



ISC 互联网安全大会



360 互联网安全中心



工业互联网的安全实践-海安盾

海尔集团

ISC 互联网安全大会 | 中国·北京
2018 Internet Security Conference | China · Beijing



ISC 互联网安全大会



360 互联网安全中心

目录



海安盾介绍

海安盾赋能COSMOPLAT平台

海安盾平台自身能力

海安盾未来规划

ZERO-TRUST SECURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 | 中国·北京
2018 Internet Security Conference | China · Beijing
INDUSTRIAL AUTOMATION

海安盾定位

构建工业互联网生态圈安全态势智能感知，敏捷安全响应的统一平台，实现工业互联网全链条安全可感、可控、可防。



ZERO-TRUST SECURITY



安全态势感知平台多级联动

- 资产发现
- 安全预警
- 安全扫描
- 多源情报
- 安全响应
- 安全关差

静 → 动 → 感



ISC 互联网安全大会



360 互联网安全中心

目录

海安盾介绍



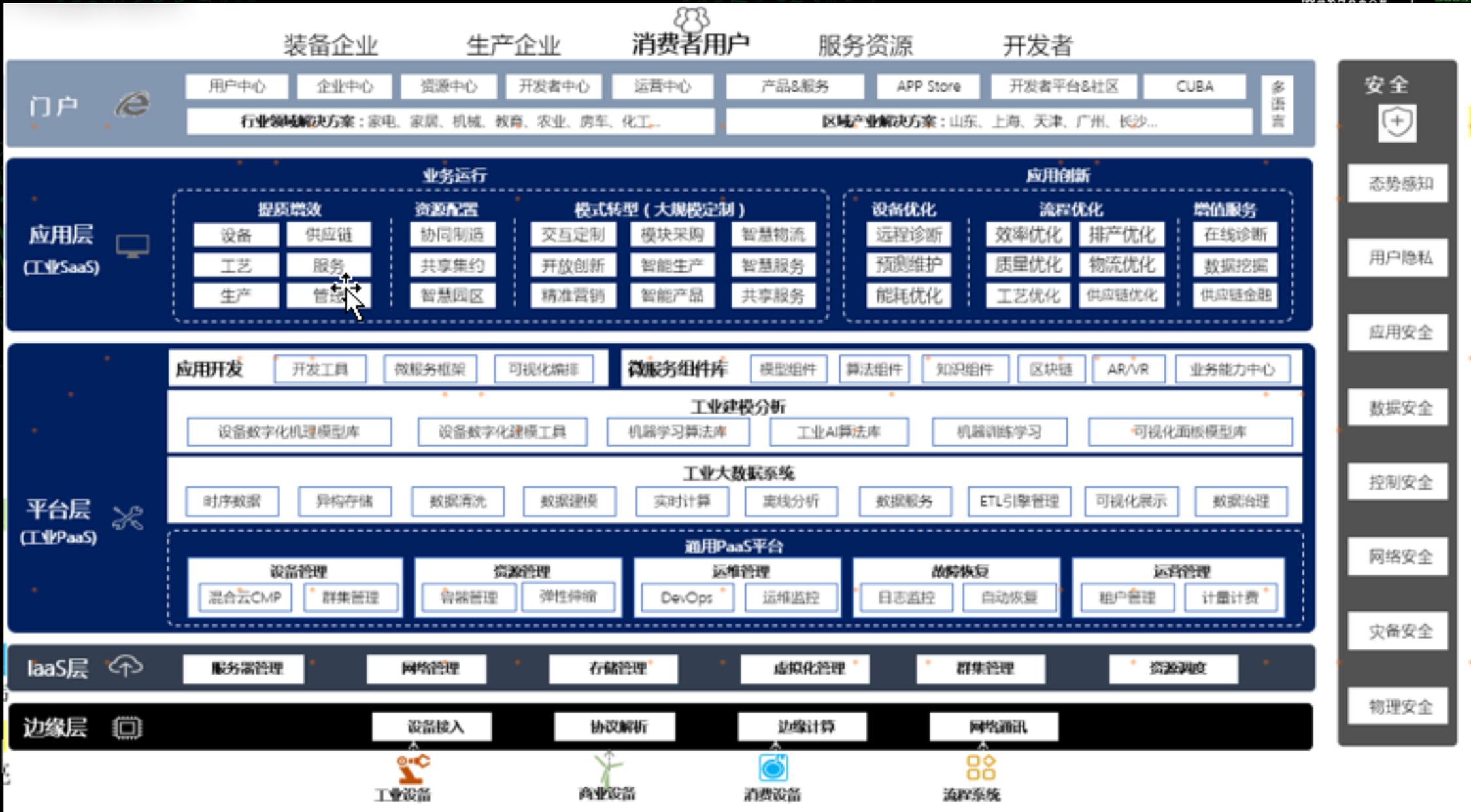
海安盾赋能COSMOPLAT平台

海安盾平台自身能力

海安盾未来规划

ZERO-TRUST SECURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 | 中国·北京
2018 Internet Security Conference | China · Beijing
INDUSTRIAL AUTOMATION



安全架构

- 数据中心安全
- 办公区域安全
- 工控安全架构

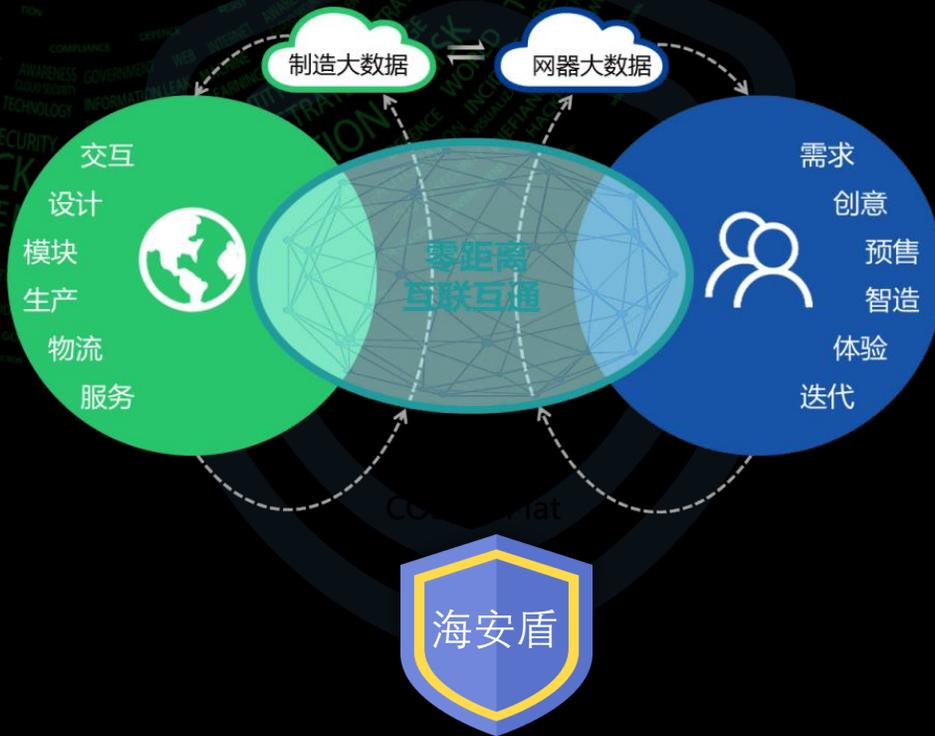
基础架构安全

- 网络主机安全
- 工控设备安全
- 互联网应用安全

应用安全

- Web/App安全
- 安全开发周期
- 业务流程安全

工控应用安全



数据安全

- 数据分类保护
- 用户隐私保护
- 数据加密
- 数据防泄漏

账号权限和访问

- 认证和访问
- 账号生命周期
- 证书管理体系

安全事件管理

- 日志收集和存储
- 日志关联
- 威胁分析和溯源

态势感知

实时监控

敏捷响应

安全审计

安全认证

工控安全



ISC 互联网安全大会



360 互联网安全中心

目录

海安盾介绍

海安盾赋能COSMOPLAT平台



海安盾平台自身能力迭代

海安盾未来规划

ZERO-TRUST SECURITY

WEB INTERNET
 INFORMATION LEAK TECHNOLOGY
 TERMINAL AGE
 PERSONAL PRIVACY IDENTITY SECURITY
 IDENTITY
 AUTHENTICATION
 ISC 互联网安全大会 中国·北京
 2018 Internet Security Conference China · Beijing
 INDUSTRIAL AUTOMATION

09:46:06
18/08/29

告警 APT 攻击 网络流量

受害者 异常行为 攻击溯源

网络流量

物联网安全态势感知

资产总数

扫描 356 | 漏洞 20 | 木马 129 | web攻击 1056

告警及阻断次数

攻击来源TOP5

192.168.1.100	27.223.82.138	66.111.57.22	58.218.56.110	112.6.125.237
---------------	---------------	--------------	---------------	---------------

攻击目的TOP5

10.115.37.124	10.138.111.23	10.115.108.712	10.115.11.168	10.118.1.199
---------------	---------------	----------------	---------------	--------------

攻击列表

时间	攻击源IP	攻击源国家	攻击目标IP	攻击目标国家	攻击类型	等级
09:40:37	42.119.39.178	越南	10.115.11.168	中国	攻击_远程命令执行	
09:41:13	192.158.238.104	美国	10.115.11.168	中国	扫描探测_网络爬虫	
09:41:22	192.158.238.104	美国	10.115.11.168	中国	扫描探测_网络爬虫	
09:41:37	183.146.185.116	中国	10.115.11.168	中国	攻击_Webshell	
09:41:42	47.75.74.28	加拿大	10.115.11.168	中国	攻击_漏洞攻击	
09:41:56	80.82.70.118	荷兰	10.115.11.168	中国	扫描探测_端口扫描	
09:42:14	183.26.240.6	中国	10.115.11.168	中国	攻击_http_访问	
09:44:24	35.4.64.98	中国	10.115.11.168	中国	攻击_http_访问	

目的系统TOP5

事件实时统计

应用安全响应中心

互联网漏洞总数 32

已修复的漏洞总数 32

超过15天未修复的漏洞数 0

扫描漏洞明细

安全运营中心

工业控制网络

互联网

工控系统

工控系统

物联网终端扫描中心

产业维度漏洞总数

物联网安全事件中心

事件总数 23490

高危事件 149

中危事件 162

低危事件 1000

SQL注入漏洞

事件来源TOP5

物联网业务稳定监控

平均响应时间 91.11 ms

峰值响应时间 4.634.262 ms

城市维度性能最慢T单位: op5

系统维度性能最慢T单位: 5

物联网访问攻击分析

产业维度访问次数占比

系统维度访问次数占比

年累计告警总次数 66,519,835

IP地址告警次数TOP10

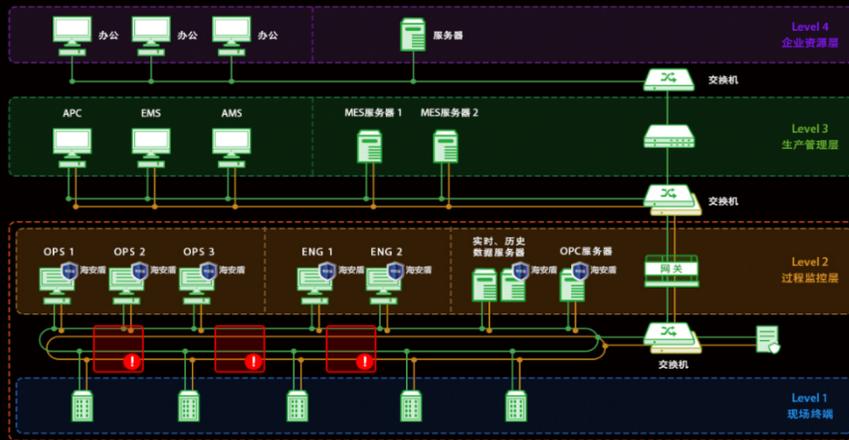
产业维度告警次数占比

系统维度告警次数占比

注: 取数范围为 2h

物联网安全事件中心

事件总数 186129



告警			
时间	源	目的	类型
2018-08-28 16:47:30	10.136.115.22	93.89.226.17	
2018-08-28 16:47:29	10.136.115.22	206.189.61.126	
2018-08-28 16:39:44	10.136.116.12	212.61.180.100	
2018-08-28 16:06:35	10.136.116.12	192.168.100.2	
2018-08-28 16:06:35	192.168.100.2	10.136.116.12	
2018-08-28 15:37:19	10.136.115.22	93.89.226.17	
2018-08-28 15:37:18	10.136.115.22	206.189.61.126	
2018-08-28 15:33:28	10.136.116.12	212.61.180.100	

PLC: #施耐德 #GE #罗克韦尔 #西门子1200
协议: #MODBUS #OPC-DA #S7 #EGD #ENIP #TOTAL



行业首个全流程IOT融合安全解决方案。

ISC 互联网安全大会 中国·北京
2018 Internet Security Conference China · Beijing



ISC 互联网安全大会



360 互联网安全中心

目录

海安盾介绍

海安盾赋能COSMOPLAT平台

海安盾平台自身能力迭代



海安盾未来规划

ZERO-TRUST SECURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 | 中国·北京
2018 Internet Security Conference | China · Beijing
INDUSTRIAL AUTOMATION

Haier 海安盾未来规划



ISC 互联网安全大会



360 互联网安全中心

升级路径

行业
(生态共赢)

平台
(万务互联)

方案
(随时随地)

海安盾

- 突破软硬件安全厂商束缚
- 企业级安全统一平台

海安盾平台

- 工业互联网平台的安全解决方案
- 工业互联网生态安全共享平台
- 国家、省、企业三级联动安全治理

海安盾生态

- 赋能行业，安全标准化
- 共享安全情报，响应国家安全

驱动机制

18

18

19-

战略支撑

- 国家安全战略
- 中国制造2025
- 集团物联网战略

生态资源

- 国家监管部门
- 电信运营商
- 行业协会
- 安全生态合作伙伴(360等)

社会化用户群体

- 覆盖全行业，包括大型企业和中小型企业；
- 可为大型企业提供定制服务；

核心技术

- 威胁情报
- 企业安全数据
- 业务应用数据
- 算法分析与模型
- 威胁预警

ZERO-TRUST SECURITY

ISC 互联网安全大会 中国·北京
2018 Internet Security Conference China · Beijing



ISC 互联网安全大会



360 互联网安全中心

THANKS

ISC 互联网安全大会 | 中国·北京
2018 Internet Security Conference | China·Beijing