

2018 THINK IN CLOUD BEIJING

# 云平台安全漏洞修复实践



王超

Ucloud内核研发工程师

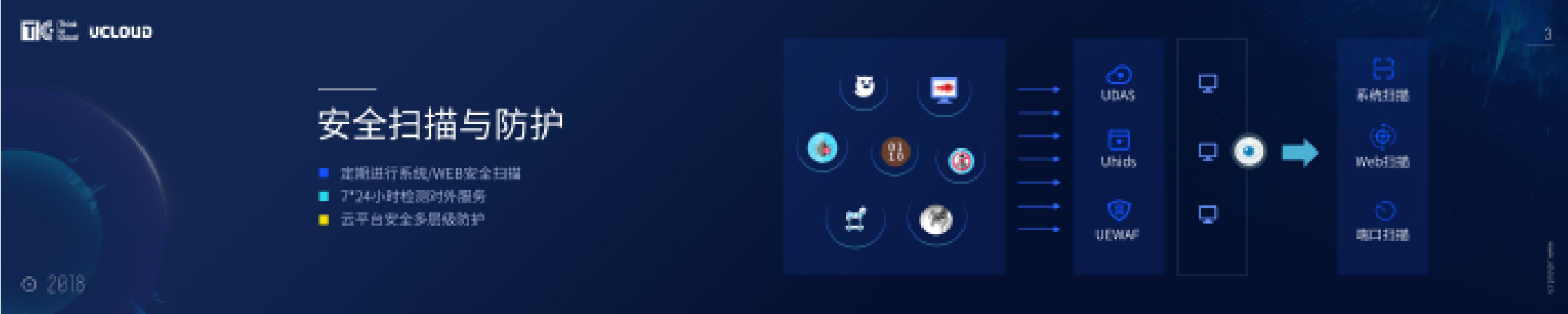
# 目 录

- |    |             |    |         |    |       |
|----|-------------|----|---------|----|-------|
| 01 | 漏洞采集与响应     | 02 | 安全扫描与防护 | 03 | 云安全体系 |
| 04 | 固件升级、模块动态替换 | 05 | 热补丁技术   | 06 | 云主机迁移 |

# 漏洞采集与响应

- 白蓝漏洞采集平台
- 7\*24小时监控
- 应急响应中心 (SRC)





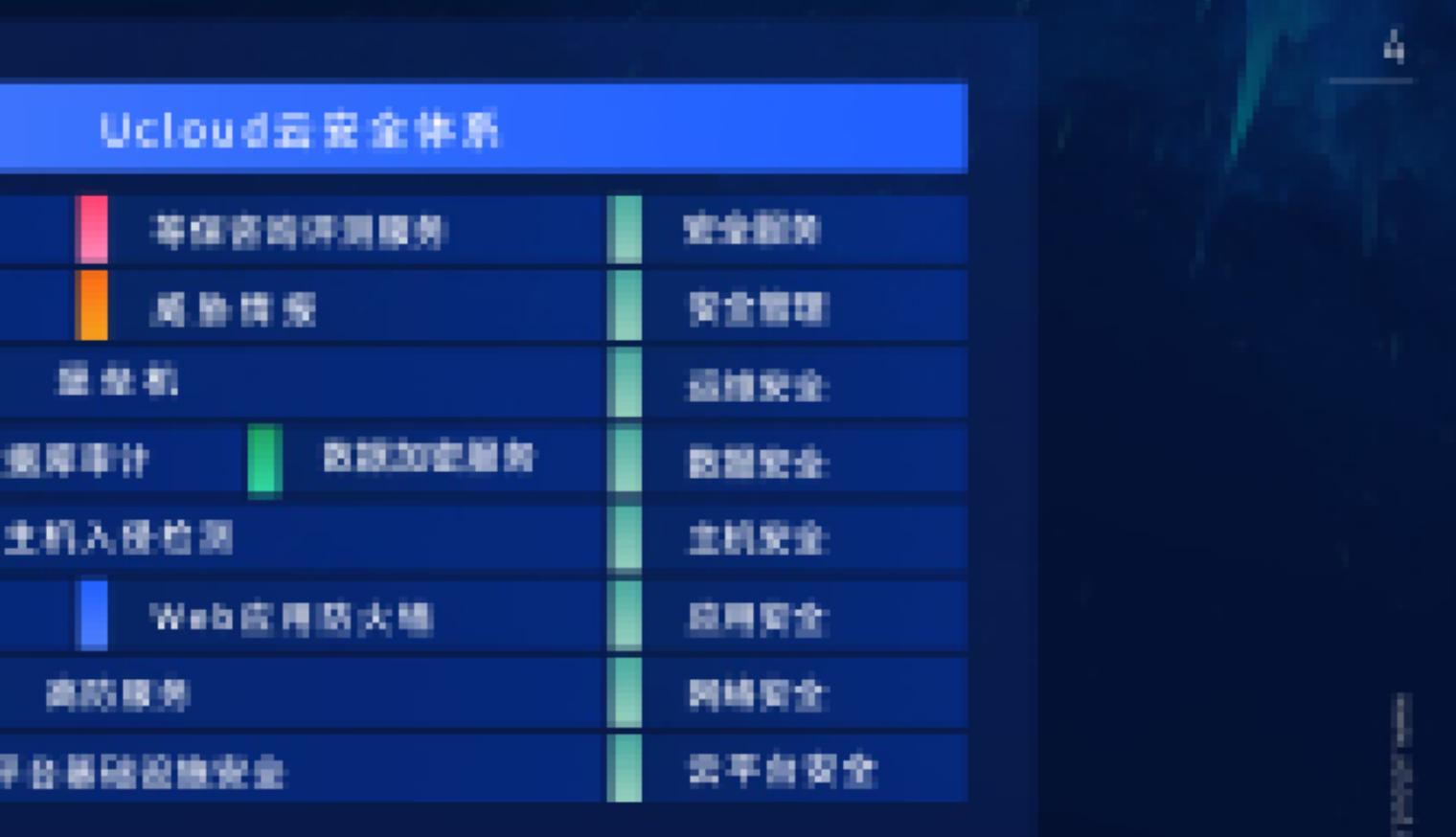
## 安全扫描与防护

- 定期进行系统/WEB安全扫描
- 7\*24小时检测对外服务
- 云平台安全多层级防护



本系

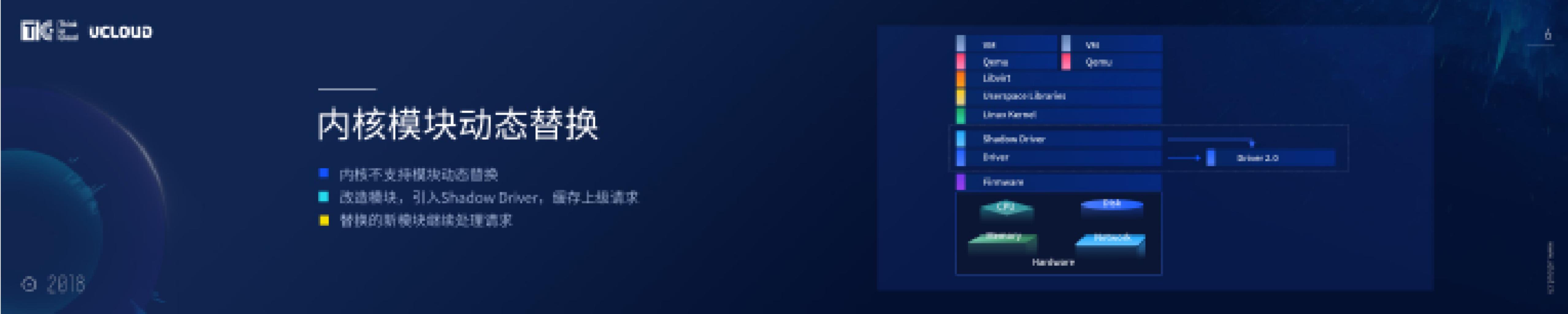
- 识别安全风险 ■ 提供安全管理与方案 ■ ISO证书



# 固件升级

- 固件是硬件设备的“操作系统”，
- 常见于BIOS、RAID卡、CPU Micro-code等
- 在线升级固件：修复bug、性能问题等





## 内核模块动态替换

- 内核不支持模块动态替换
- 改造模块，引入Shadow Driver，缓存上级请求
- 替换的新模块继续处理请求





## 热补丁技术 CONT.

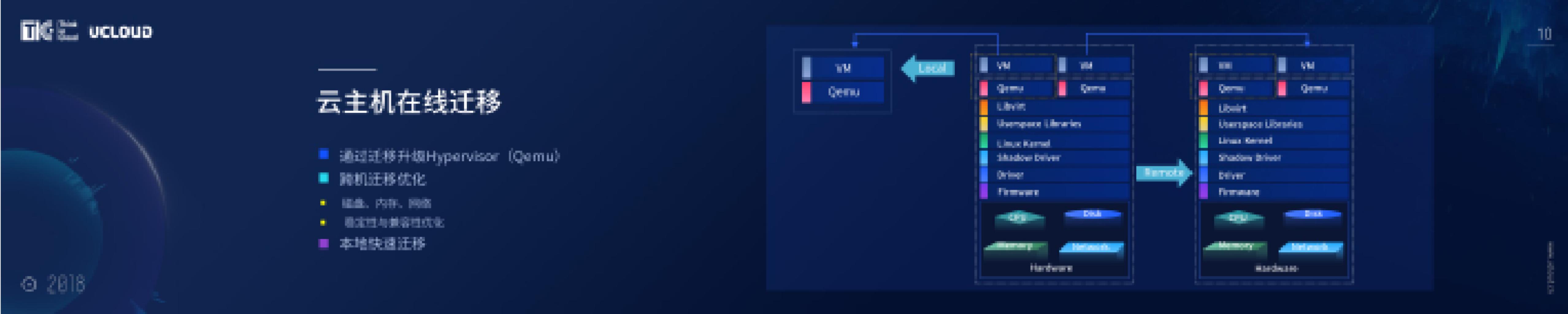
- 基本修复原理
- 修改内存中函数的头部，实现旧函数调用到新函数



## 热补丁技术 cont.

- 热补丁生成原理
  - 对比被加固后二进制代码
  - 变更修复代码
  - 编译成对加密的模块





THANKS