

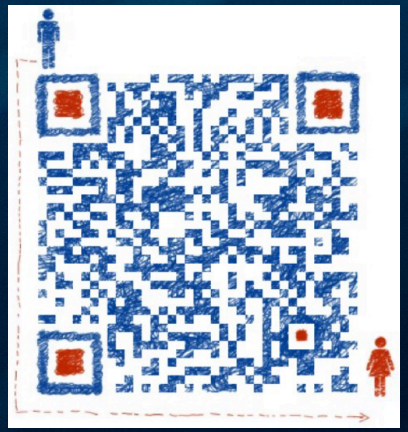
Elasticsearch 安全防护

Medcl

关于我

近 10 年 Elasticsearch 使用经验，
Elastic 中国区第一位员工，工号 001。

@medcl
https://medcl.com



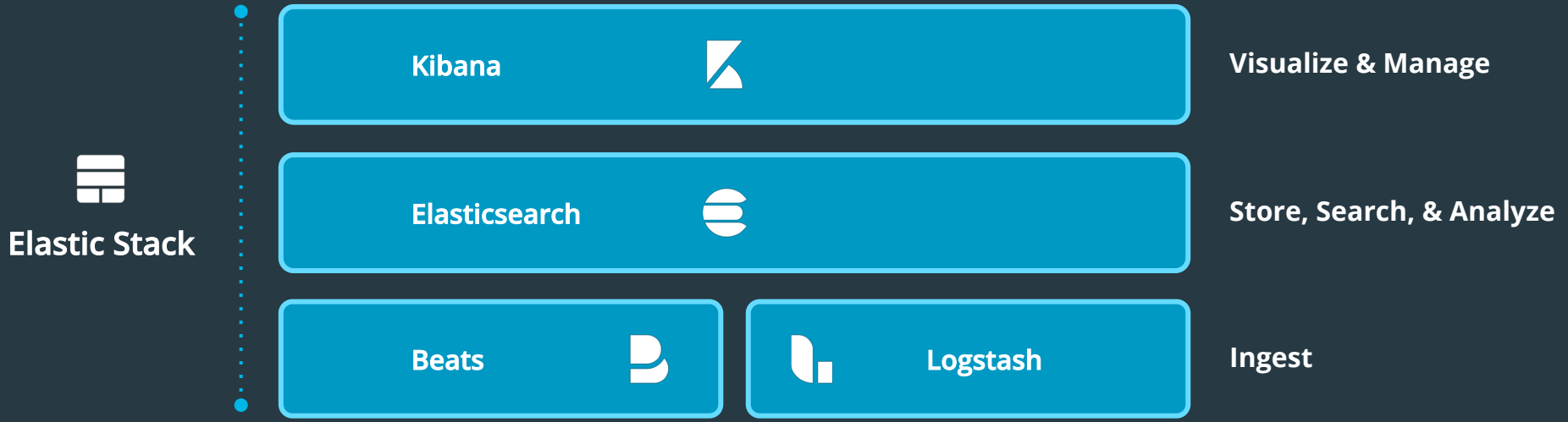


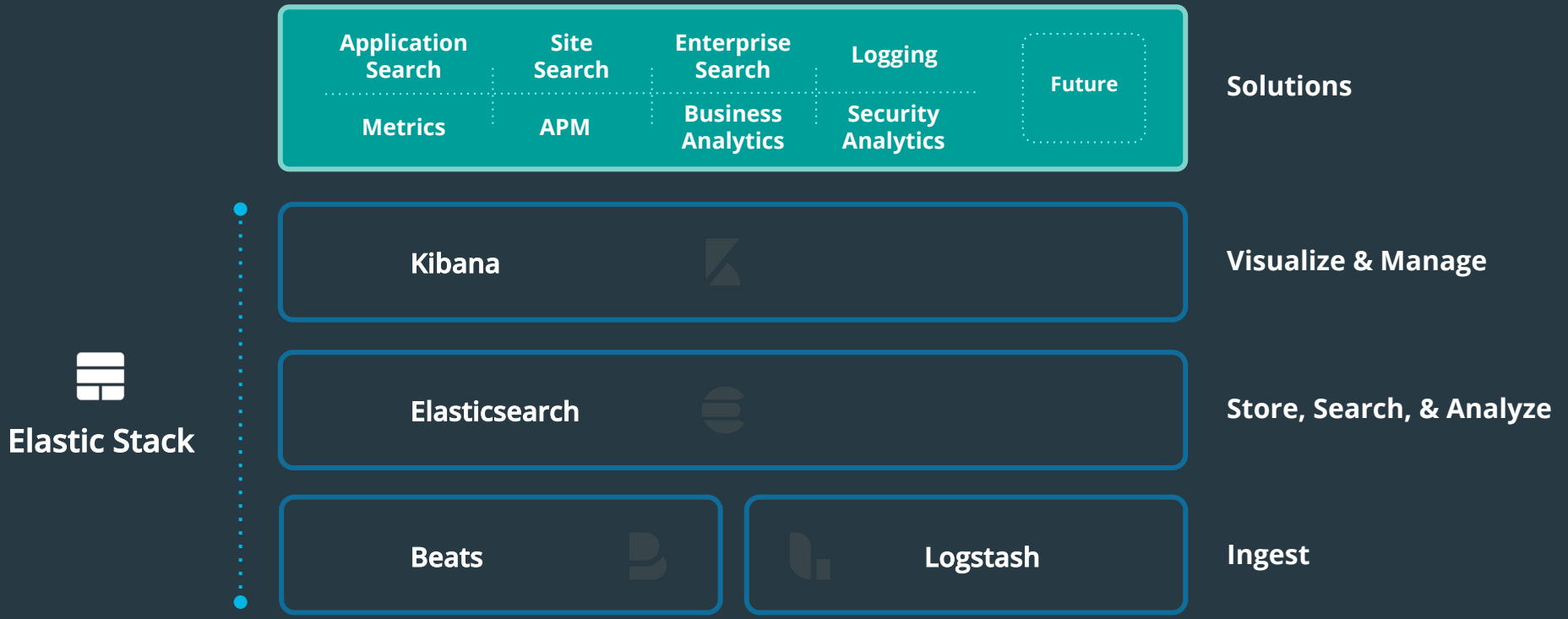
elastic

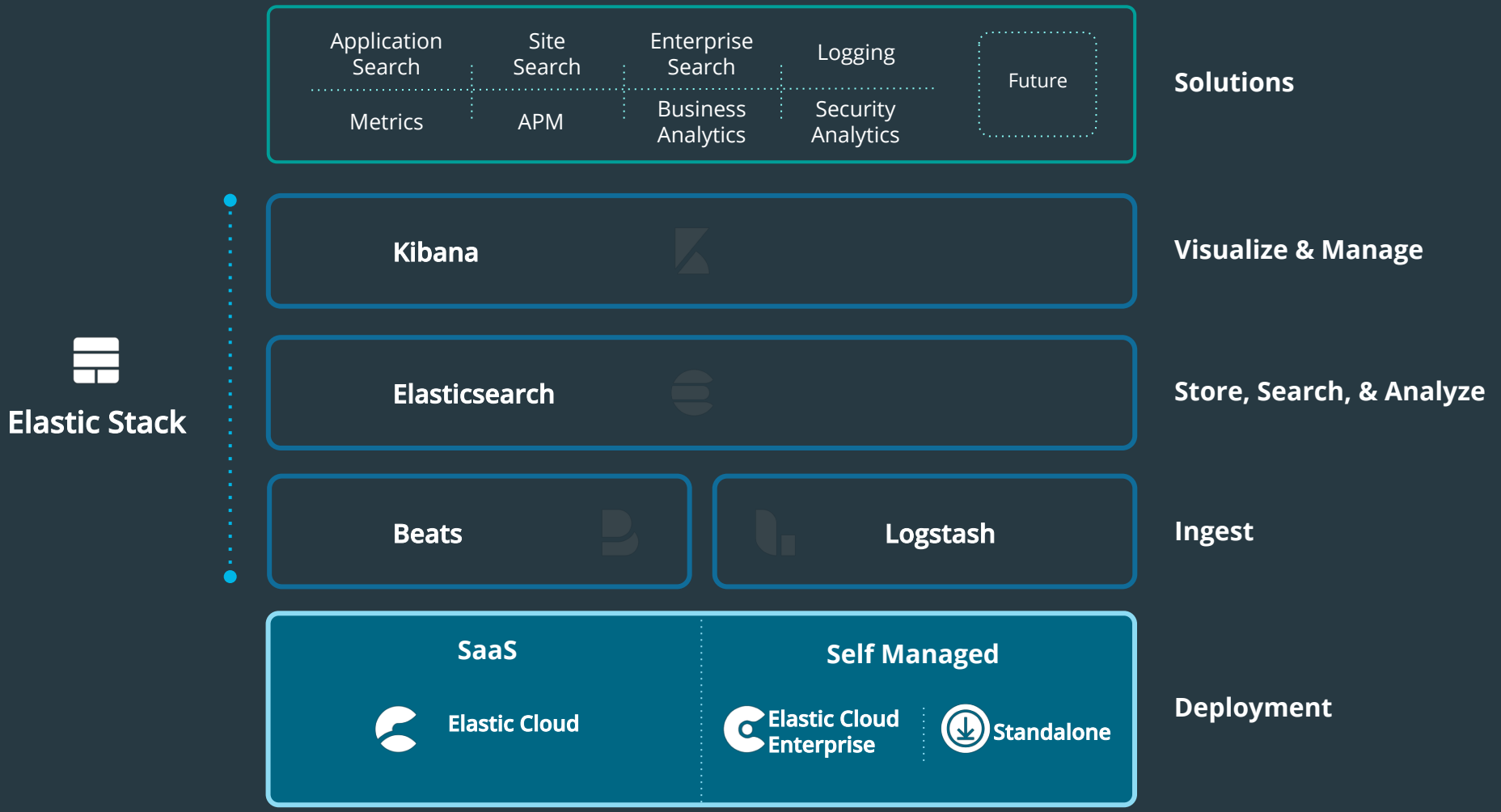
Elastic is a Search Company！

工作机会：http://grnh.se/iup1q61




Elastic Stack
Kibana
Visualize & Manage
Elasticsearch
Store, Search, & Analyze
Beats
Logstash
Ingest


Application Search
Site Search
Enterprise Search
Logging
Metrics
APM
Business Analytics
Security Analytics
Future
Solutions
Kibana
Visualize & Manage
Elasticsearch
Store, Search, & Analyze
Beats
Logstash
Ingest
Elastic Stack


Application Search
Site Search
Enterprise Search
Logging
Metrics
APM
Business Analytics
Security Analytics
Future
Solutions
Kibana
Visualize & Manage
Elasticsearch
Store, Search, & Analyze
Beats
Logstash
Ingest
Elastic Stack
SaaS
Elastic Cloud
Self Managed
Elastic Cloud Enterprise
Standalone
Deployment

历经千辛万苦，
ELASTICSEARCH 上线了！

elastic

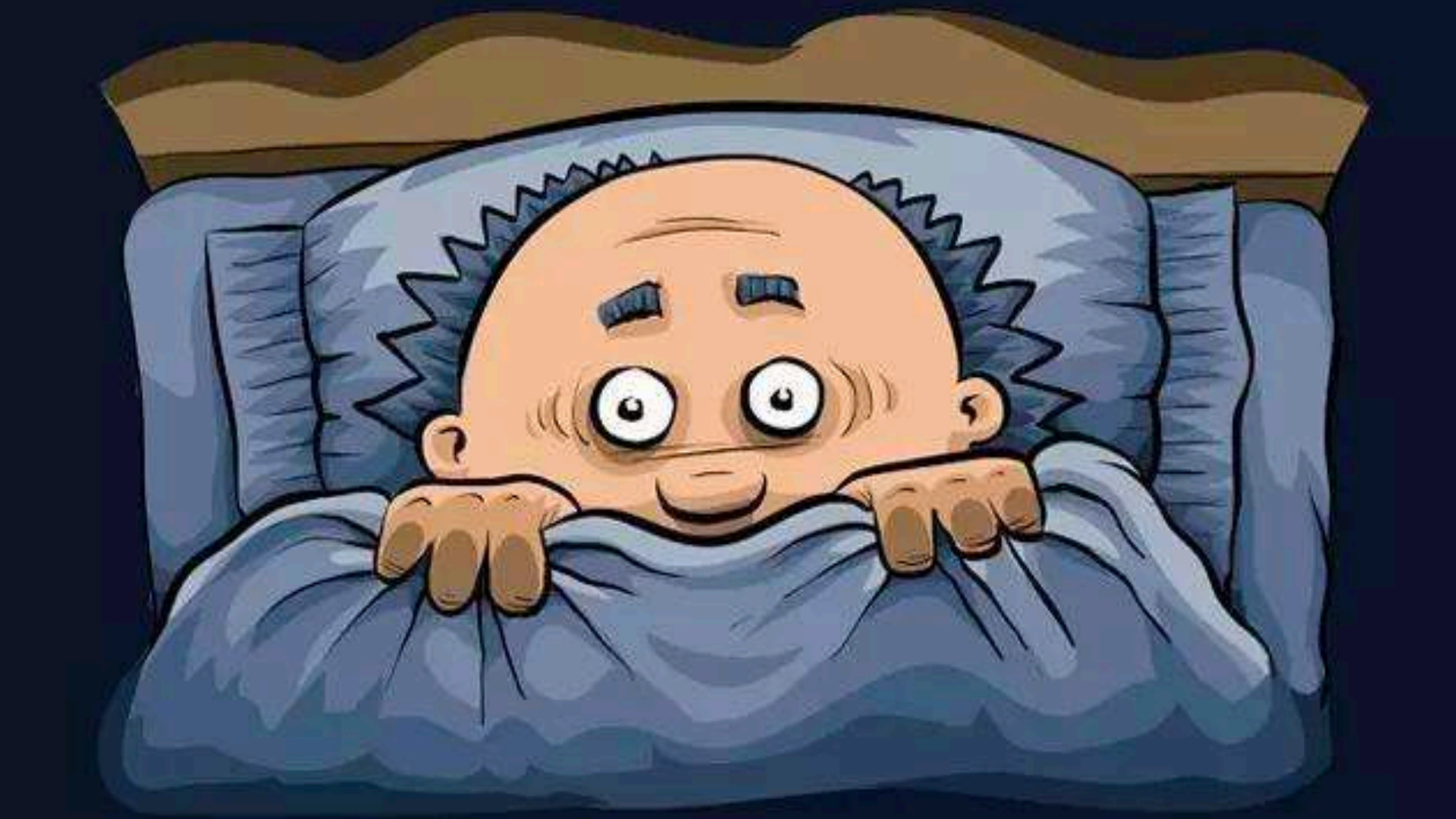

升职加薪，当上总经理，赢取白富美，走上人生巅峰。


不好意思，
我也是这样想的。



Elasticsearch 数据泄露

Google 搜索　手气不错



数据监管正受重视

安全法规相继出台

GDPR

2016年4月14日由欧洲议会（TheEuropean Parliament）投票通过，并于2018年5月25日起在所有欧盟成员国正式生效的一部对欧盟公民个人数据保护的法案。

网络安全法

2017年6月1日，我国首部《网络安全法》正式施行，这是我国网信法治领域的重大事件。

巨额罚单

谷歌的母公司 Alphabet 最高将面临 37 亿欧元罚款，Facebook 及其两家子公司 WhatsApp 和 Instagram 分别最高面临13亿欧元罚款。





数据千万条，安全第一条，
集群不设防，亲人两行泪 ...

流浪程序员

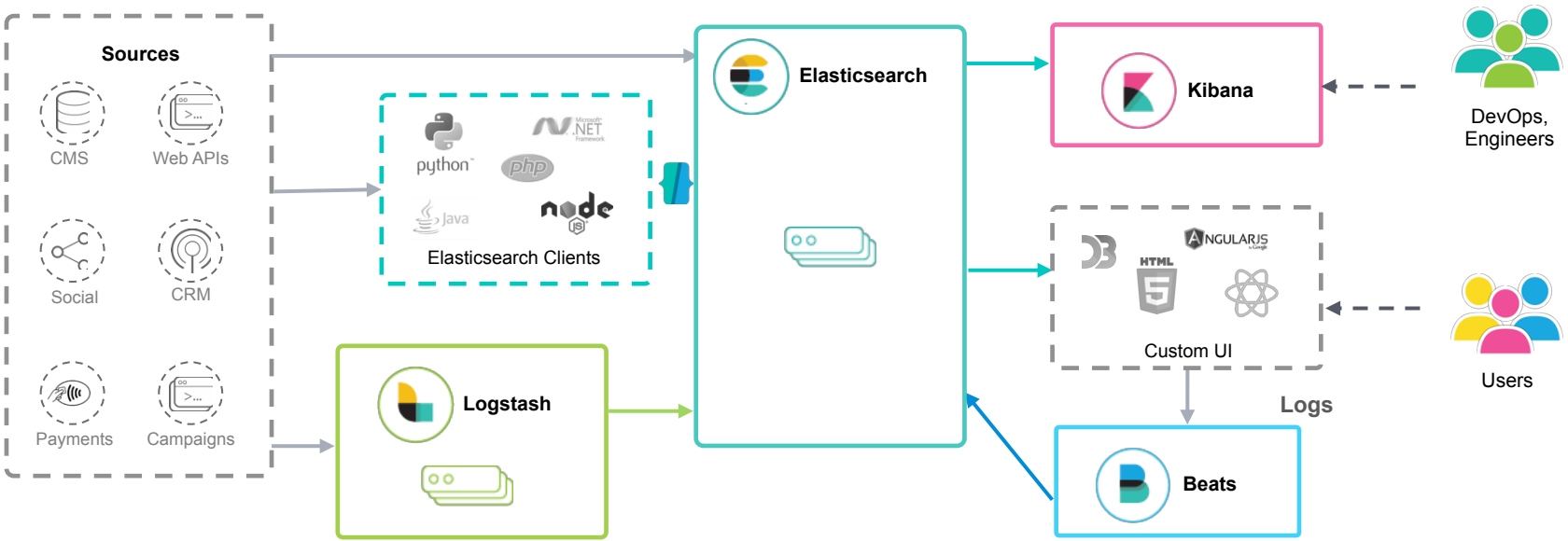
elastic

数据都是如何泄露出去的？

请问你知道不知道你不知道和知道的不知道和知道（安全风险）么？

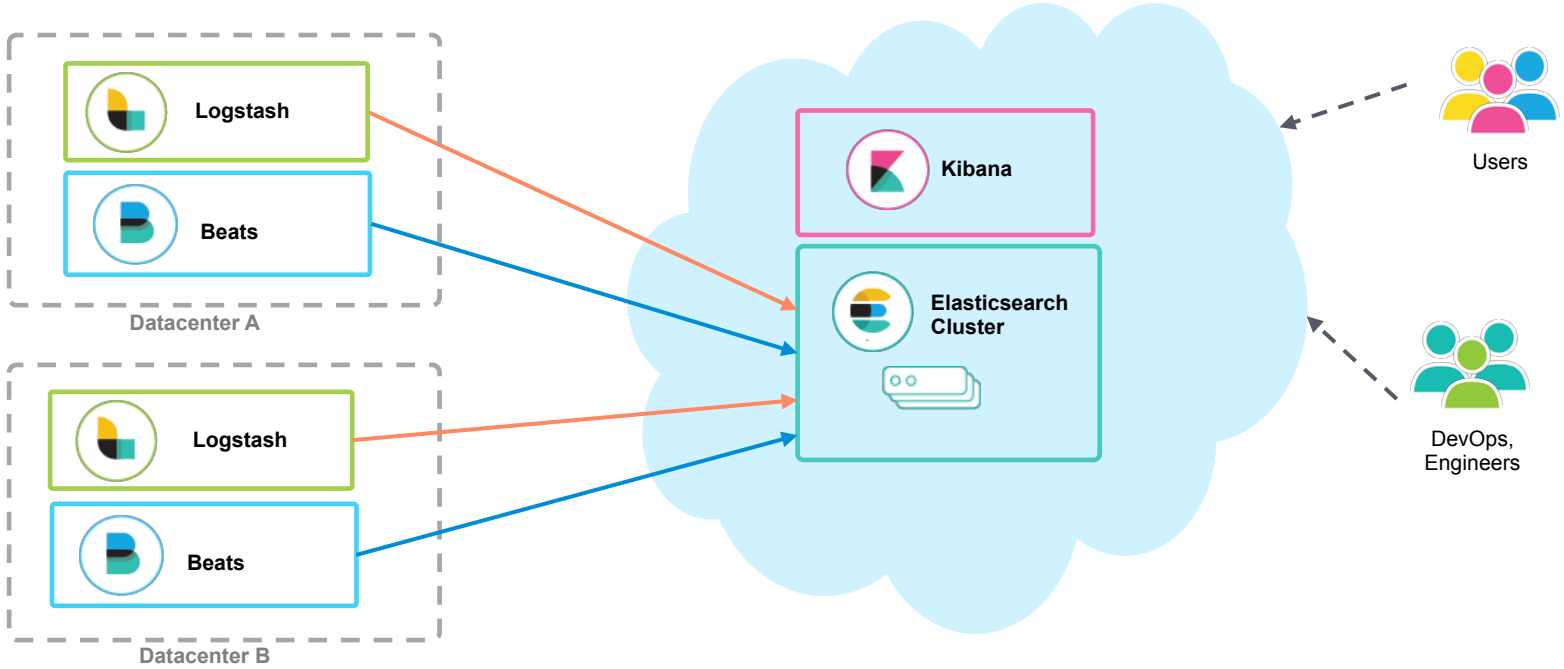
elastic

一个典型的 ELK 应用架构



elastic

云端的 Elasticsearch



elastic

一个典型的部署架构



elastic



安全是一个系统工程！

德华

elastic

网络传输

- Elasticsearch 的 RESTful 接口使用的是 HTTP 协议，属于明文传输
- 潜在威胁
  - 嗅探攻击
  - 旁路攻击
  - 中间人攻击
- 脆弱位置
  - 从 API 到接口调用方的网络传输
  - Elasticsearch 节点间的网络传输
  - 负载均衡器到 Elasticsearch 与 API 之间的网络传输
  - 服务器到浏览器之间的网络传输
  - CDN 网络传输（避免）



elastic

网络传输

- 网络流量隔离
  - 独立 VLAN
- 防火墙
- IP 策略
- 交换机 ACL
- 节点间流量加密，如 stunnel
- 对外节点加一层反向代理，如 Nginx
- 加密传输
  - 安全配置的 TLS
- 接口调用可考虑双向校验证书



elastic

Elasticsearch

- Elasticsearch 是一个分布式的复杂系统，涉及到很多组件、模块及外部参与方
- 脆弱位置
  - Elasticsearch节点及集群，本身及部署环境
  - 中间传输层，如 Kafka、Nginx等
  - 数据采集方，如 Logstash、Beats 等
  - Elasticsearch 消费方，如 web 应用，Kibana 等
- 潜在威胁
  - 未授权访问
  - 越权访问
  - 恶意节点加入
  - 数据恶意删除
  - 脚本注入攻击
  - 沙盒逃逸攻击
  - DOS 攻击
  - 跨域请求伪造
  - 跨站脚本攻击
  - 数据泄露
  - …



elastic

Elasticsearch

- 身份认证
- 数据鉴权
- 限制集群陌生新节点的加入
- 磁盘文件的加密
- JVM Security Management
- 使用安全的带沙盒机制的脚本，限制脚本操作
- API 访问限制与白名单子集准入
- 合理的跨域设置
  - http.cors.enabled
- 限制客户端查询的构造
- 进程及资源隔离（容器/用户）



elastic

Elasticsearch

- 插件的安全性评估与审计
- 开启审计日志，单独存放并记录用户操作
- 正确设置 Elasticsearch 的数据目录
- 给 Elasticsearch 所在的服务器加固
- 禁用批量删除索引
- 不要暴露 Elasticsearch 在公网上
- 集群节点角色分离
- 禁用不必要的服务
  - 可选择只对外暴露协调节点，关闭 master 等节点 9200
  - 停掉服务器上的其他不必要的服务



elastic

反向代理

- 身份认证
- TLS
- 限速
- 限流
- 记录访问日志
- 限制 Verb
- 常见错误
  - 用了 Basic 身份认证却不开启 TLS
  - 弱密码
  - 弱证书



elastic



性能不是裸奔的理由！

许仙

elastic

数据采集

- Beats、Logstash 等工具分散运行在网络内各个系统内，用于采集各种类型的数据，通过 API 将数据发送到 Elasticsearch
- 潜在威胁
  - 网络嗅探监听
  - 请求截获
  - 密码泄露
  - 恶意修改的版本
  - 后门植入
  - 数据泄露
- 脆弱位置
  - 配置文件
  - 传输过程
  - 程序本身



elastic

数据采集

- 从可信官网下载程序包
- 校验程序包完整性
- 不要在配置文件内使用明文密码
- 使用 Keystore 代替明文密码
- 按采集类型创建单独角色，限制为只写权限和接口
- 使用单独的用户运行程序
- 文件目录的权限合理设置
- 使用加密传输协议发送数据到 Elasticsearch



elastic

Kibana

- 潜在威胁
  - 非授权与越权访问
  - 跨站脚本攻击（XSS）
  - 跨域请求伪造（CSRF）
  - 数据恶意删除
  - 数据恶意泄露
  - 分析指标泄露
  - …
- 脆弱位置
  - 使用人员
  - Kibana 服务器
  - 用户端浏览器
  - Kibana 到用户的网络传输



elastic

Kibana

- 身份认证授权
  - LDAP
  - AD
  - SSO
  - …
- 不使用明文密码配置（keystone）
- 数据细粒度权限分离（集群、索引、文档、字段）
  - 同一个报表应做到不同人看到不同数据
- 避免 Dashboard 的泄密
  - 不同人应该只能看到各自的 Dashboard
- Kibana 安全使用培训



elastic

应用侧安全

- 开发人员要具备安全意识、了解安全常识
- 不要使用明文密码，定期更新
- 开发、线上环境配置独立/隔离
- 避免公用账号，按应用权限分离
- 缓存的使用
- 查询预处理、过滤
- 参数范围及数据类型断言



elastic

数据安全

- 认证授权
- 不要存放敏感数据
- 混淆敏感数据
- 定期备份与备份的完整性检查
- 备份归档的加密存储
- 足够的副本冗余 (跨机架感知)
- 异地多活、异地备份
- 安全存放的访问日志



elastic



是不是解决前面提到的这些就安全了呢？

elastic





中国移动 下午1:22 13%

¥599

希捷6T 6000GB V4 3.5寸 SAS接口硬盘 实物拍照，企业级硬盘 正规大型机房下架9成新以上无任何坏道，状态完美，基本待机，2016年出厂，通电时间不到2年，数量不多了，要的抓紧，支持128M缓存平均无故障时间140万小时，sas企业级硬盘是为24小时全天运转设计的，寿命和速度比家用SATA接口硬盘高了不止一个档次，故障率非常低，非常适合个人组建nas服务器和装机使用，请看好是SAS接口7200转，连续读写200M每秒左右，家用电脑也可以用，需要配合SAS卡使用，主板有空余pcie8x或16x插槽就行，一个卡最多可以接8块硬盘，sas卡我也有型号DellH700/512M缓存阵列卡或DellH200直通卡，区别就是阵列卡需要设置才可以认硬盘但支持raid和缓存，一但换卡数据可能需要重建或丢失，直通卡不用设置直接使用，换卡换电脑不影响硬盘数据，两种卡都是120一片都支持希捷6T硬盘，sas1分2硬盘线15一根，sas卡带1分2sas硬盘线135元一套，卡和线你可以自己买，我就是进价出给买硬盘的人图个方便不用二次采购，硬盘健康度100%，请注意是100%哦，等于基本没怎么使用过，无任何坏

超赞 留言 收藏 卖掉了

中国移动 下午1:22 12%

¥599







超赞 留言 收藏 卖掉了



内网安全

- 内网人员
- 专人专号
- 安全策略
- LDAP/AD 域的设置
- 密码策略
- VPN
- 防病毒
- 人为泄露、破坏
- 运维规范
- 安全守则
- 背景调查



elastic

其他一些安全实践

- 服务器网络硬件加固
- 定期更新操作系统（使用可信软件源）
- 使用最新和推荐的 JAVA JDK， 关注是否有安全漏洞及补丁
- 保持更新 Elasticsearch，关注官方的安全披露消息
  - https://www.elastic.co/community/security
- 独立部署、应用隔离
- 修改默认特征配置
  - 9200, 9300, cluster_name etc.
- 权限、相关设置遵循最小化原则
- 对系统做全面的漏洞扫描
- 成立安全小组/SOC、组织培训、定期安全体检
- 分析安全日志、主动监测、建立异常告警规则与应急处理流程



elastic



安全问题千万种，
所有问题全在人！

法海

elastic

Elastic 商业服务

咨询、产品、培训、售后服务

- 提供完整的商业解决方案
- 提供行业应用的最佳实践
- 完善的产品售后支持服务
- 提供全方位产品培训
- 专家上门的顾问咨询服务
- 长期的战略规划与顾问服务
- 7x24小时的及时响应
- 主动预警与应急补丁

https://www.elastic.co/cn/contact



安全

细粒度紧密集成

认证

本地（内置）
第三方(LDAP 以及 AD)
SSO (SAML 以及 Kerberos)
自定义（添加您自己的认证）

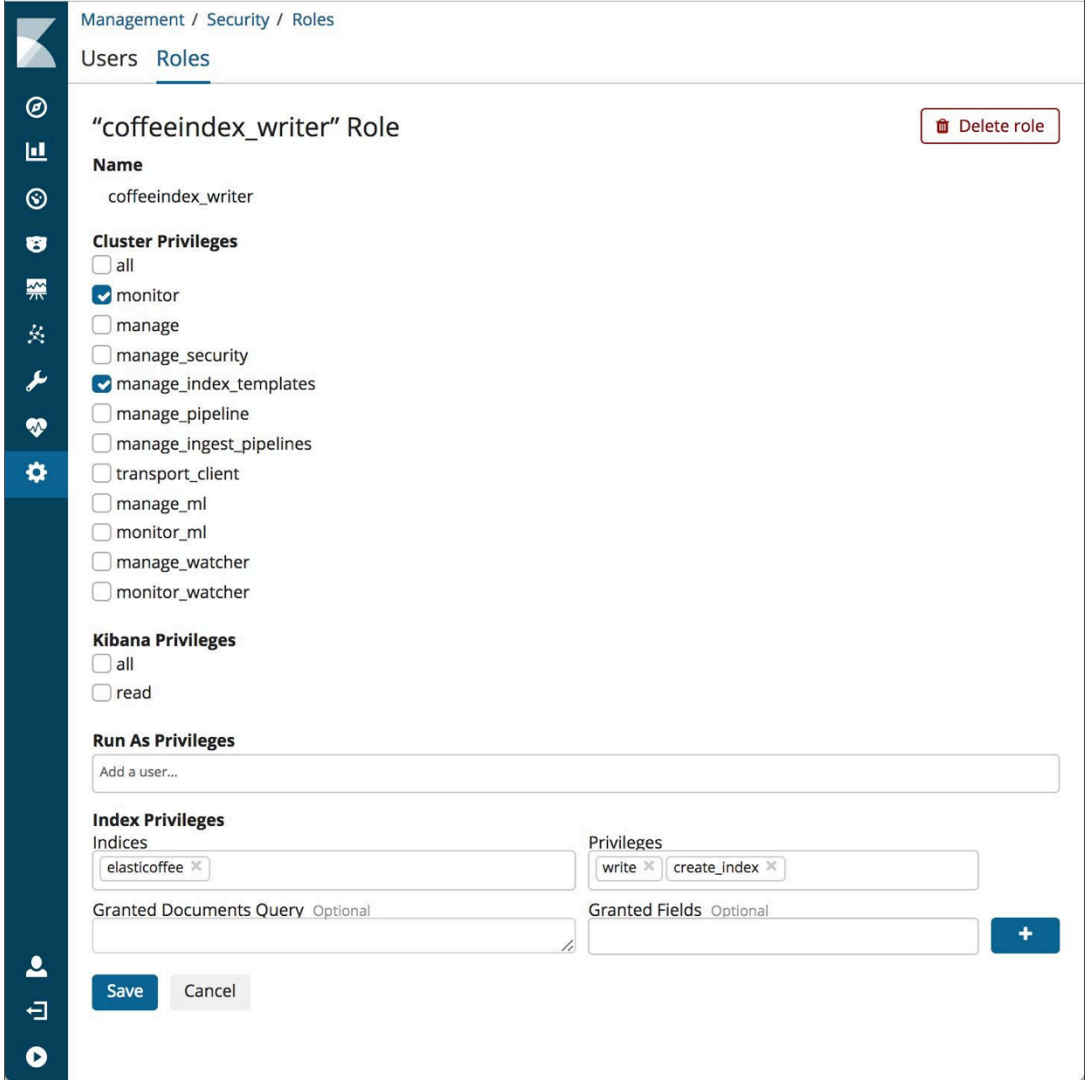
粒度控制

文档和字段级权限
与Kibana Space集成

加密

传输过程中(TLS 以及 SSL)
磁盘加密 (使用 dmcrypt)

还有更多 (审计日志, IP 过滤,...)



安全

细粒度紧密集成

认证

本地（内置）
第三方(LDAP 以及 AD)
SSO (SAML 以及 Kerberos)
自定义（添加您自己的认证）

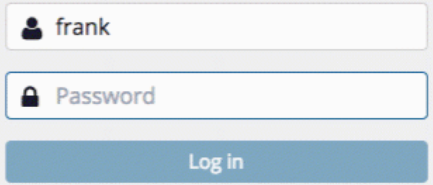
粒度控制

文档和字段级权限
与Kibana Space集成

加密

传输过程中(TLS 以及 SSL)
磁盘加密 (使用 dmcrypt)

还有更多 (审计日志, IP 过滤,...)





风险常在，
未雨绸缪！
亡羊补牢，
为时不晚！
像管人民币一样管好你的数据！

鲁迅

elastic



Questions?



Thank You

- Web : www.elastic.co
- Products : https://www.elastic.co/products
- Forums : https://discuss.elastic.co/
- 中文社区: https://elasticsearch.cn/



elastic
中文社区

专业、垂直、纯粹的 Elastic 开源技术交流社区
https://elasticsearch.cn/