阈值告					ECS03-MC08-31	各重要设备流量统计与阈值告警	
	协议流量统计							

总体情况：

迅捷PDF编辑器

网络安全仿真验证环境建设及平台工具研发-电力工控固件漏洞挖掘工具项目概要设计方案功能比对偏差表

可研批复内容		软件需求内容		概要设计方案				说明
一级功能	二级功能	一级功能	二级功能	一级功能编号	一级功能	二级功能编号	二级功能	
固件收集	支持通过特定URL爬取固件	固件收集	支持通过特定URL爬取固件	ECS02-MC01	固件收集	ECS02-MC01-01	支持通过特定URL爬取固件	
	支持FTP爬取固件							删除功能
	基于固件厂商分类		基于固件厂商分类			ECS02-MC01-02	基于固件厂商分类	
	基于固件设备型号分类		基于固件设备型号分类			ECS02-MC01-03	基于固件设备型号分类	
固件信息提取	支持固件文件头自动解码或解析	固件信息提取	支持固件文件头自动解码或解析	ECS02-MC02	固件信息提取	ECS02-MC02-01	支持固件文件头自动解码或解析	
	支持SquashFS文件系统提取		支持SquashFS文件系统提取			ECS02-MC02-02	支持SquashFS文件系统提取	
	支持JFFS2文件系统提取		支持JFFS2文件系统提取			ECS02-MC02-03	支持JFFS2文件系统提取	
	支持YAFFS文件系统提取					ECS02-MC02-04	**支持YAFFS文件系统提取**	
	支持UBIFS文件系统提取					ECS02-MC02-05	**支持UBIFS文件系统提取**	
	支持Romfs文件系统提取		支持Romfs文件系统提取			ECS02-MC02-06	支持Romfs文件系统提取	
	支持CRAMFS文件系统提取		支持CRAMFS文件系统提取			ECS02-MC02-07	支持CRAMFS文件系统提取	
	X86架构识别		X86架构识别			ECS02-MC02-08	X86架构识别	
	ARM架构识别		ARM架构识别			ECS02-MC02-09	ARM架构识别	
	MIPS架构识别		MIPS架构识别			ECS02-MC02-10	MIPS架构识别	
	PowerPC架构识别		PowerPC架构识别			ECS02-MC02-11	PowerPC架构识别	
	组件加载基址解析		组件加载基址解析			ECS02-MC02-12	组件加载基址解析	
	X86函数编译优化级别识别					ECS02-MC02-13	**X86函数编译优化级别识别**	
固件脆弱性分析	支持函数分析的并行处理	固件脆弱性分析	支持函数分析的并行处理	ECS02-MC03	固件脆弱性分析	ECS02-MC03-01	支持函数分析的并行处理	
	支持固件分析的并行处理		支持固件分析的并行处理			ECS02-MC03-02	支持固件分析的并行处理	
	支持固件中二进制代码的函数识别		支持固件中二进制代码的函数识别			ECS02-MC03-03	支持固件中二进制代码的函数识别	
	x86汇编代码转换成中间语言					ECS02-MC03-04	**x86汇编代码转换成中间代码**	
	arm汇编代码转换成中间语言					ECS02-MC03-05	**ARM汇编代码转换成中间代码**	
	mips汇编代码转换成中间语言					ECS02-MC03-06	**MIPS汇编代码转换成中间代码**	
	powerpc汇编代码转换成中间语言					ECS02-MC03-07	**PowerPC汇编代码转换成中间代码**	
	支持脆弱性函数识别		支持脆弱性函数识别			ECS02-MC03-08	支持脆弱性函数识别	
	支持污点数据源识别		支持污点数据源识别			ECS02-MC03-09	支持污点数据源识别	
	支持用户自定义污点数据源		支持用户自定义污点数据源			ECS02-MC03-10	支持用户自定义污点数据源	
	函数参数识别		函数参数识别			ECS02-MC03-11	函数参数识别	
	函数返回值识别		函数返回值识别			ECS02-MC03-12	函数返回值识别	
	变量类型识别		变量类型识别			ECS02-MC03-13	变量类型识别	
	栈空间大小提取		栈空间大小提取			ECS02-MC03-14	栈空间大小提取	
	堆空间大小提取		堆空间大小提取			ECS02-MC03-15	堆空间大小提取	
			常量区大小提取				**常量区大小提取**	
			静态数据区大小提取				**静态数据区大小提取**	
			代码区大小提取				**代码区大小提取**	
	变量的语义信息提取					ECS02-MC03-16	**变量的语义信息提取**	
	变量的约束信息提取					ECS02-MC03-17	**变量的约束信息提取**	
	简单数据结构恢复					ECS02-MC03-18	**简单数据结构恢复**	
	基于缓冲区溢出漏洞模型生成					ECS02-MC03-19	**检测缓冲区溢出漏洞**	
	基于整数溢出漏洞模型生成					ECS02-MC03-20	**检测整数溢出漏洞**	
	基于命令注入漏洞模型生成					ECS02-MC03-21	**检测命令注入漏洞**	
	污点源到脆弱点路径生成		污点源到脆弱点路径生成			ECS02-MC03-22	污点源到脆弱点路径生成	
	缓冲区溢出漏洞检测		缓冲区溢出漏洞检测			ECS02-MC03-23	缓冲区溢出漏洞检测	

试读PDF结束

	整数溢出漏洞检测		整数溢出漏洞检测			ECS02-MC03-24	整数溢出漏洞检测	
	命令注入漏洞检测		命令注入漏洞检测			ECS02-MC03-25	命令注入漏洞检测	
固件漏洞关联	开源组件源码爬取	固件漏洞关联	开源组件源码爬取	ECS02-MC04	固件漏洞关联	ECS02-MC04-01	开源组件源码爬取	
	开源组件交叉编译					ECS02-MC04-02	**支持开源组件的编译**	
	漏洞组件特征提取		漏洞组件特征提取			ECS02-MC04-03	漏洞组件特征提取	
	组件HashMap余弦相似度		组件HashMap余弦相似度			ECS02-MC04-04	组件HashMap余弦相似度	
	组件HashMap倒排索引		组件HashMap倒排索引			ECS02-MC04-05	组件HashMap倒排索引	
	组件的在线快速漏洞关联		组件的在线快速漏洞关联			ECS02-MC04-06	组件的在线快速漏洞关联	
漏洞库	支持漏洞库的漏洞信息添加	漏洞库	支持漏洞库的漏洞信息添加	ECS02-MC05	漏洞库	ECS02-MC05-01	支持漏洞库的漏洞信息添加	
	支持漏洞库的漏洞信息删除		支持漏洞库的漏洞信息删除			ECS02-MC05-02	支持漏洞库的漏洞信息删除	
	支持漏洞库的漏洞信息修改		支持漏洞库的漏洞信息修改			ECS02-MC05-03	支持漏洞库的漏洞信息修改	
	支持漏洞库的漏洞信息查找		支持漏洞库的漏洞信息查找			ECS02-MC05-04	支持漏洞库的漏洞信息查找	
	漏洞的选择							删除功能
	支持漏洞的厂商信息查看		支持漏洞的厂商信息查看			ECS02-MC05-05	支持漏洞的厂商信息查看	
	支持漏洞的设备型号信息查看		支持漏洞的设备型号信息查看			ECS02-MC05-06	支持漏洞的设备型号信息查看	
	支持漏洞的固件版本信息查看		支持漏洞的固件版本信息查看			ECS02-MC05-07	支持漏洞的固件版本信息查看	
	支持漏洞的类型信息查看		支持漏洞的类型信息查看			ECS02-MC05-08	支持漏洞的类型信息查看	
	支持漏洞的威胁等级分类		支持漏洞的威胁等级分类			ECS02-MC05-09	支持漏洞的威胁等级分类	
报表生成	日志记录格式定制	报表生成	日志记录格式定制	ECS02-MC06	报表生成	ECS02-MC06-01	日志记录格式定制	
	日志记录列表生成		日志记录列表生成			ECS02-MC06-02	日志记录列表生成	
	日志记录列表上传							删除功能
	日志记录的更新							删除功能
	日志记录的备份		日志记录的备份			ECS02-MC06-03	日志记录的备份	
	日志记录的删除		日志记录的删除			ECS02-MC06-04	日志记录的删除	
	日志记录的查询		日志记录的查询			ECS02-MC06-05	日志记录的查询	
	日志记录的选择							删除功能
	支持PDF格式的报告		支持PDF格式的报告			ECS02-MC06-06	支持PDF格式的报告	
	报告文件的定义							删除功能
	报告文件的选择							删除功能
	报告文件的生成		报告文件的生成			ECS02-MC06-07	报告文件的生成	
	报告文件的下载		报告文件的下载			ECS02-MC06-08	报告文件的下载	
界面展示	展示固件分析的进度	界面展示	展示固件分析的进度	ECS02-MC07	界面展示	ECS02-MC07-01	展示固件分析的进度	
	展示固件分析的剩余时间		展示固件分析的剩余时间			ECS02-MC07-02	展示固件分析的剩余时间	
	CPU使用率实时监控		CPU使用率实时监控			ECS02-MC07-03	CPU使用率实时监控	
	内存使用率实时监控		内存使用率实时监控			ECS02-MC07-04	内存使用率实时监控	
	硬盘使用率监控		硬盘使用率监控			ECS02-MC07-05	硬盘使用率监控	
	展示后台系统的内存大小		展示后台系统的内存大小			ECS02-MC07-06	展示后台系统的内存大小	
	展示后台系统的硬盘大小		展示后台系统的硬盘大小			ECS02-MC07-07	展示后台系统的硬盘大小	
	漏洞类型展示		漏洞类型展示			ECS02-MC07-08	漏洞类型展示	
	漏洞统计分析展示		漏洞统计分析展示			ECS02-MC07-09	漏洞统计分析展示	
系统管理	用户名和密码联合验证	系统管理	用户名和密码联合验证	ECS02-MC08	系统管理	ECS02-MC08-01	用户名和密码联合验证	
	登录失败的尝试次数限制		登录失败的尝试次数限制			ECS02-MC08-02	登录失败的尝试次数限制	
	添加用户		添加用户			ECS02-MC08-03	添加用户	
	删除用户		删除用户			ECS02-MC08-04	删除用户	
	修改密码		修改密码			ECS02-MC08-05	修改密码	
	修改用户权限		修改用户权限			ECS02-MC08-06	修改用户权限	
	授权文件生成							删除功能
	授权文件导入							删除功能

试读PDF编辑器

	授权文件匹配					删除功能
	固件分析版本选择			ECSO2-MC08-07	选择查看不同版本固件的分析结果	
	漏洞关联厂商选择			ECSO2-MC08-08	查看漏洞的关联厂商	
	系统配置备份与恢复	系统配置备份与恢复		ECSO2-MC08-09	系统配置备份与恢复	
	恢复出厂设置	恢复出厂设置		ECSO2-MC08-10	恢复出厂设置	
	系统帮助	系统帮助		ECSO2-MC08-11	系统帮助	

总体情况：

迅捷PDF编辑器

网络安全仿真验证环境建设及平台工具研发-网络安全靶场试验管控平台项目概要设计方案功能比对偏差表

可研批复内容		软件需求内容		概要设计方案				
一级功能	二级功能	一级功能	二级功能	一级功能编号	一级功能	二级功能编号	二级功能	说明
IaaS平台	集群管理	IaaS平台		ECS06-MC01	IaaS平台	ECS06-MC01-01	集群管理	
	虚拟机管理					ECS06-MC01-02	虚拟机管理	
	统计总览					ECS06-MC01-03	统计总览	
	虚拟机镜像					ECS06-MC01-04	虚拟机镜像	
	云盘功能					ECS06-MC01-05	云盘功能	
	快照管理					ECS06-MC01-06	快照管理	
	多租户环境（VPC）					ECS06-MC01-07	多租户环境（VPC）	
	网络管理					ECS06-MC01-08	网络管理	
	存储管理					ECS06-MC01-09	存储管理	
SDN控制器主机	全局网络拓扑视图维护	SDN控制器主机		ECS06-MC02	SDN控制器主机	ECS06-MC02-01	全局网络拓扑视图维护	
	网络感知服务					ECS06-MC02-02	网络感知服务	
	网络性能加速					ECS06-MC02-03	网络性能加速	
	SDN集成					ECS06-MC02-04	SDN集成	
	NFV集成					ECS06-MC02-05	NFV集成	
虚拟机Agent组件	操作系统的安全配置信息监控（虚拟机、物理机）	虚拟机Agent组件	操作系统的安全配置信息监控（虚拟机、物理机）	ECS06-MC03	虚拟机Agent组件	ECS06-MC03-01	操作系统的安全配置信息监控（虚拟机、物理机）	
	系统服务信息监控（虚拟机、物理机）		系统服务信息监控（虚拟机、物理机）			ECS06-MC03-02	系统服务信息监控（虚拟机、物理机）	
	系统状态信息监控（虚拟机、物理机）		系统状态信息监控（虚拟机、物理机）			ECS06-MC03-03	系统状态信息监控（虚拟机、物理机）	
可视化拓扑自动组网引擎	支持拓扑连线管理功能	可视化拓扑自动组网引擎	支持拓扑连线管理功能	ECS06-MC04	可视化拓扑自动组网引擎	ECS06-MC04-01	支持拓扑连线管理功能	
	拓扑图内节点（即组件）属性配置管理		拓扑图内节点（即组件）属性配置管理			ECS06-MC04-02	拓扑图内节点（即组件）属性配置管理	
	拓扑节点名与IP的映射解析		拓扑节点名与IP的映射解析			ECS06-MC04-03	拓扑节点名与IP的映射解析	
	支持网络拓扑编辑器功能		支持网络拓扑编辑器功能			ECS06-MC04-04	支持网络拓扑编辑器功能	
资源库	支持资产节点（即组件资源）管理功能	资源库	支持资产节点（即组件资源）管理功能	ECS06-MC05	资源库	ECS06-MC05-01	支持资产节点（即组件资源）管理功能	
	支持设备管理（含物理设备和虚拟设备）功能		支持设备管理（含物理设备和虚拟设备）功能			ECS06-MC05-02	支持设备管理（含物理设备和虚拟设备）功能	
数据采集	支持Agent对节点进行数据采集	数据采集	支持Agent对节点进行数据采集	ECS06-MC06	数据采集	ECS06-MC06-01	支持Agent对节点进行数据采集	
	支持租户信息数据录入采集		支持租户信息数据录入采集			ECS06-MC06-02	支持租户信息数据录入采集	
	支持节点的资源信息数据采集		支持节点的资源信息数据采集			ECS06-MC06-03	支持节点的资源信息数据采集	
			支持节点状态数据采集			ECS06-MC06-04	支持节点状态数据采集	增加功能
	支持节点系统的静态配置数据采集		支持节点系统的静态配置数据采集			ECS06-MC06-05	支持节点系统的静态配置数据采集	
	支持节点系统的实时状态数据采集		支持节点系统的实时状态数据采集			ECS06-MC06-06	支持节点系统的实时状态数据采集	
	支持节点系统的性能数据采集		支持节点系统的性能数据采集			ECS06-MC06-07	支持节点系统的性能数据采集	
数据分析	数据预处理					ECS06-MC06-08	数据预处理	
	日志数据分析		日志数据分析			ECS06-MC06-09	日志数据分析	
	支持节点Agent采集数据的分析		支持节点Agent采集数据的分析			ECS06-MC06-10	支持节点Agent采集数据的分析	
	节点和数据关联关系的分析		节点和数据关联关系的分析			ECS06-MC06-11	节点和数据关联关系的分析	
	节点和数据统计关系分析		节点和数据统计关系分析			ECS06-MC06-12	节点和数据统计关系分析	
	可视化关联分析		可视化关联分析			ECS06-MC06-13	可视化关联分析	
数据可视化	告警分类统计	数据可视化	告警分类统计	ECS06-MC07	数据可视化	ECS06-MC07-01	告警分类统计	
	告警数量统计		告警数量统计			ECS06-MC07-02	告警数量统计	
	网络拓扑展示		网络拓扑展示			ECS06-MC07-03	网络拓扑展示	
	节点网络流量过程监控		节点网络流量过程监控			ECS06-MC07-04	节点网络流量过程监控	
	支持漏洞库管理		支持漏洞库管理			ECS06-MC08-01	支持漏洞库管理	

试读PDF结束

漏洞库	支持漏洞库漏洞编号关联	漏洞库	支持漏洞库漏洞编号关联	ECS06-MC08	漏洞库	ECS06-MC08-02	支持漏洞库漏洞编号关联	
	支持电力工控类型漏洞库		支持电力工控类型漏洞库			ECS06-MC08-03	支持电力工控类型漏洞库	
	支持信息系统类型漏洞库		支持信息系统类型漏洞库			ECS06-MC08-04	支持信息系统类型漏洞库	
	支持威胁情报库		支持威胁情报库			ECS06-MC08-05	支持威胁情报库	
	支持攻击脚本库		支持攻击脚本库			ECS06-MC08-06	支持攻击脚本库	
设备指纹库	设备指纹库管理	设备指纹库	设备指纹库管理	ECS06-MC09	设备指纹库	ECS06-MC09-01	设备指纹库管理	
	设备指纹库格式定制		设备指纹库格式定制			ECS06-MC09-02	设备指纹库格式定制	
扫描器	离线漏洞扫描	扫描器	离线漏洞扫描	ECS06-MC10	扫描器	ECS06-MC10-01	离线漏洞扫描	
	离线漏洞扫描结果人工验证		离线漏洞扫描结果人工验证			ECS06-MC10-02	离线漏洞扫描结果人工验证	
	离线漏洞扫描结果告警发布		离线漏洞扫描结果告警发布			ECS06-MC10-03	离线漏洞扫描结果告警发布	
	离线漏洞扫描结果报表生成		离线漏洞扫描结果报表生成			ECS06-MC10-04	离线漏洞扫描结果报表生成	
系统管理	用户管理	系统管理	用户管理	ECS06-MC11	系统管理	ECS06-MC11-01	用户管理	
	日志管理		日志管理			ECS06-MC11-02	日志管理	
总体情况：								

备注：
1.表格的左侧“可研批复内容”，须从本项目可研批复中查找相关的一级、二级等功能内容，如果可研批复没有完整的功能清单，则从可研评审意见(评审报告)中查找完整的内容，如果可研批复与可研评审意见(评审报告)出现差异，则以可研批复为准。
2.表格的右侧“概要设计方案”，须从本次提交的概要设计报告中，查找相应的一级、二级等功能设计内容。
3.概要设计与可研批复功能分别对比，并以可研批复内容为基准结合实际进行比照对应，概设不一定强制要求与可研名称顺序完全一致，整体覆盖可研即可，若存在差异要统计并进行简要说明。
4.无论可研批复内容和概要设计方案中各级功能内容是否存在差异，都必须完整编制本材料并提交；请务必确认相关内容一致性、真实性和完整性，否则会直接影响评审结果。

迅捷PDF编辑器