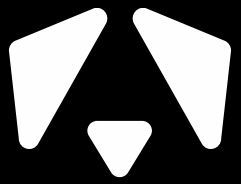
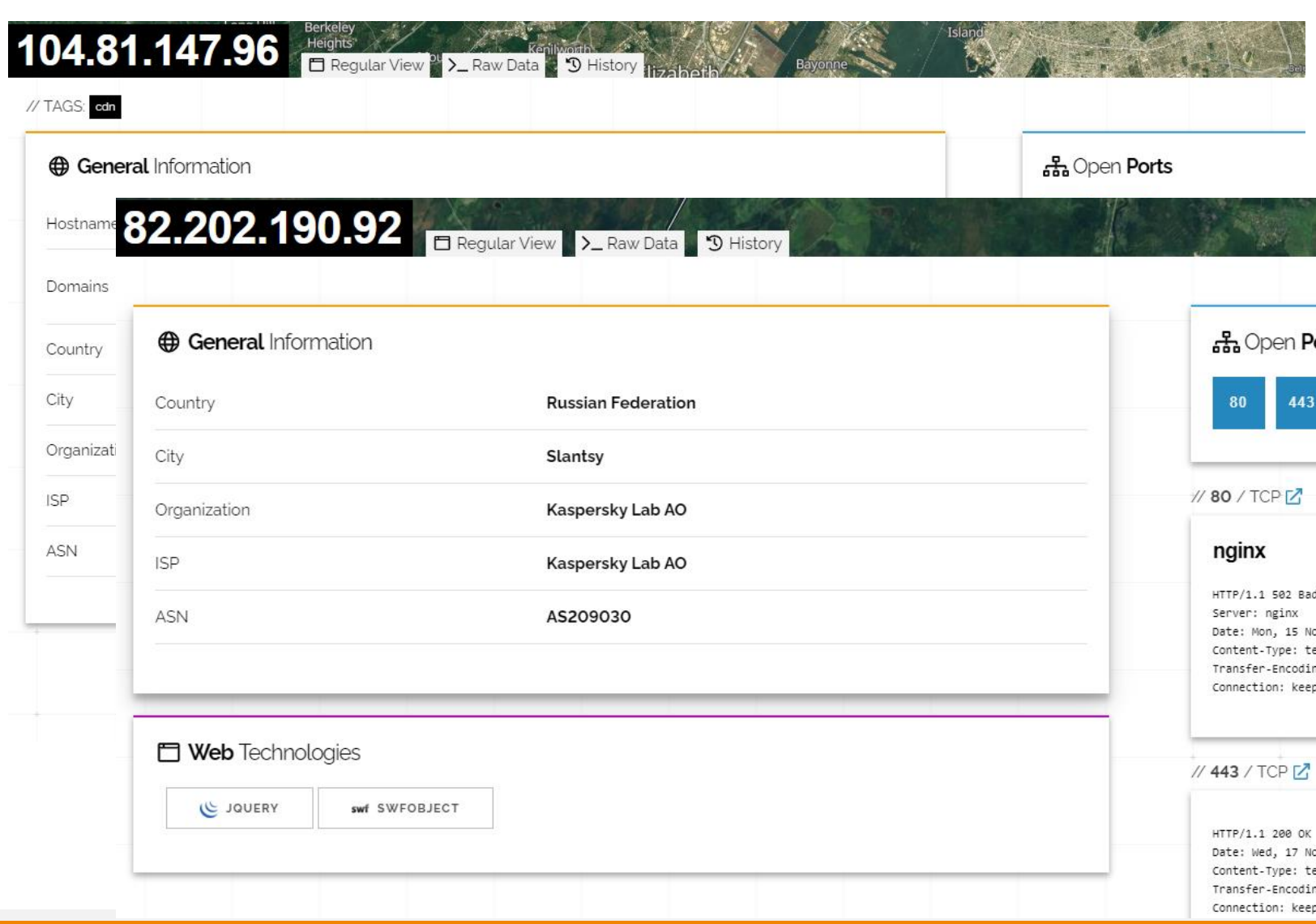


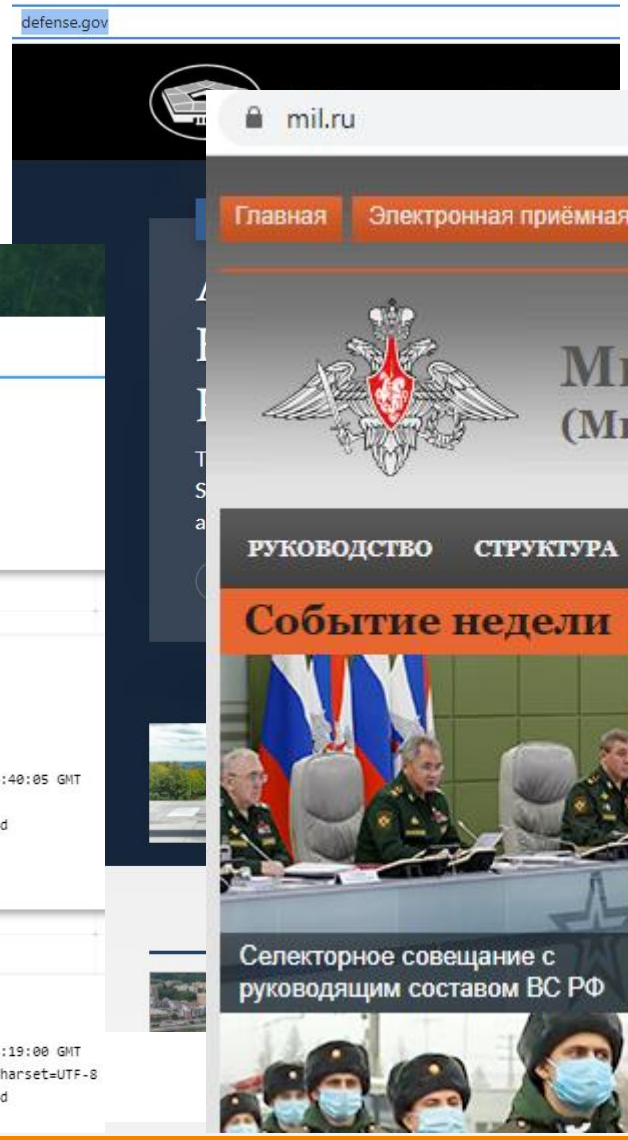
ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Чем мониторинг открытых систем может помочь ИБшнику?

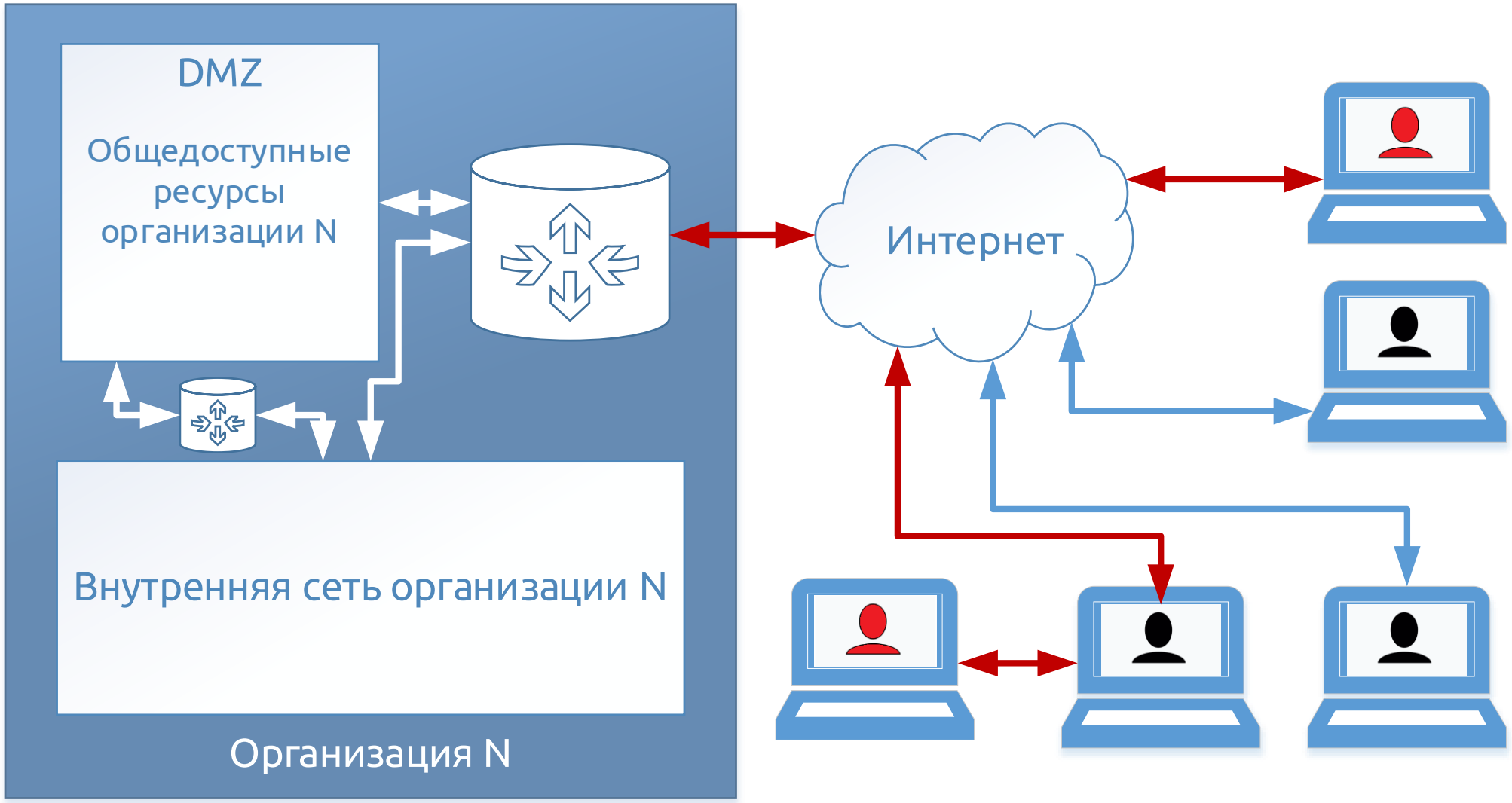
Денис Строченко, руководитель направления

О каких системах речь?

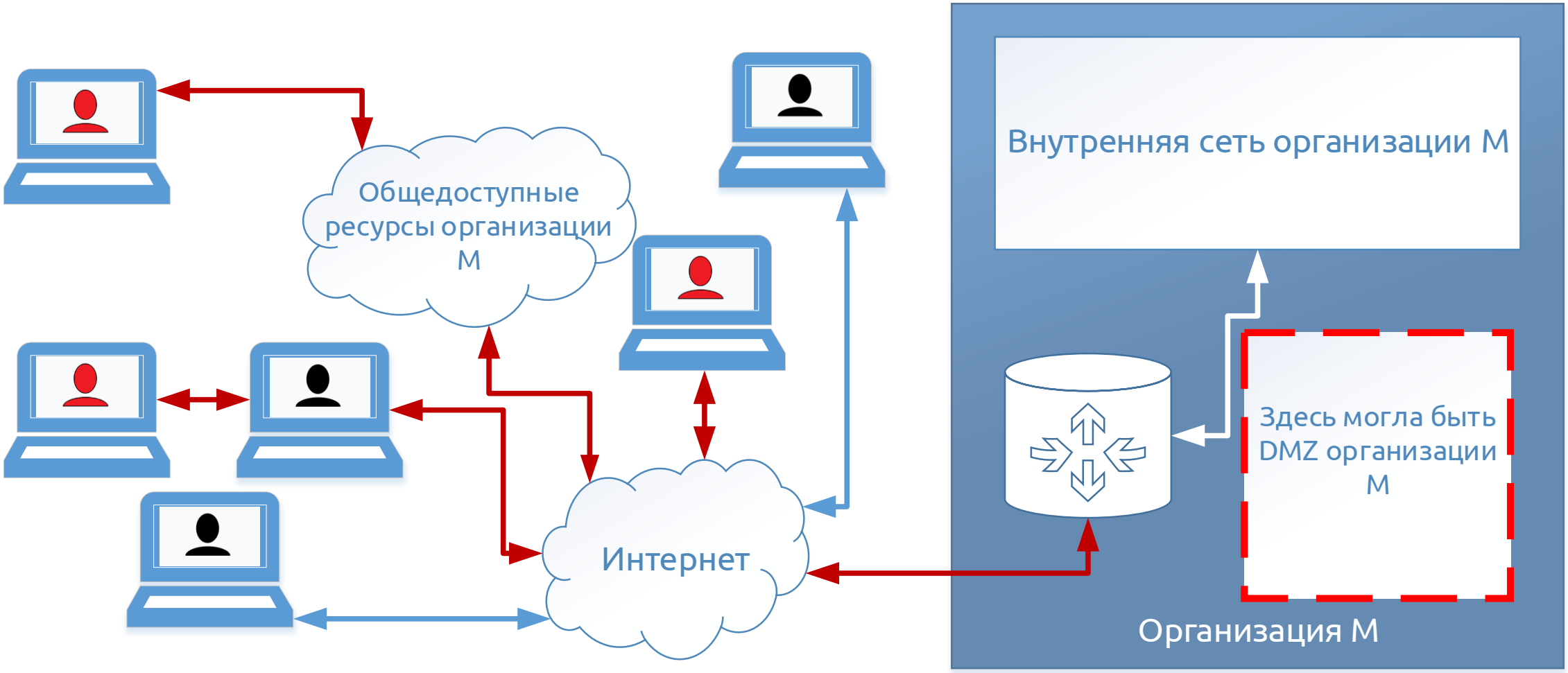




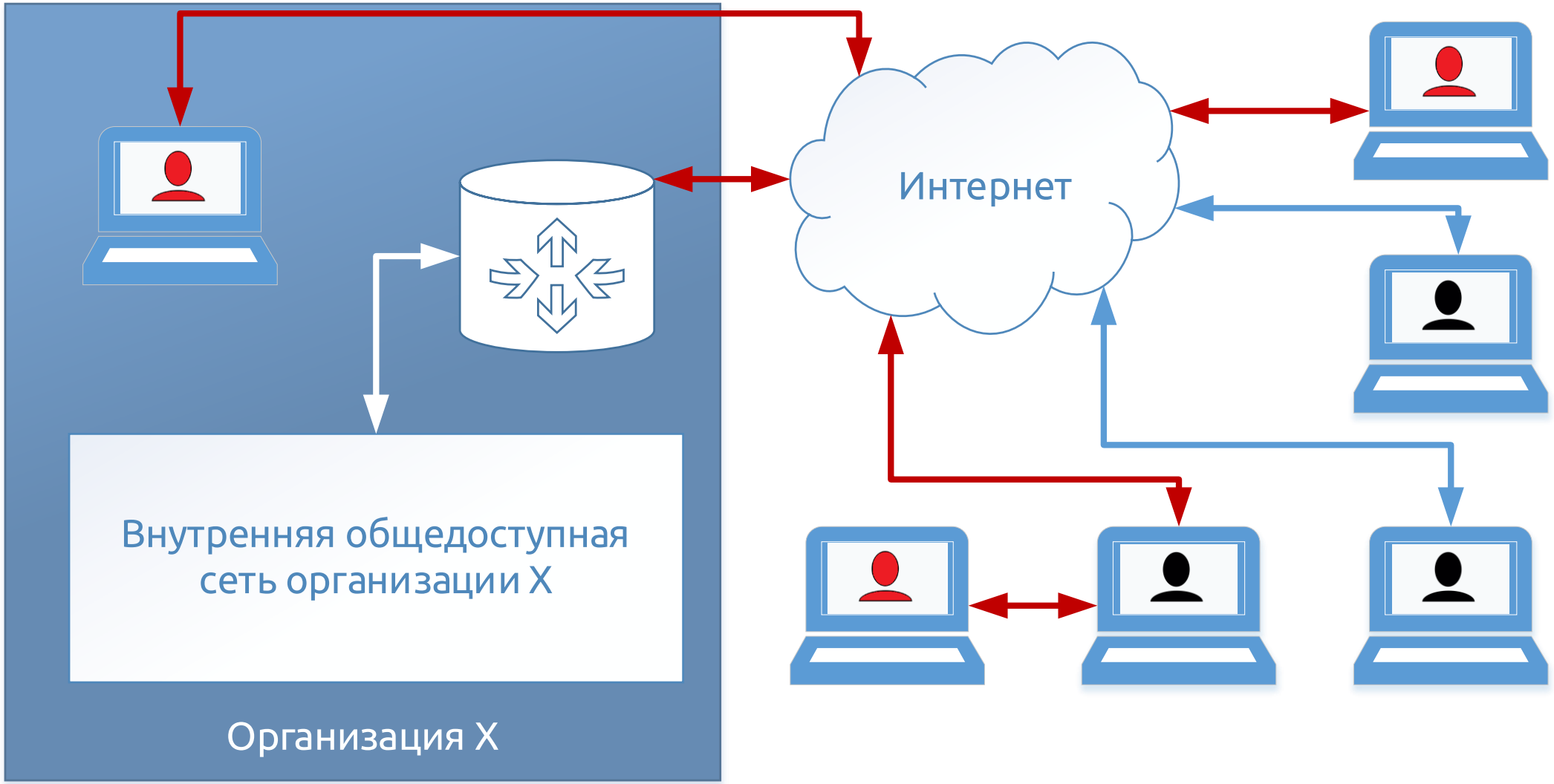
Как эти системы могут строиться?



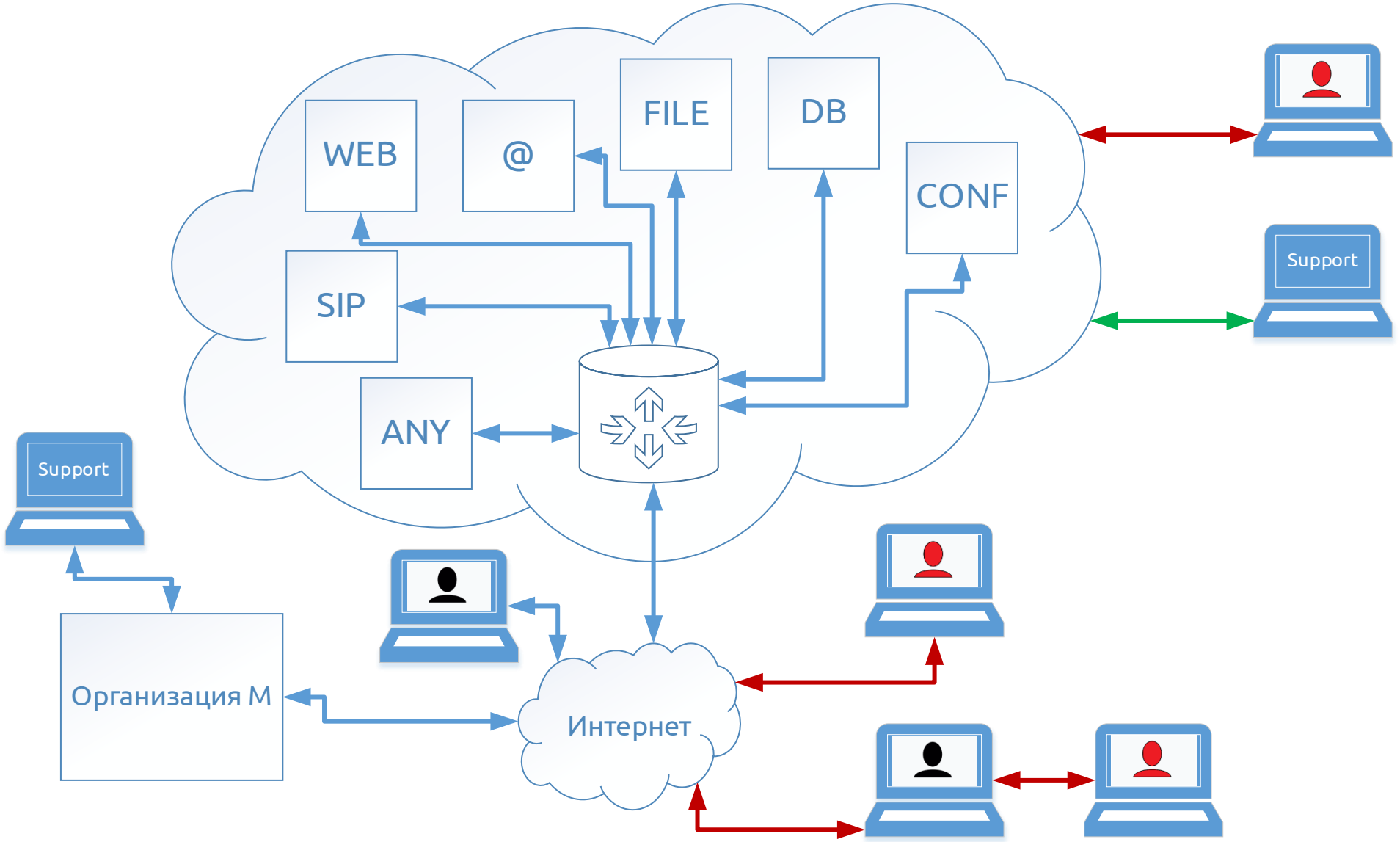
Как эти системы могут строиться?



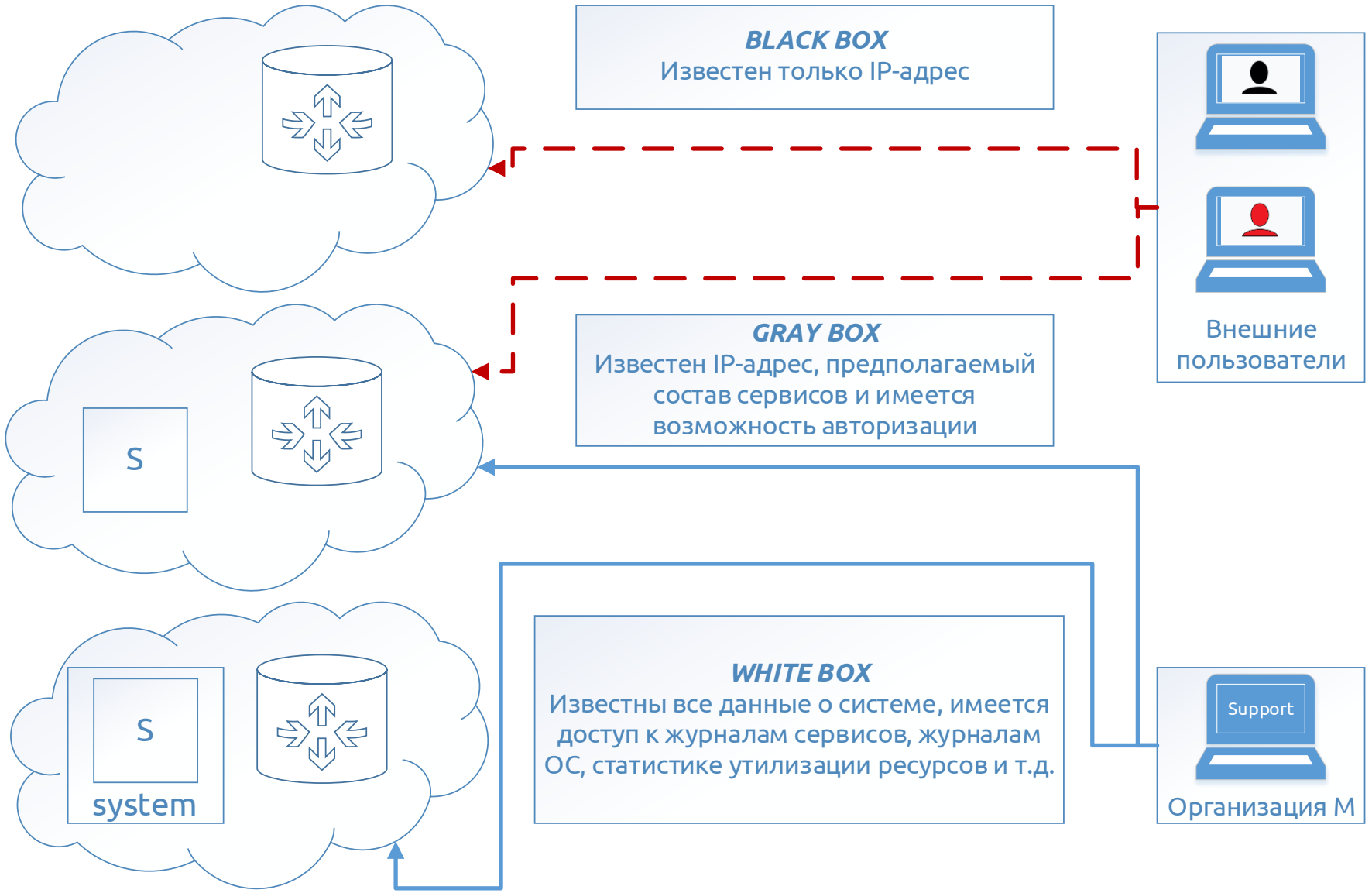
Как эти системы могут строиться?



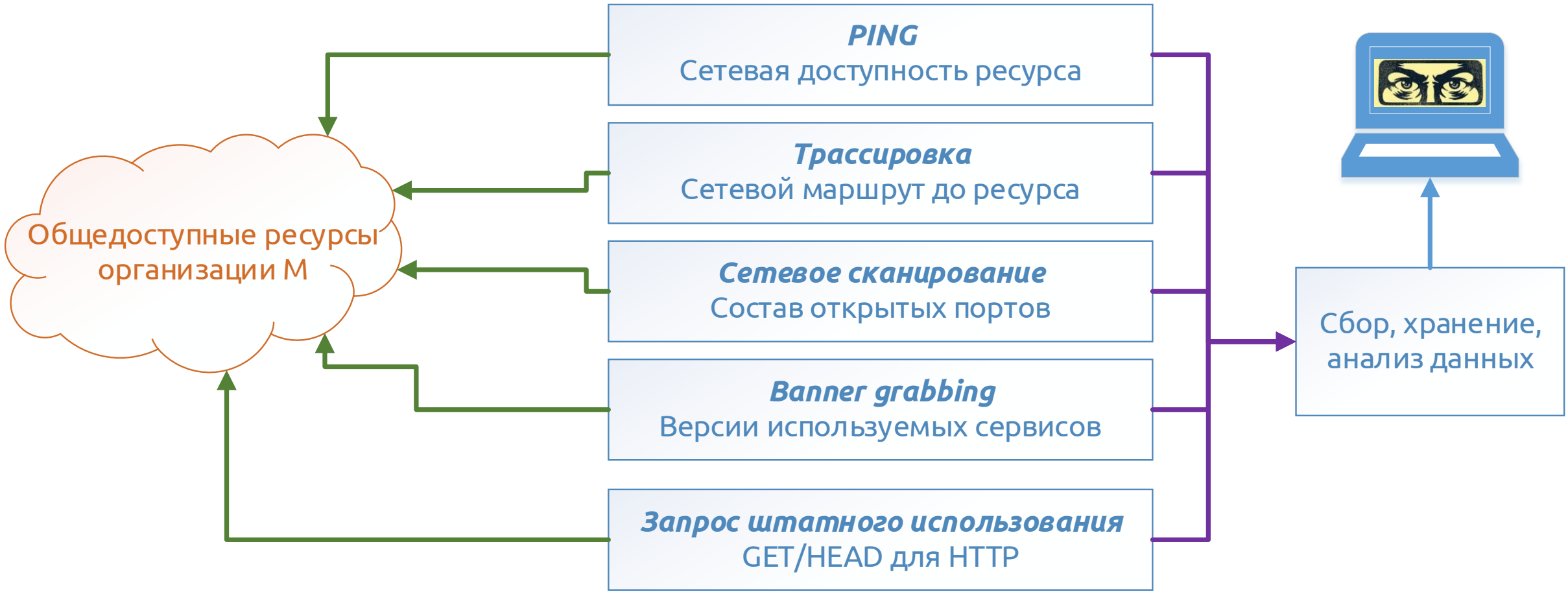
Как эти системы могут строиться?



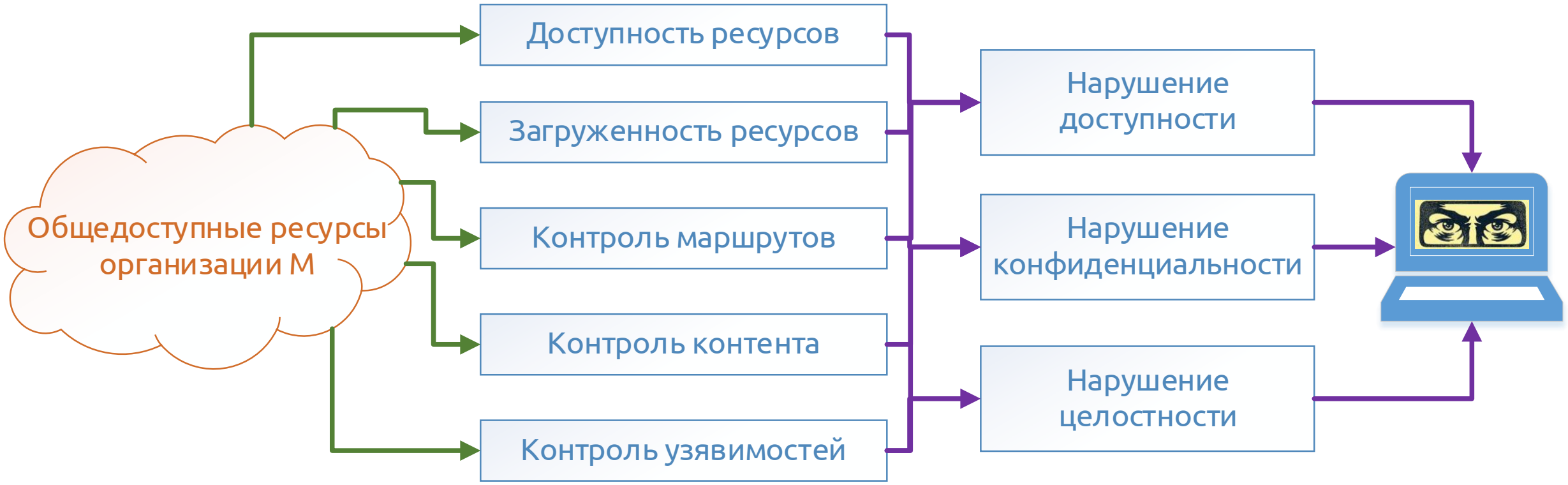
Как защищать такие системы?



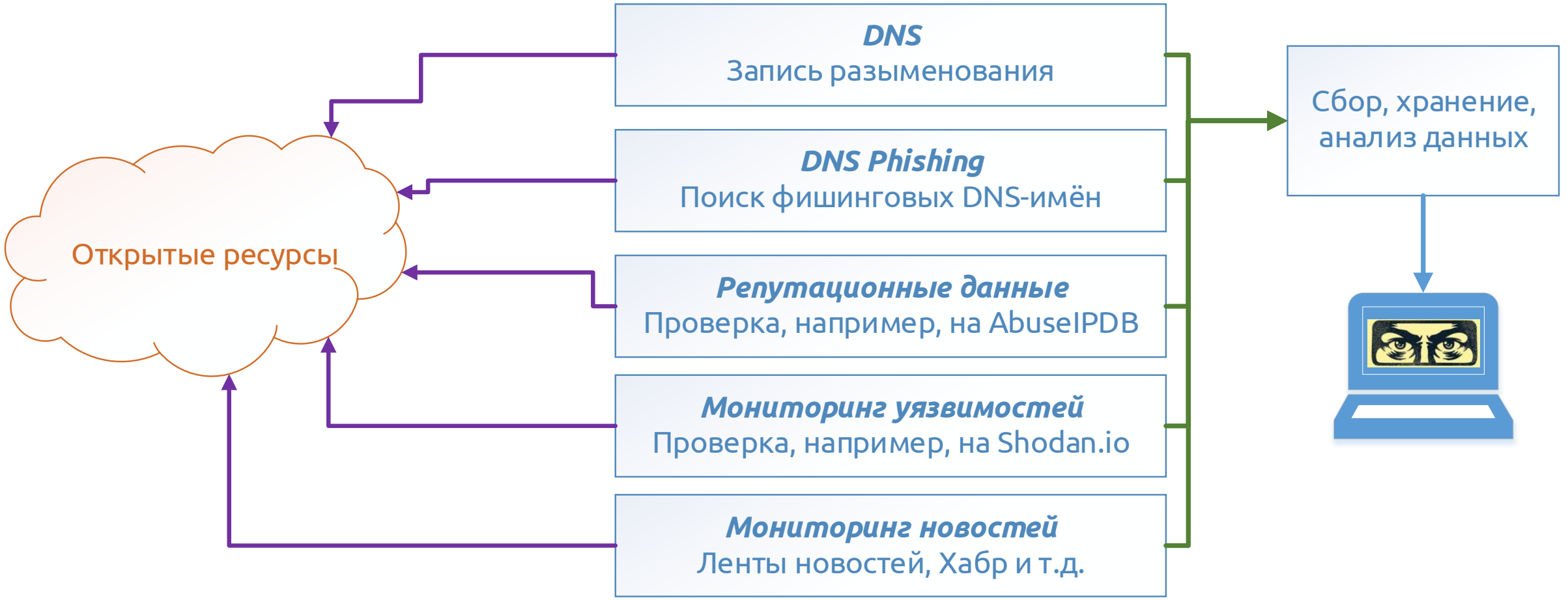
Black box (инструменты)



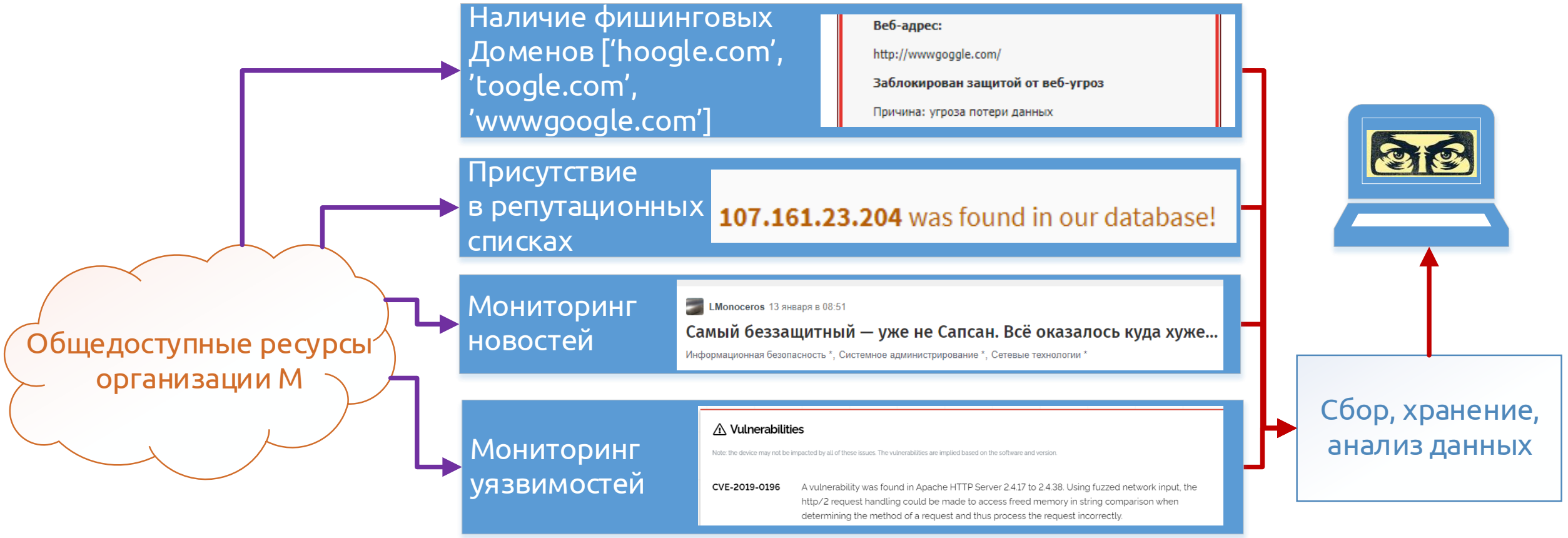
Black box (контролируемые сущности)



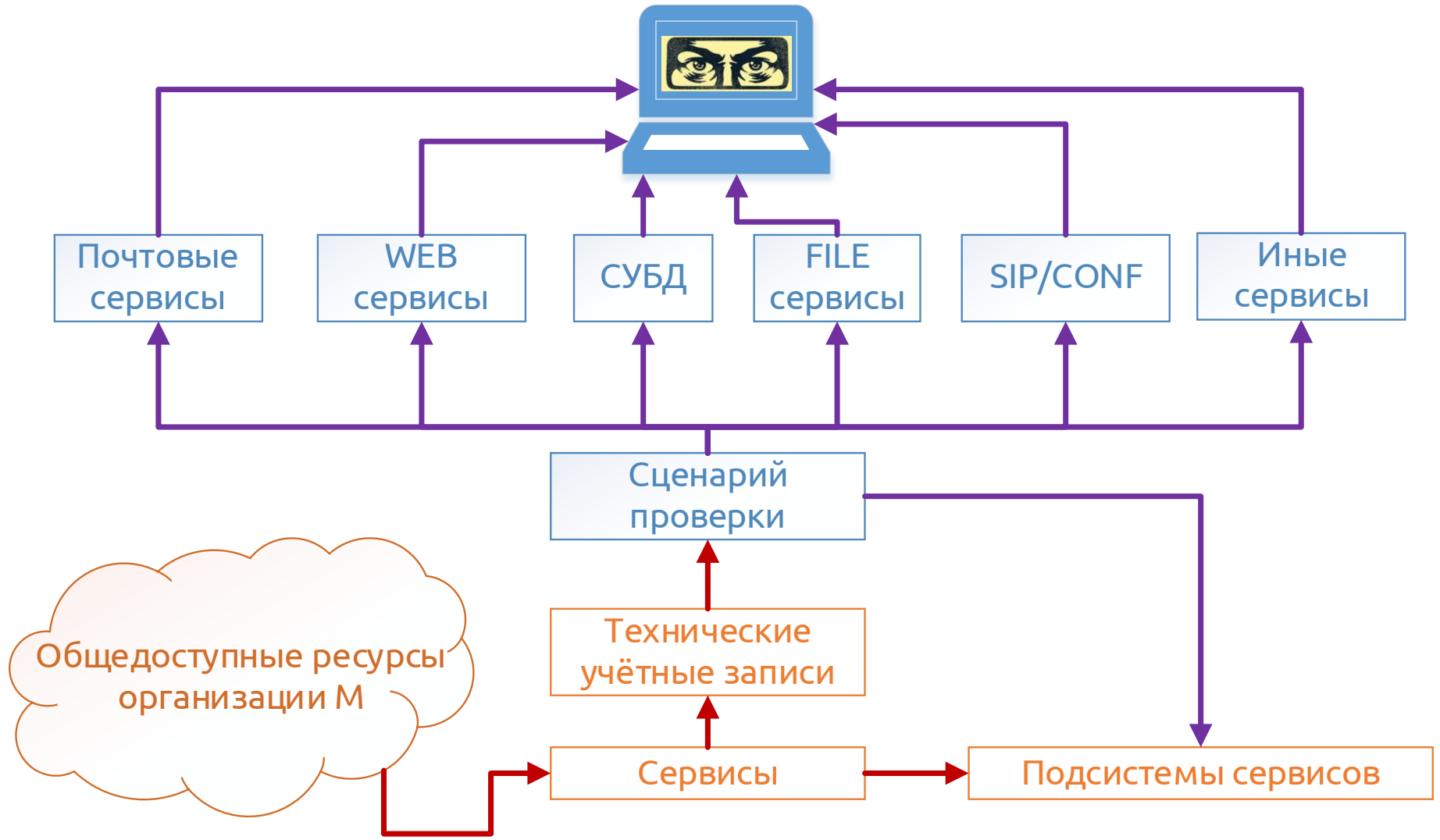
Black box (инструменты)



Black box (OSINT)

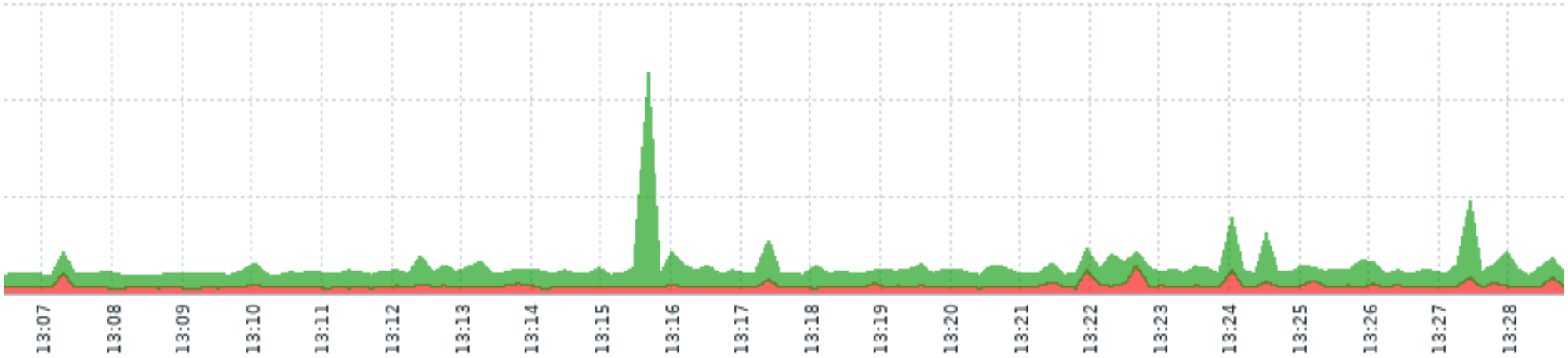


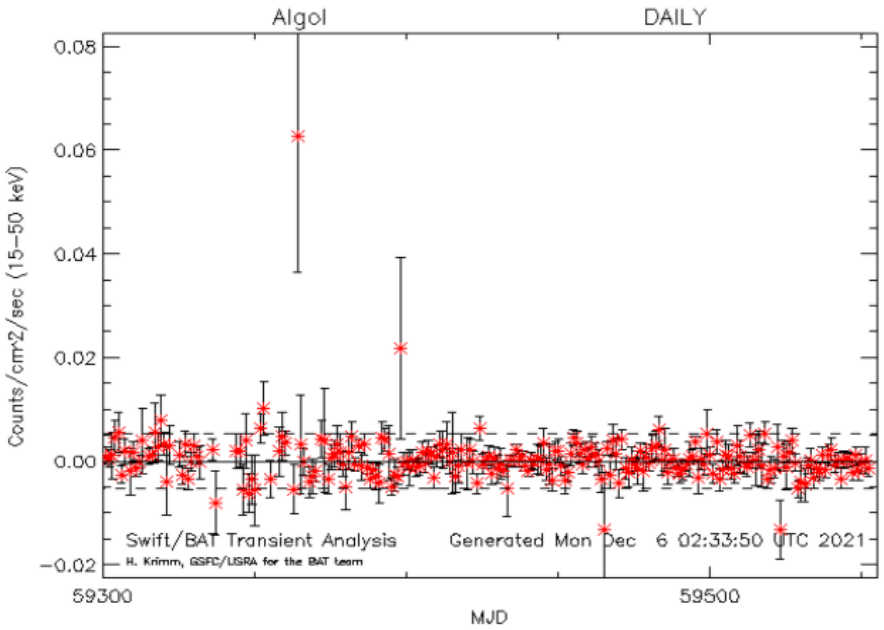
Gray box (сценарии)

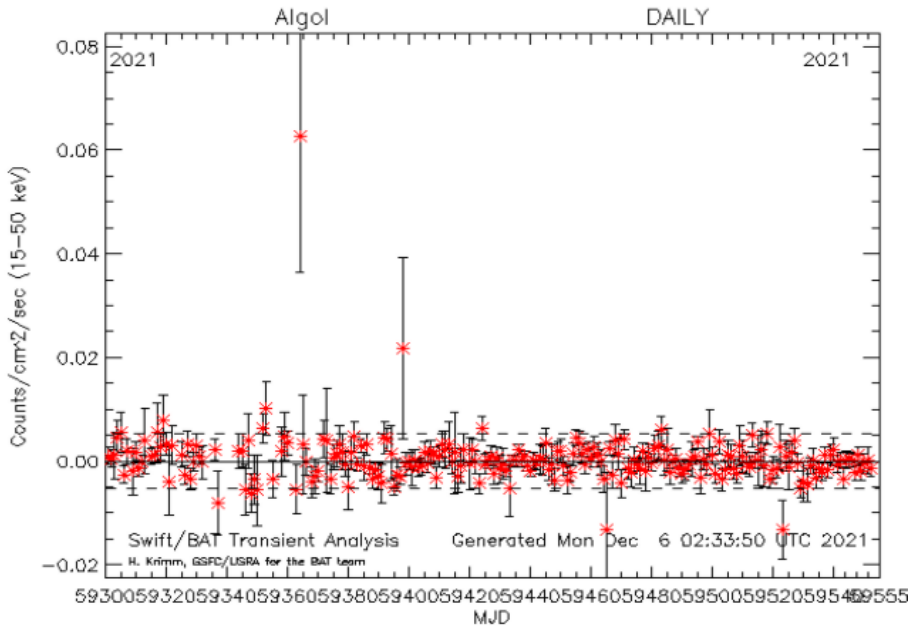


Gray box (параметры)

Gray box (пример)



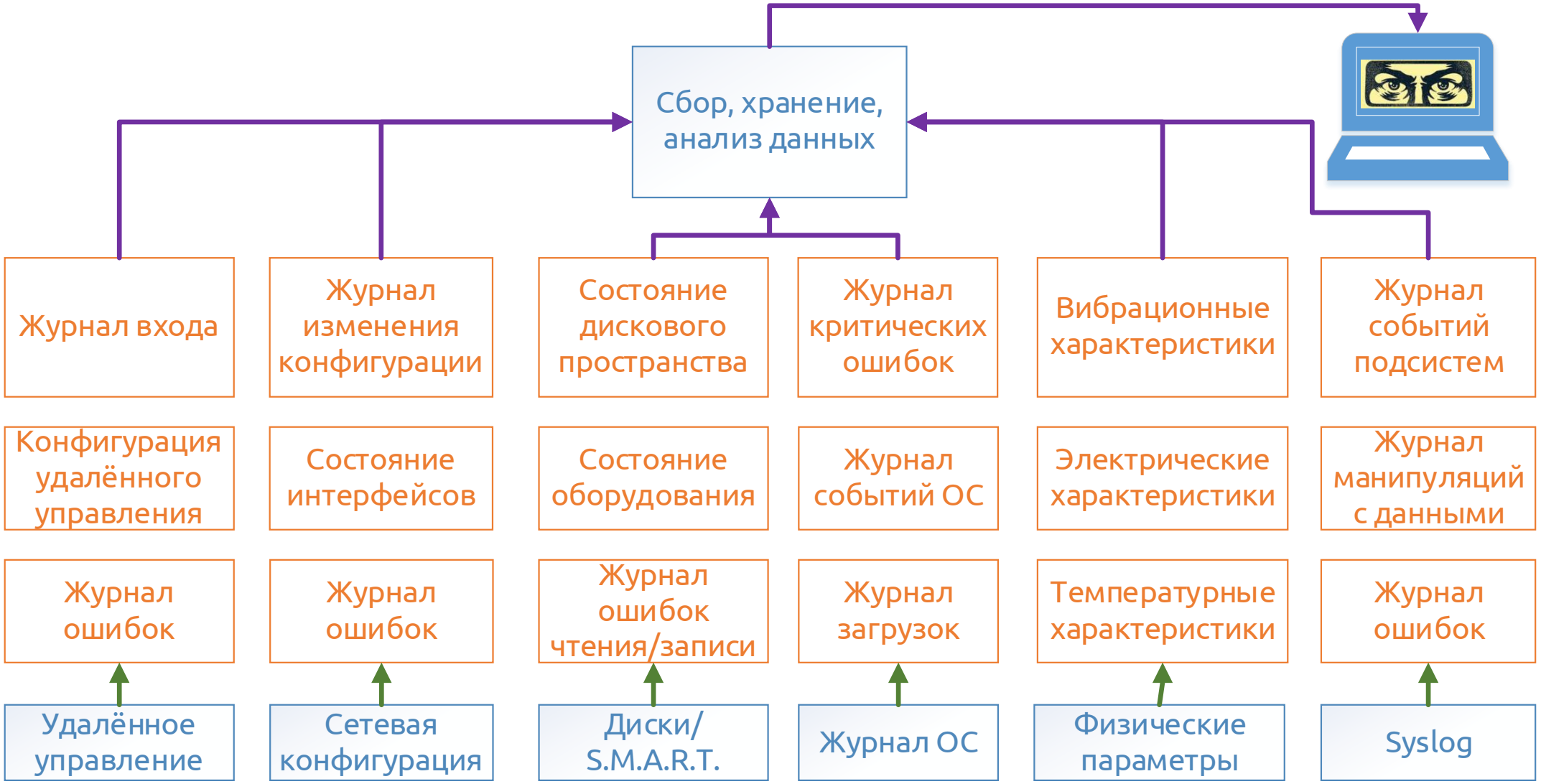




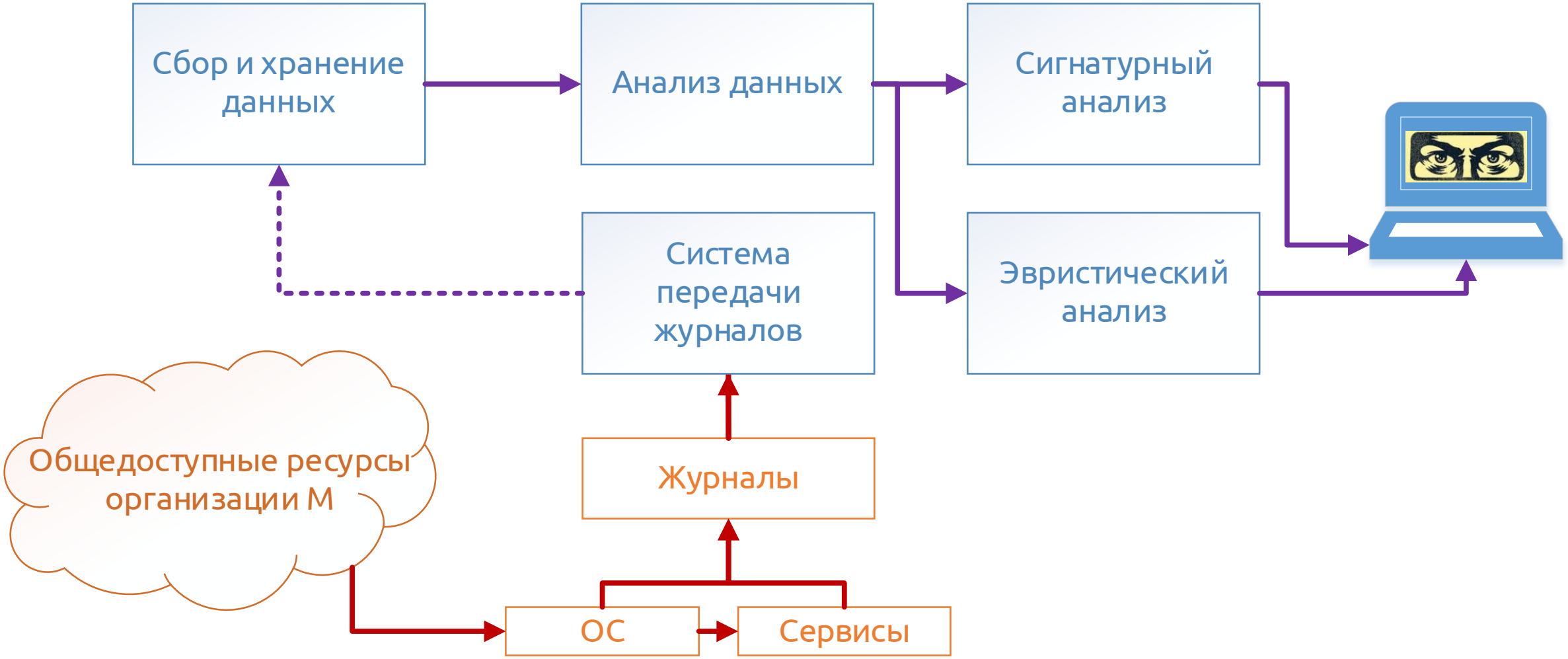
White box (логика)

White box (журналы сервисов)

White box (журналы ОС)

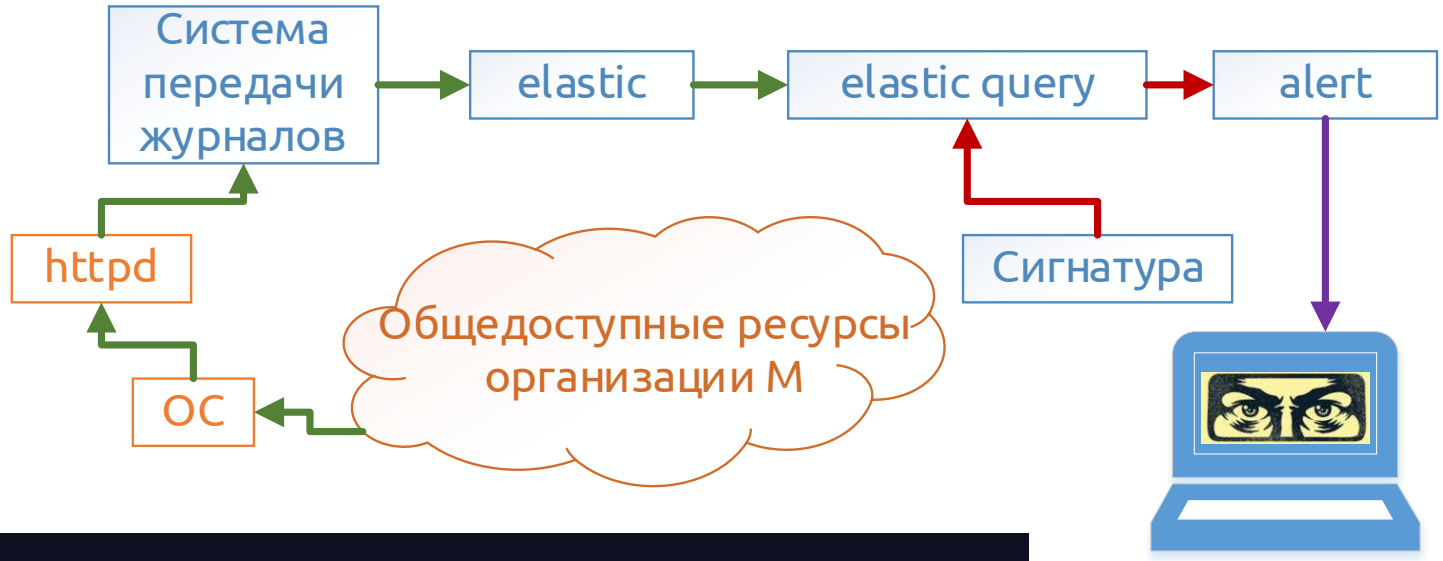


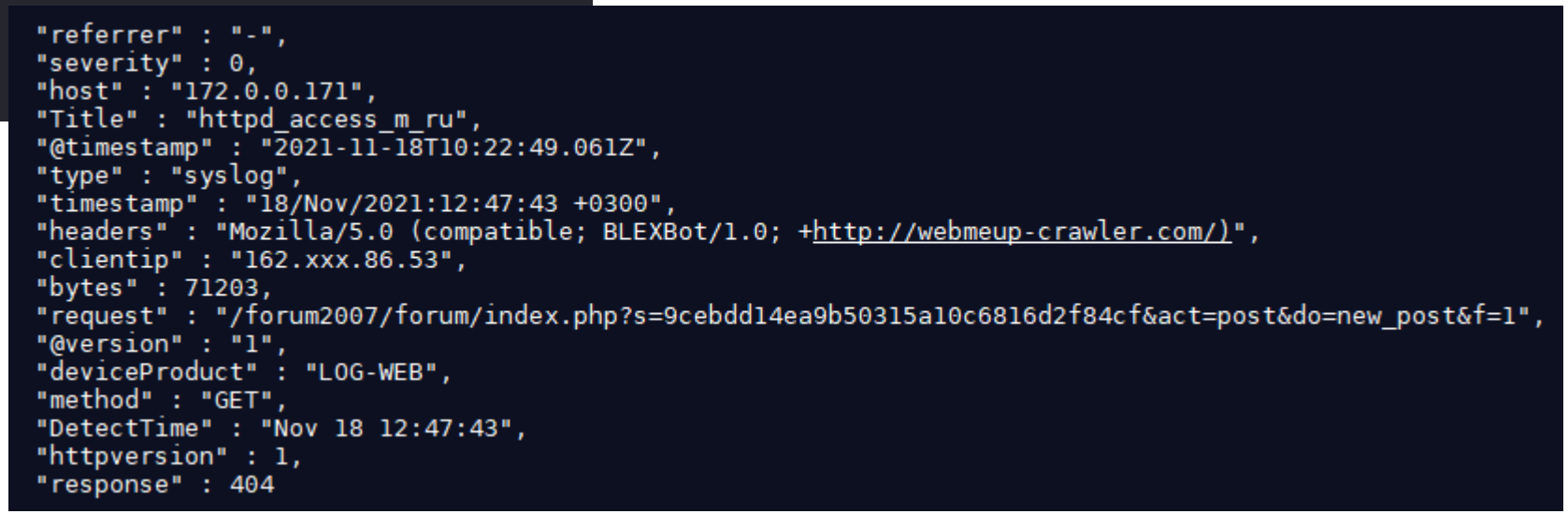
White box (логика)



White box (сигнатурный анализ)

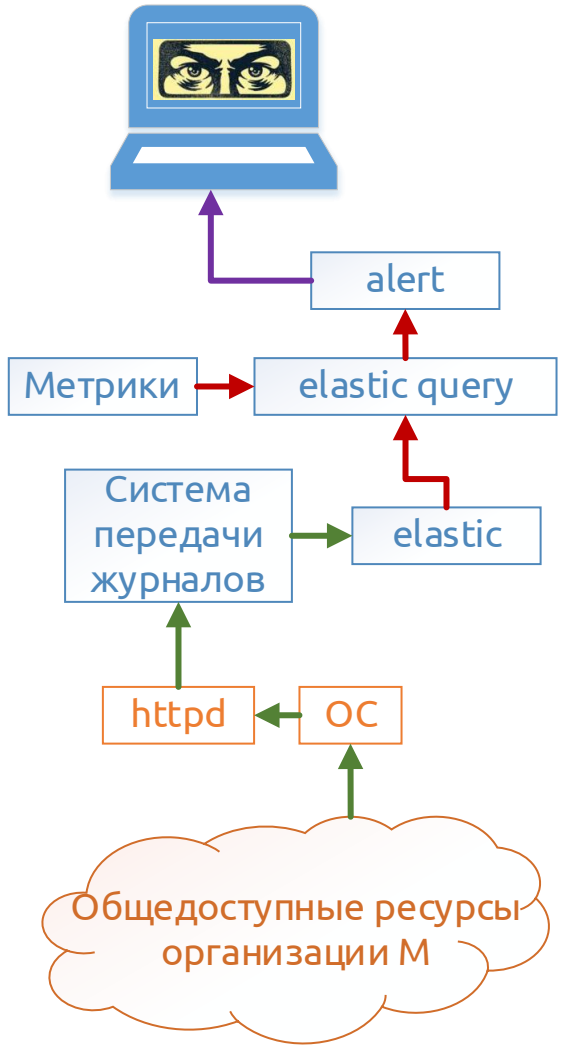
```
GET /log-weblog-11.2021/_search
{
  "size":10000,
 "query": {"bool": {
    "must": [
    {"query_string": {"query": "GET",  "default_field": "method"}},
    {"query_string": {"query": "act=", "default_field": "request"}},
    {"query_string": {"query": 404,    "default_field": "response"}}
  ],
    "must_not": []}},
  "sort":
  [
    {
      "@timestamp":"asc"
    }
  ]
}
```

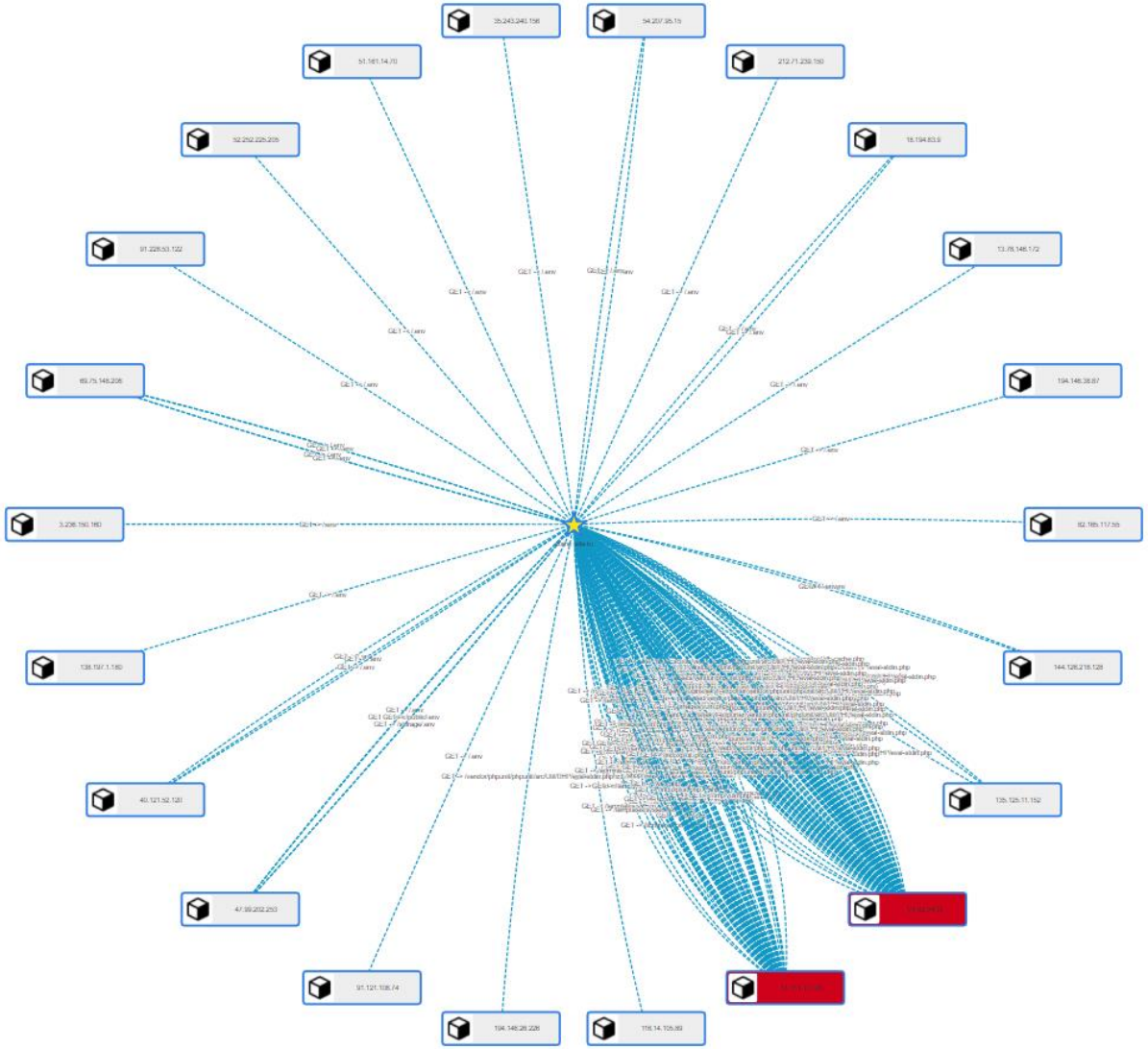




```
"referrer" : "-",
"severity" : 0,
"host" : "172.0.0.171",
"Title" : "httpd_access_m_ru",
"@timestamp" : "2021-11-18T10:22:49.061Z",
"type" : "syslog",
"timestamp" : "18/Nov/2021:12:47:43 +0300",
"headers" : "Mozilla/5.0 (compatible; BLEXBot/1.0; +http://webmeup-crawler.com/)",
"clientip" : "162.xxx.86.53",
"bytes" : 71203,
"request" : "/forum2007/forum/index.php?s=9cebdd14ea9b50315a10c6816d2f84cf&act=post&do=new_post&f=1",
"@version" : "1",
"deviceProduct" : "LOG-WEB",
"method" : "GET",
"DetectTime" : "Nov 18 12:47:43",
"httpversion" : 1,
"response" : 404
```

White box (эвристический анализ)





Итоги

Имеется возможность обеспечивать безопасность открытых систем без использования каких-либо средств защиты и изменения конфигурации сервисов

При минимальном изменении конфигурации сервисов возможна расширенная проверка согласно сценариям

При обеспечении непрерывной передачи журналов сервисов имеется возможность обеспечить безопасность открытых сервисов на высоком уровне

АО «ПМ» уже внедрило в процесс работы SOC данные механизмы мониторинга

Спасибо!

Денис Строченко

Denis.Strochenko@amonitoring.ru