国家电网
STATE GRID
国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

目 录

大型企业安全运维实践

国家电网
STATE GRID
国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

背景和目标

安全形势 → 国内外动态 → 运维目标

国家和企业信息化投入增加、对信息化依赖程度逐步增高。信息安全建设方面其主要手段为购买信息安全防护硬件产品。企业在信息安全事件处置、监控、警报、评估、应急等方面缺少一套完整的安全服务体系来有效保障，而信息安全服务还存在较大的差距、进行信息安全工作时还缺乏主动性，没有建立统一、全面、体系的集中安全运维及服务机制。

随着业务信息价值逐步增高，面临的安全威胁，数据泄露、非法操作、恶意破坏。因此，在建设基础安全措施和配置基本安全策略后，有必要通过引入专业的信息安全服务团队，来保障自身信息系统的稳定安全运行，同时通过专业的安全咨询和服务，逐步构建动态、完整、高效的客户信息安全整体，形成能持续完善、自我优化并不断持续改进的安全运维体系和安全管理体系。

国家电网
STATE GRID
国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

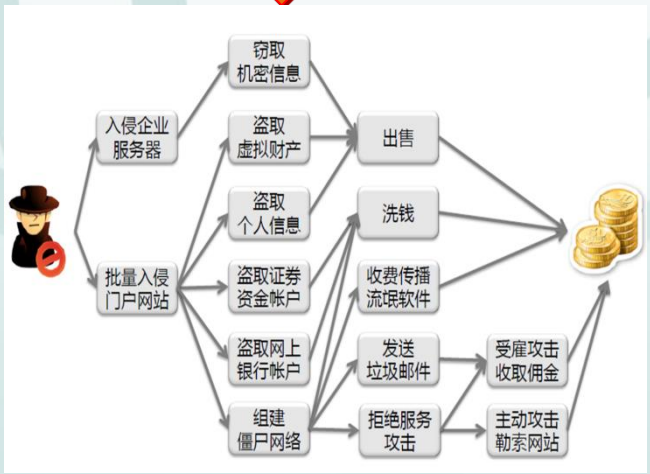
背景和目标

安全形势 → 国内外动态 → 运维目标

攻击从损人不利己向获取利益转变

攻击变得越来越功利，攻击从损人不利己向获取利益转变;

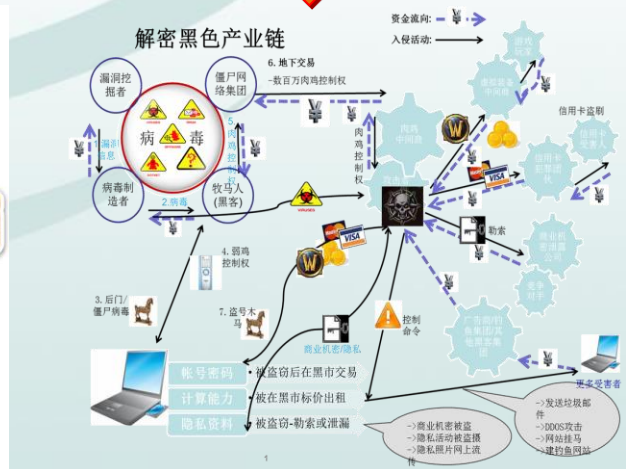
黑客行动的动力转向牟利后，其攻击行为以获取有价值资料作为主要攻击目标，无论机构组织还是个人用户的危险也被大大加深。



信息安全无处不在

攻击变得越来越有组织性，攻击从个人英雄向组织犯罪转变;

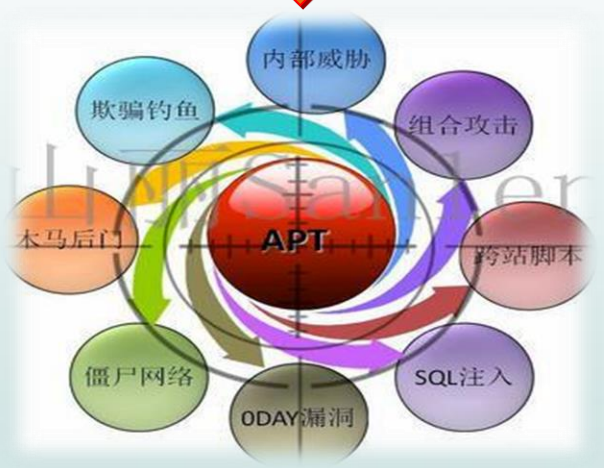
有组织的攻击犯罪攻击资源更多，更加有效，造成的安全威胁更大



攻击手段体系化

采用体系化攻击手段的APT攻击呈爆发趋势，带来越来越大的安全威胁。

APT攻击以窃取核心资料为目的，会运用各种攻击工具、受感染的各种介质、供应链和社会工程学等体系化的攻击手段实施先进的、持久的且有效的威胁和攻击。



国家电网
STATE GRID
国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

背景和目标

安全形势 → 国内外动态 → 运维目标

信息安全上升到国家安全高度

美国 --- 《网络空间安全国家战略》，

- 美国21世纪的经济繁荣依赖于网络空间安全
- 将网络空间安全威胁定位为举国面临的最严重的国家经济和国家安全挑战之一

英国 --- 《英国网络安全战略》

- 使英国面对网络攻击的恢复力更强，并保护其在网络空间中的利益；
- 帮助塑造一个可供英国大众安全使用的、开放的、稳定的、充满活力的网络空间，并进一步支撑社会开放；

中国 --- 国家网络安全战略形成

- 十六届四中全会首次明确将信息安全作为国家安全的主要内容
- 2014年2月27日，中央网络安全和信息化领导小组宣告成立，中共中央总书记、国家主席、中央军委主席习近平亲自担任组长。网络安全上升到国家安全战略。
- 习近平主席指出，没有网络安全就没有国家安全。

信息安全工作存在的主要问题

三个“忽视”	三个“缺乏”
重视安全技术，忽视安全管理	缺乏统一安全架构规划与协调
重视外部防护，忽视内部安全	缺乏信息安全组织与治理
重视产品购买，忽视产品使用	缺乏信息安全意识教育与培训

国家电网
STATE GRID
国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

背景和目标

安全形势 → 国内外动态 → 运维目标

建立基于云模式的可管理的安全运维服务支撑

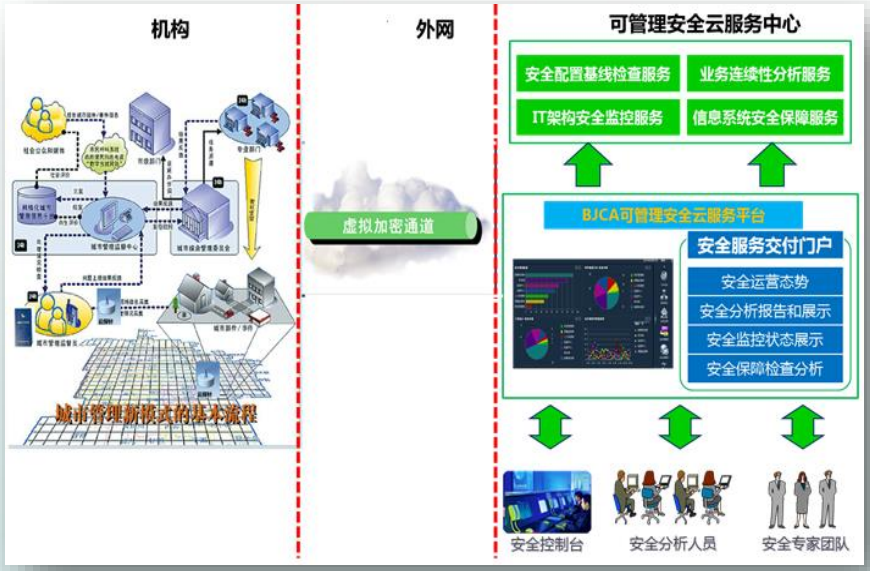
可管理安全运维服务平台应该包括体系化的安全状态监测、安全配置核查、安全事件分析与展示的安全风险管控的功能。能够做到及时了解业务系统安全风险状况，提升组织安全管控能力。

感知	自动化感知单位内信息安全配置信息和运行状态信息的服务
分析	对安全相关信息的分析处理服务
度量	对安全状态和安全态势进行科学度量；对安全绩效工作进行度量和评价
管理	对资产、安全事件、安全风险、安全运维实现有效的管控
展示	多方式、多维度、多视角对安全态势进行直观展示
指挥	为统一协调、指挥、调度信息安全事件的应急处置提供支持服务

构建可管理的安全运维服务支撑的方式

构建自有的可管理安全运营支撑平台；

依托第三方安全服务机构提供安全运营支撑服务。



国家电网
STATE GRID
国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

背景和目标

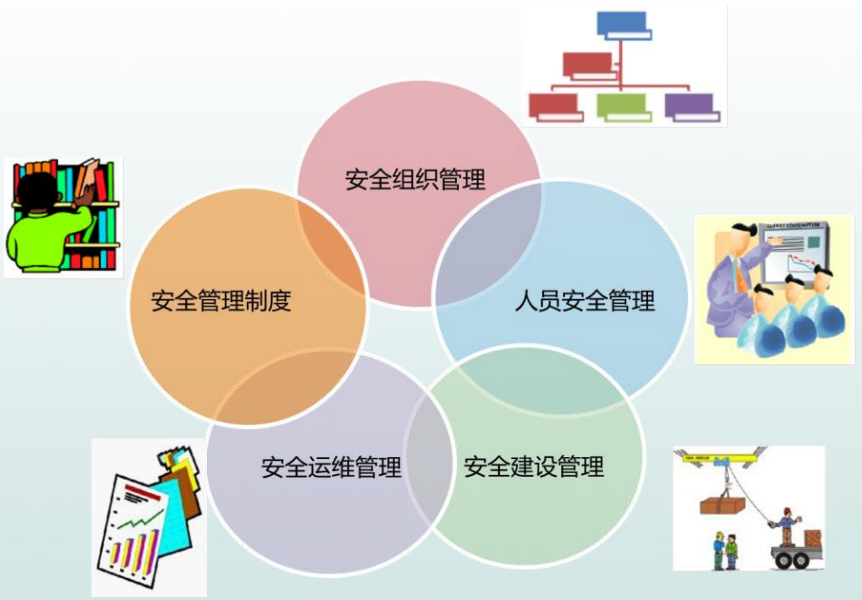
安全形势 → 国内外动态 → 运维目标

建设组织内高素质的信息安全队伍

如果安全管理有漏洞，其它安全措施投入再大也无济于事。因此，应加强信息安全从业人员队伍建设，明确组织机构信息安全岗、人员，对其进行有针对性的培训

以国家有关要求建设信息安全管理制度规范

信息安全管理策略、目标和活动应该反映业务目标；
信息安全管理制度规范的制定与业务部门的紧密配合；
建设过程中应该鼓励暴露和发现管理方面的问题和风险；
信息安全管理制度规范要具有可操作性和可实施性。



国家电网
STATE GRID
国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

目 录

大型企业安全运维实践

国家电网
STATE GRID
国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

安全运维总体思路

安全运维发展 → 运维体系 → 运维目标

第一阶段

- 驻场服务
- 提供咨询服务
- 定期简单渗透
- 在安全制度、用系统、体系方面收集整理息、技术支持起辅助和执行用。
- 渗透测试作为助服务内容，月进行远程渗测试
- 缺点：无明确路。
- 方式和内容不体系

第二阶段

- 在驻场服务基础上，增加风评和等保业务；
- 风评和等保业务结合，形成信息安全相对完善的服务点体系。
- 引进专业信息安全工具，如漏扫设备；
- 增加巡检服务内容
- 特点：技术服务点趋于完善。服务内容增加（渗透、巡检、安全基线建设）

第三阶段

- 驻场服务内容完善；
- 周期性渗透测试和定期巡检
- 组建SRT应急响应小组，解决企业应急响应、信息安全事件处置
- 安全事件溯源
- 丰富和规范巡检手册和检测手册
- 新增上线前系统安全测评业务

第四阶段

- 新增人员培养业务，提供人员技术培训、全员信息安全意识培训等；
- 团队内部专业化细分，形成方案编制、项目实施、测评等专业团队
- 形成驻场服务前端和后端安全团队联动和支持

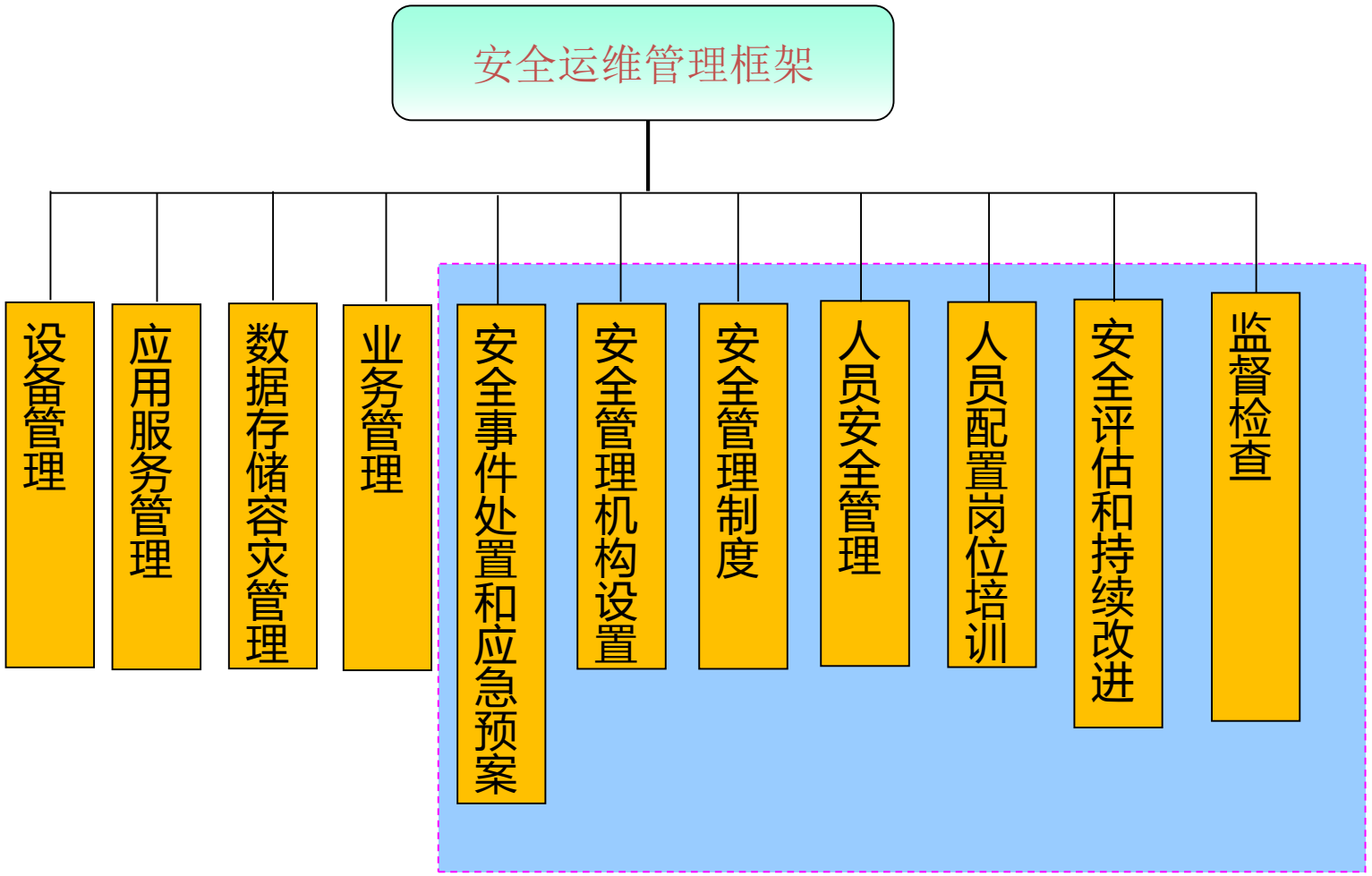
未来目标

- 逐步完善与丰富安全运维服务体系和标准
- 建设安全运维自动化体系

国家电网
STATE GRID
国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

安全运维总体思路

安全运维发展 → 运维体系 → 运维目标

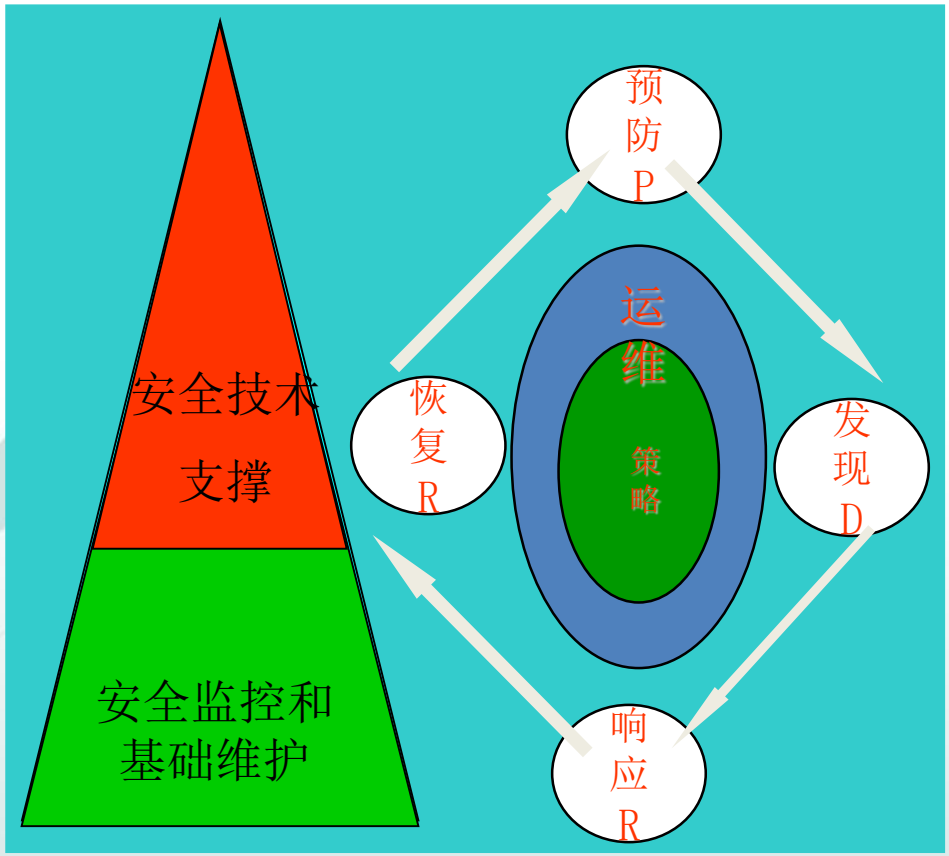


国家电网
STATE GRID
国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

安全运维总体思路

运维阶段 → 运维体系 → 运维目标

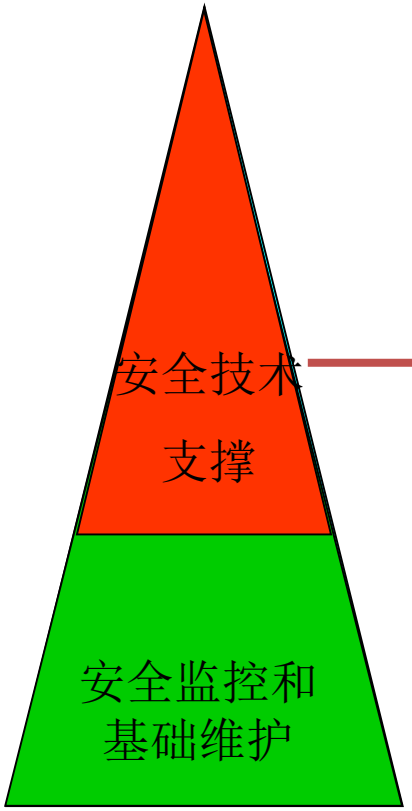
- 省公司实现安全监控和基础维护；
- 在总部建立集中的安全技术支撑队伍；
- 围绕“积极预防、及时发现、积极响应、确保恢复”四个环节，形成分层、闭环的维护体系；
- 锻造一支专业的网络与信息安全队伍。



国家电网
STATE GRID
国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

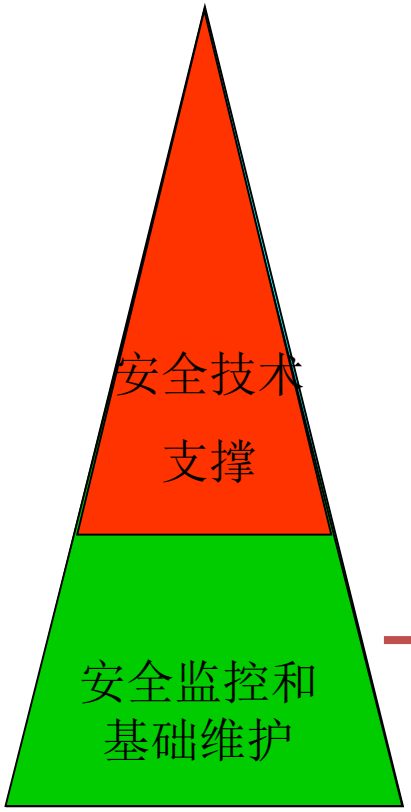
安全运维总体思路

运维阶段 → 运维体系 → 运维目标



1. 制定网络和系统层面的整体安全技术保护方案和技术规范；
2. 逐步实现安全自评估，全面掌握安全风险；
3. 提供重大安全预警信息发布和解决方案；
4. 协调响应网络层面的各类重大安全事件；
5. 对各类安全事件有关数据进行综合分析，形成安全运行分析报告；
6. 对生产层面的安全策略进行集中控制；
7. 跟踪研究各种安全问题和技术，收集各种基础信息资源。

安全运维总体思路

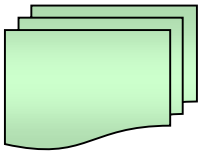


1. 进行7×24小时的日常安全安全事件监测，负责受理安全投诉。
2. 对安全事件进行收集汇总，进行事件预处理。
3. 系统日常口令维护，加载安全补丁和梳理服务端口等
4. 实施各类安全设备和配套管理设备的日常维护。
5. 实施一般安全预警和安全应急事件的处理。
6. 落实系统自身安全应急预案，并参加安全应急演练

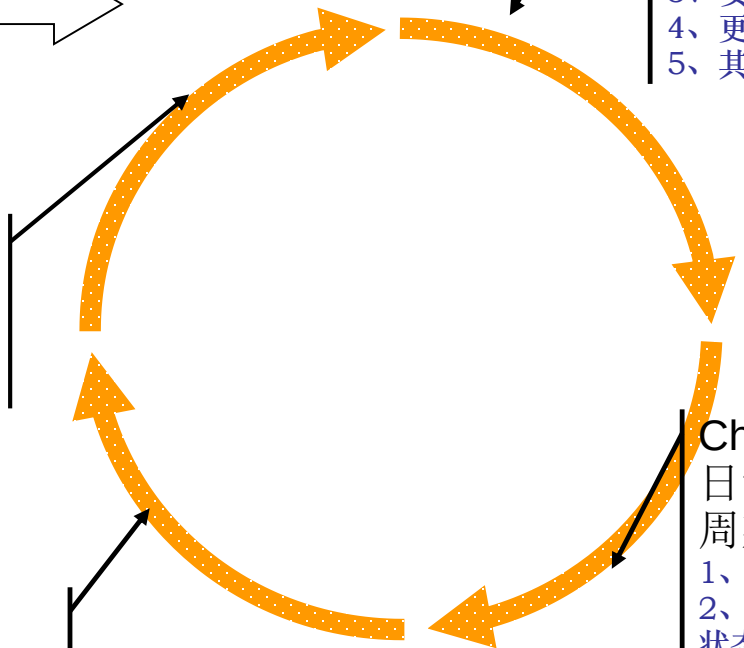
国家电网
STATE GRID
国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

安全运维总体思路

运维阶段 → 运维体系 → 运维目标



安全目标遵循的PDCA执行过程



Do：
安全项目建设
安全维护作业
1、更新资产补丁\拓扑\服务等状态
2、安全事件通报….
3、安全加固
4、更新安全现状和安全目标要求差距
5、其他…..

PLAN：
安全目标要求—安全现状
安全计划（建设；维护…）

Check：
日常安全检查
周期性安全评估
1、检查安全目标要求的完成状态
2、评估安全状况（资产状态；弱点状态），
3、安全现状是否符合可控安全环境

Action：
调整安全目标要求
规划安全项目
绩效考核各部门、安全管理员

国家电网 STATE GRID

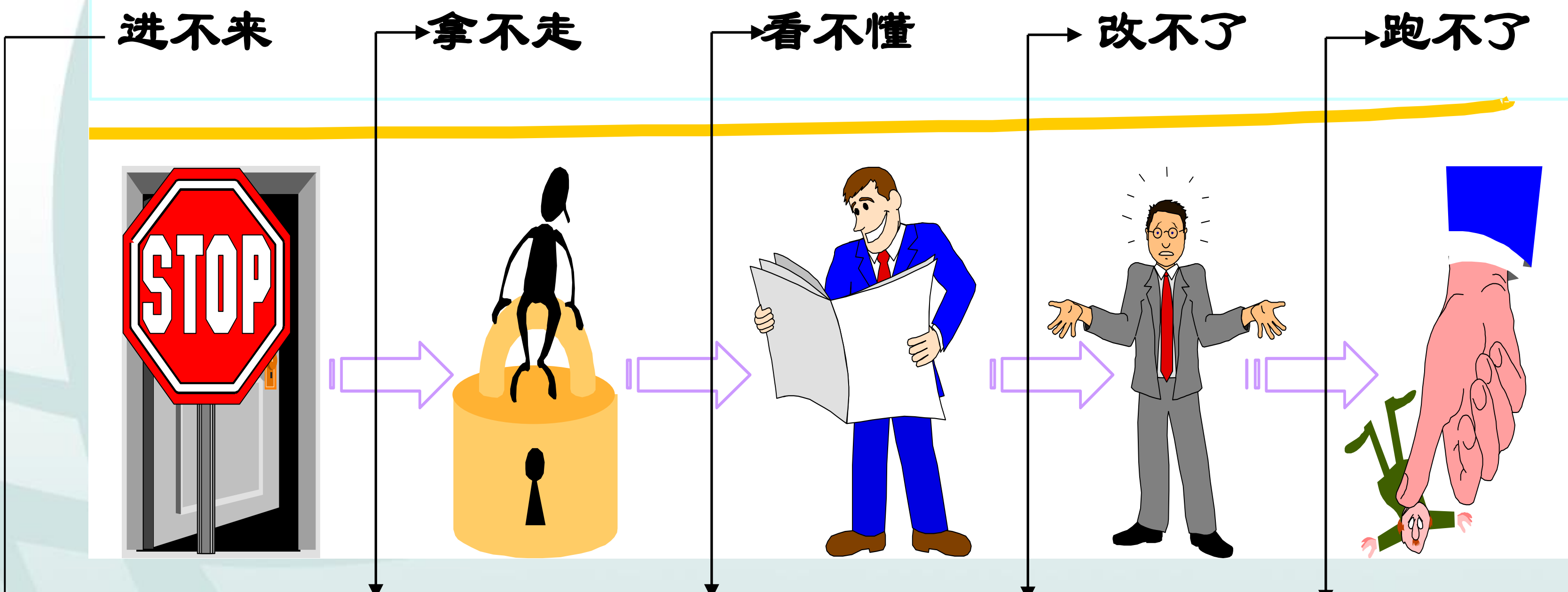
国网信通产业集团北京中电普华公司

BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

安全运维总体思路

运维阶段 → 运维体系 → 运维目标

- **安全工作的目的就是为了在安全法律、法规、政策的支持与指导下，通过采用合适的安全技术与安全管理措施，完成下述网络与信息安全的保障任务。**

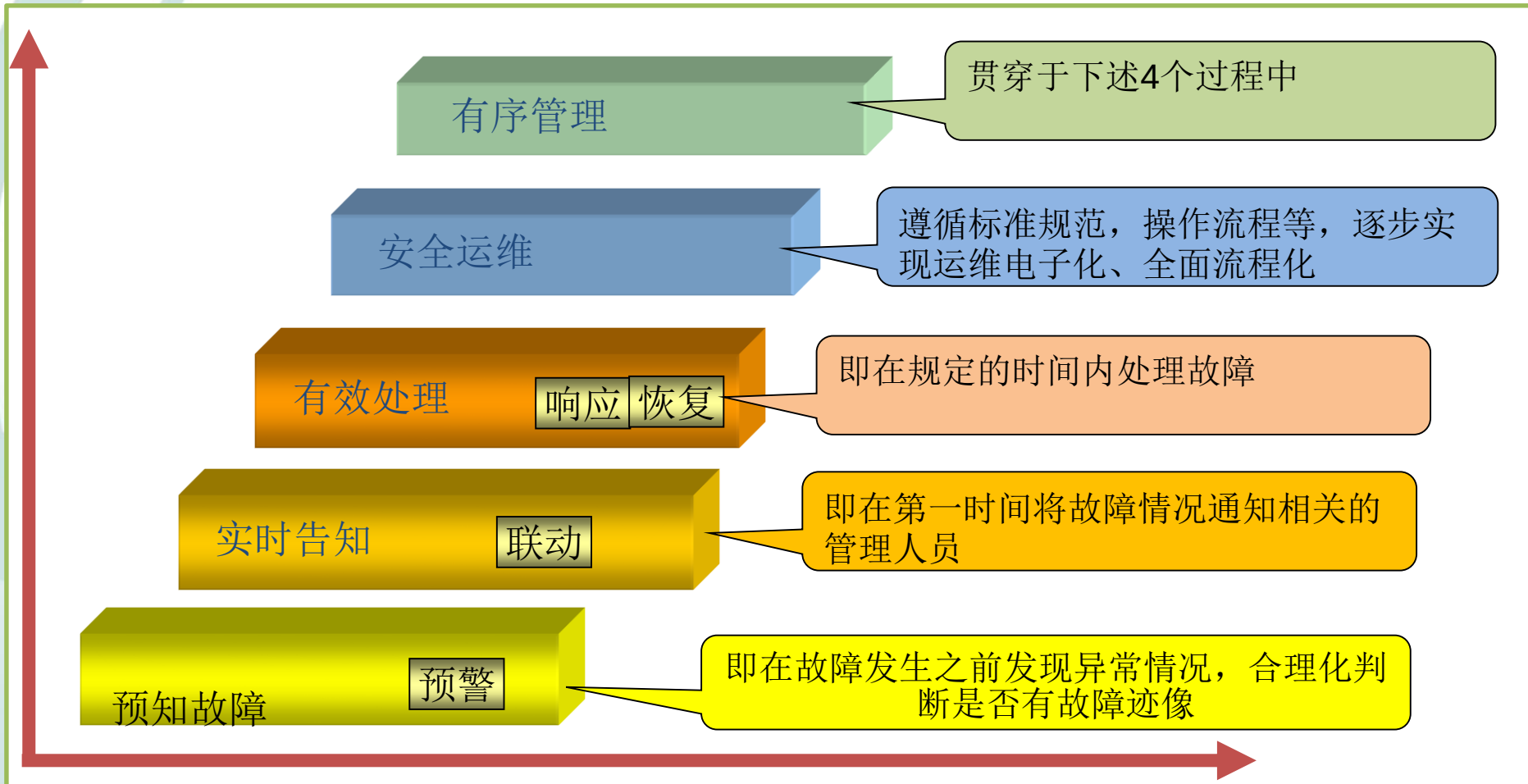


国家电网
STATE GRID
国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

安全运维总体思路

运维阶段 → 运维体系 → 运维目标

保障信息系统的正常运行，要做到：



国家电网
STATE GRID
国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

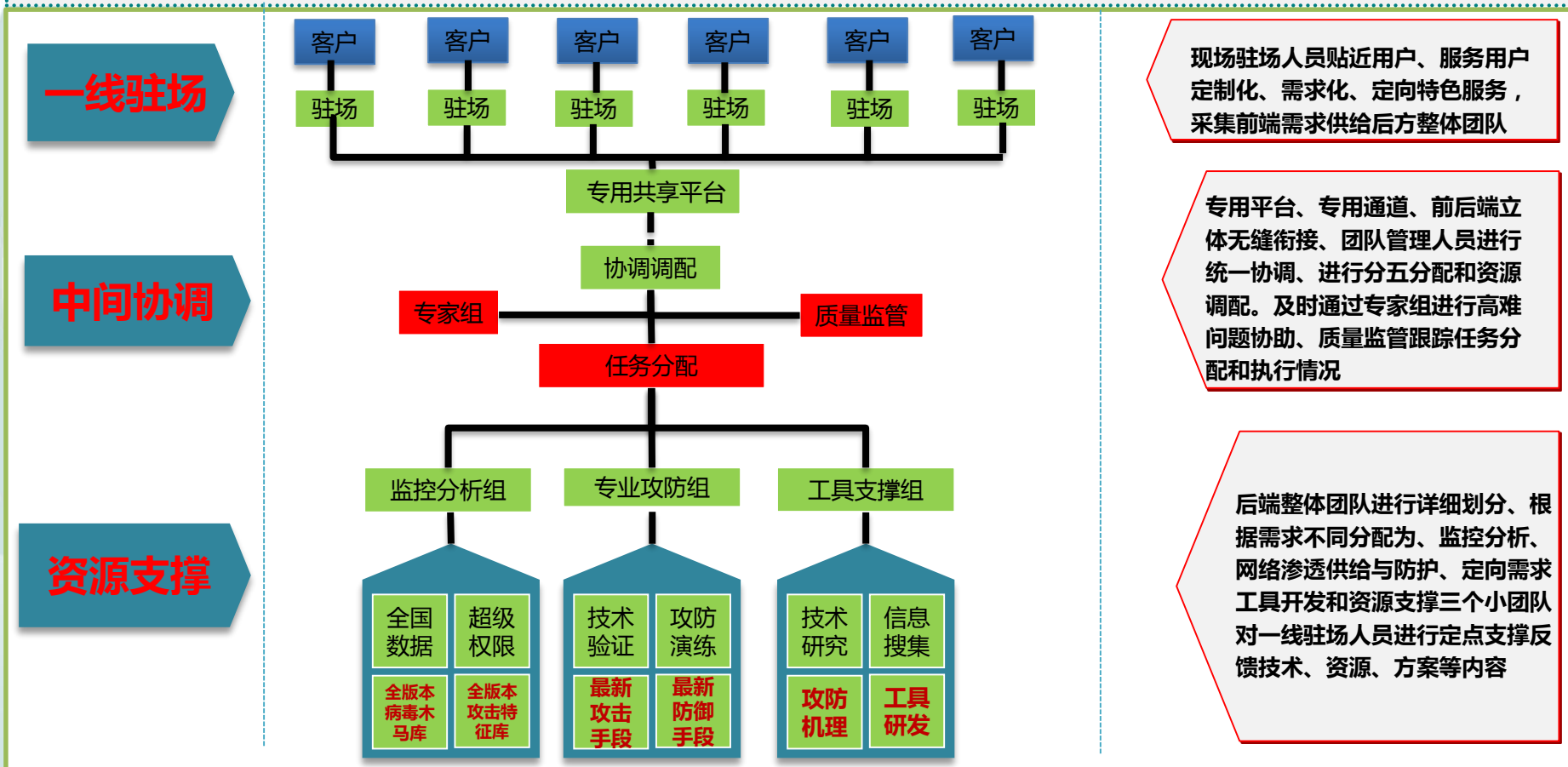
目 录

大型企业安全运维实践

安全运维技术

安全运维方式 → 安全运维工具 → 日志分析

众所周知信息安全服务在企业中主要是人员、技术能力、综合解决方案能力等几个方面，其中人员和协调管理是整个业务的关键点，而安全运维更是需要人、需要综合解决能力的特殊服务项目、普华安全服务团队在总结之前工作方式和方法后，进行了安全运维服务团队的整体调整，如下图所示：



国家电网
STATE GRID

国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

安全运维技术

安全运维技术

通过分析网站日志，我们可以清楚的得知用户是什么IP、什么时间、用什么操作系统、什么浏览器、什么分辨率显示器的情况下访问了你网站的哪个页面，是否访问成功。

无论什么类型的网站日志，有几个记录是最基本的：

1、访问的IP
2、访问的页面
3、访问的时间
4、访问是否成功（HTTP状态吗）

```
[08/Apr/2014:15:04:58 +0800] "GET /struts-2.3.16/ HTTP/1.1" 404 1020
[08/Apr/2014:15:05:00 +0800] "GET /struts-2.3.16/ HTTP/1.1" 404 1020
[08/Apr/2014:15:05:19 +0800] "GET /struts-2.3.16 HTTP/1.1" 302 -
[08/Apr/2014:15:05:19 +0800] "GET /struts-2.3.16/ HTTP/1.1" 404 1020
[08/Apr/2014:15:05:26 +0800] "GET / HTTP/1.1" 200 11450
[08/Apr/2014:15:05:26 +0800] "GET /tomcat.css HTTP/1.1" 304 -
[08/Apr/2014:15:05:26 +0800] "GET /tomcat.png HTTP/1.1" 304 -
[08/Apr/2014:15:05:26 +0800] "GET /bg-upper.png HTTP/1.1" 304 -
[08/Apr/2014:15:05:26 +0800] "GET /bg-nav.png HTTP/1.1" 304 -
[08/Apr/2014:15:05:26 +0800] "GET /asf-logo.png HTTP/1.1" 304 -
[08/Apr/2014:15:05:26 +0800] "GET /bg-button.png HTTP/1.1" 304 -
[08/Apr/2014:15:05:26 +0800] "GET /bg-middle.png HTTP/1.1" 304 -
[08/Apr/2014:15:05:28 +0800] "GET / HTTP/1.1" 200 11450
[08/Apr/2014:15:05:28 +0800] "GET /tomcat.css HTTP/1.1" 304 -
[08/Apr/2014:15:05:28 +0800] "GET /tomcat.png HTTP/1.1" 304 -
[08/Apr/2014:15:05:28 +0800] "GET /bg-upper.png HTTP/1.1" 304 -
```

安全运维技术

通常，无论是任何型号的行为监控设备，安全预警设备，IDS,IPS，防火墙等等，都会有一个特征库，特征库也就是根据特定的关键字，或者特定行为进行判断这个是属于哪种活动，由于我们主要是分析日志，所以外面的主要特征是采用关键字分析这种，更灵活的也可以采用正则，但是正则的贪婪模式也觉决定了匹配效率的性能下降，但是这个已经足够日常的特征匹配分析了。

下面列举一些常见的关键字，当然，实际上规则可能非常多，这里就不一一列举

注入类型的关键字：

select|union|order|by|and|or|like|in|not|is|
|%|0x|char|chr|asc|ascii|substring|<|>|'|*|/|+|-
|=|insert|update|..|delete|load_file|outfile|exec

跨站类型的关键字：

Alert| javascript |Xss

文件包含类型的关键字：

../../|..%5c..%5c

文件上传类型的：

xxx.php.xxx|xxx.asp;.jpg|php1|php2||asa|cer

安全运维技术

安全运维思路 → 安全运维工具 → 日志分析

Web日志安全分析报告

报告生成时间：2015-12-15

恶意IP列表

ID	攻击者IP	所在地区	查　看
1	112.67.37.132	海南省儋州市 电信	查看详细
2	140.240.145.170	海南省 电信	查看详细
3	112.67.43.46	海南省儋州市 电信	查看详细
4	112.67.110.16	海南省海口市 电信	查看详细
5	150.255.89.175	海南省 联通	查看详细
6	59.50.232.83	海南省陵水市 电信	查看详细
7	60.13.118.15	海南省 联通	查看详细

每IP详细访问列表

攻击者IP地址：112.67.37.132	所在地区：海南省儋州市 电信	+展开详情+

ID	访问时间	数据提交方式	访问地址（URL）	攻击方法	浏览器类型	响应码
1	2015-12-06 00:00:15	GET	/ws_person/WebForm_Person.aspx?family_id=64791&ion=97&town=3271&village=0&nature=0&type=&size=10&index=1&Medical=151203023&Family=&enbleFlag=undefined&userName=undefined&exec_id=305&jiaofei_id=	SQL注入攻击	Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/4.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729)	200
2	2015-12-06 00:00:45	POST	/ws_person/WebForm_Person.aspx?family_id=64791&ion=97&town=3271&village=0&nature=0&type=&size=10&index=1&Medical=151203023&Family=&enbleFlag=undefined&userName=undefined&exec_id=305&jiaofei_id=	SQL注入攻击	Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/4.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729)	200
3	2015-12-06 00:01:27	POST	/ws_person/WebForm_Person.aspx?family_id=64791&ion=97&town=3271&village=0&nature=0&type=&size=10&index=1&Medical=151203023&Family=&enbleFlag=undefined&userName=undefined&exec_id=305&jiaofei_id=	SQL注入攻击	Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/4.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729)	200
4	2015-12-06 00:01:34	POST	/ws_PayIndividual/ws_PayIndividual.aspx?exec_id=305&family_id=64791	SQL注入攻击	Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/4.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729)	200
5	2015-12-06 00:01:34	POST	/ws_PayIndividual/ws_PayIndividual.aspx?exec_id=305&family_id=64791	SQL注入攻击	Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/4.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729)	200
6	2015-12-06 00:01:39	POST	/ws_PayIndividual/ws_PayIndividual.aspx?exec_id=305&family_id=64791	SQL注入攻击	Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/4.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729)	200
7	2015-12-06 00:01:50	POST	/ws_PayIndividual/ws_PayIndividual.aspx?exec_id=305&family_id=78157	SQL注入攻击	Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/4.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729)	400
8	2015-12-06 00:01:51	POST	/ws_PayIndividual/ws_PayIndividual.aspx?exec_id=305&family_id=78157	SQL注入攻击	Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/4.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729)	200
9	2015-12-06 00:02:25	GET	/ws_person/WebForm_Person.aspx?family_id=78157&ion=97&town=3271&village=0&nature=0&type=&size=10&index=1&Medical=151203064&Family=&enbleFlag=undefined&userName=undefined&exec_id=305&jiaofei_id=	SQL注入攻击	Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/4.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729)	200
10	2015-12-06 00:02:59	POST	/ws_person/WebForm_Person.aspx?family_id=78157&ion=97&town=3271&village=0&nature=0&type=&size=10&index=1&Medical=151203064&Family=&enbleFlag=undefined&userName	SQL注入攻击	Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/4.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.	200

国家电网
STATE GRID
国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

目 录

大型企业安全运维实践

安全运维保障

安全运维保障

需求分析	只有明了IT系统的安全需求才能有针对性地构建适合于自己的安全体系结构，正确的安全分析需求是保证网络系统安全的根源。
需求分析	风险管理是对需求分析结果中存在的威胁和业务需求进行风险评估，以可以接受的投资，进行最大限度的网络安全防范工作。
制定安全防范策略	根据组织和部门的安全防范需求和风险评估的结论，制定切实可行的计算机网络安全防范策略。
定期安全审核	安全审核的首要任务是审核组织的安全策略是否被有效地和正确地执行。因为网络安全防范是一个动态的过程，安全的需求可能会发生变化；为了在安全需求发生变化时，策略和控制措施能够及时反映这种变化，必须进行定期安全审核。

国家电网
STATE GRID
国网信通产业集团北京中电普华公司
BEIJING CHINA-POWER INFORMATION TECHNOLOGY CO., LTD.
STATE GRID INFORMATION & TELECOMMUNICATION GROUP

安全运维保障

需求分析	只有明了IT系统的安全需求才能有针对性地构建适合于自己的安全体系结构，正确的安全分析需求是保证网络系统安全的根源。
风险管理	风险管理是对需求分析结果中存在的威胁和业务需求进行风险评估，以可以接受的投资，进行最大限度的网络安全防范工作。
制定安全防范策略	根据组织和部门的安全防范需求和风险评估的结论，制定切实可行的计算机网络安全防范策略。
定期安全审核	安全审核的首要任务是审核组织的安全策略是否被有效地和正确地执行。因为网络安全防范是一个动态的过程，安全的需求可能会发生变化；为了在安全需求发生变化时，策略和控制措施能够及时反映这种变化，必须进行定期安全审核。
管理制度	通过技术手段保障管理制度有效贯彻执行，通过技术手段，进行有效的网络边界控制；保证系统补丁、防病毒软件安装执行情况；监督最先安全事件源；建立安全防护监控体；进行有效的风险评估。
绩效考核	自查自评、日常监测、检查评议、结合日常工作和年度任务综合评价。
日常作业管理	对日常运行维护工作进行管理，是一些周期性的、相对固定的日常维护作业管理。目的是规范日常作业计划、规范日常作业内容、规范维护人员行为、为人员考核提供基础依据。
加强人员培训	加强培训以保障管理机制执行，提高运维人员的技能和安全意识，对运维人员的安全意识的培养、安全技能的教育伴随着整个安全治理工作全程，不会仅限于某个特定步骤。

谢谢！