



31/05/2018

ПРАКТИКА ЛОВЛИ ХАКЕРОВ НА БЛЕСНУ: ОПЫТ ПРИМЕНЕНИЯ DECEPTION-TOOLS

**Анна
Богданова**

Руководитель направления SOC ЦИБ АО «Инфосистемы Джет»
av.bogdanova@jet.msk.su / +7 916 784-70-95

ПРОБЛЕМАТИКА



Периметровые средства не дают 100%-защиты от современных атак



С помощью SIEM-систем сложно задетектировать APT-атаки



Зачастую горизонтальный трафик в сети никак не контролируется

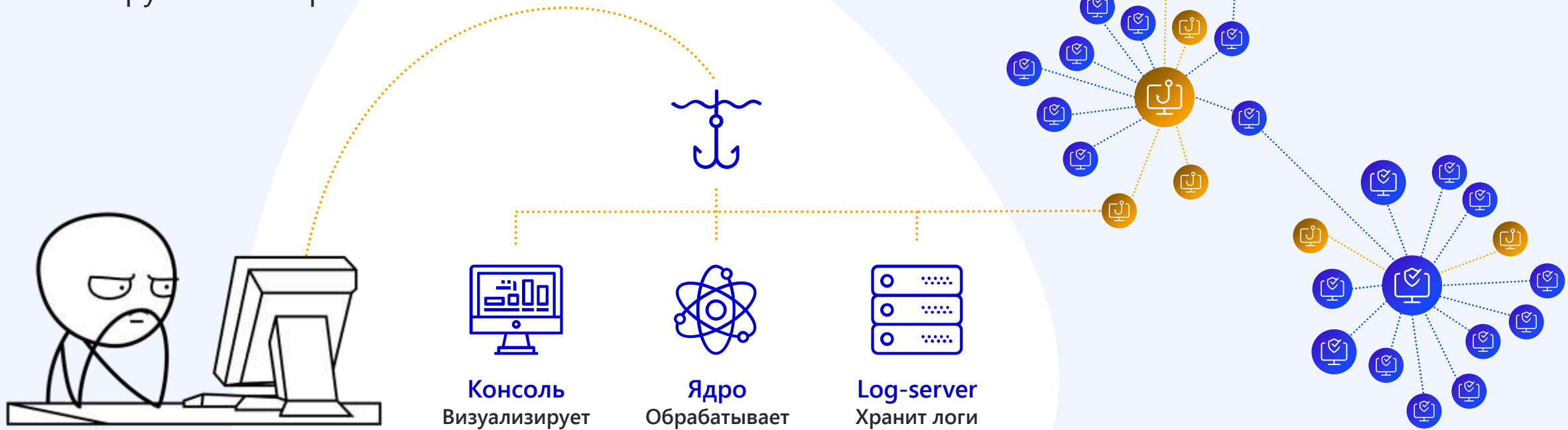


Shadow IT,
Bring Your Own Device

DECEPTION-РЕШЕНИЯ



- Потомки классических honey pot'ов
- Своего рода «сигнальные сети», состоящие из поддельных «условно уязвимых» узлов
- Распределенные системы обнаружения вторжений



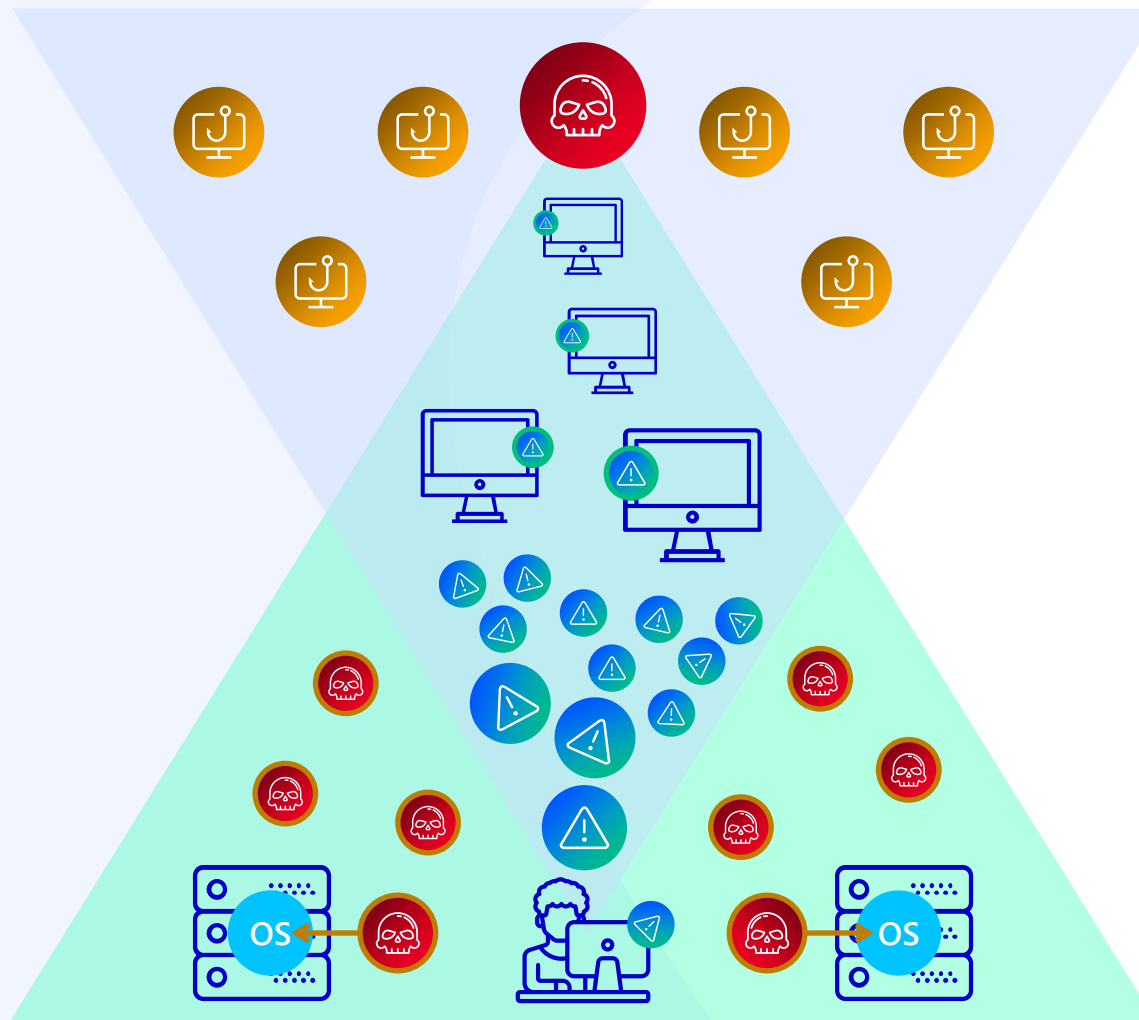
TRAPX DECEPTION GRID



Токены (приманки)

Сетевые сенсоры (ловушки)

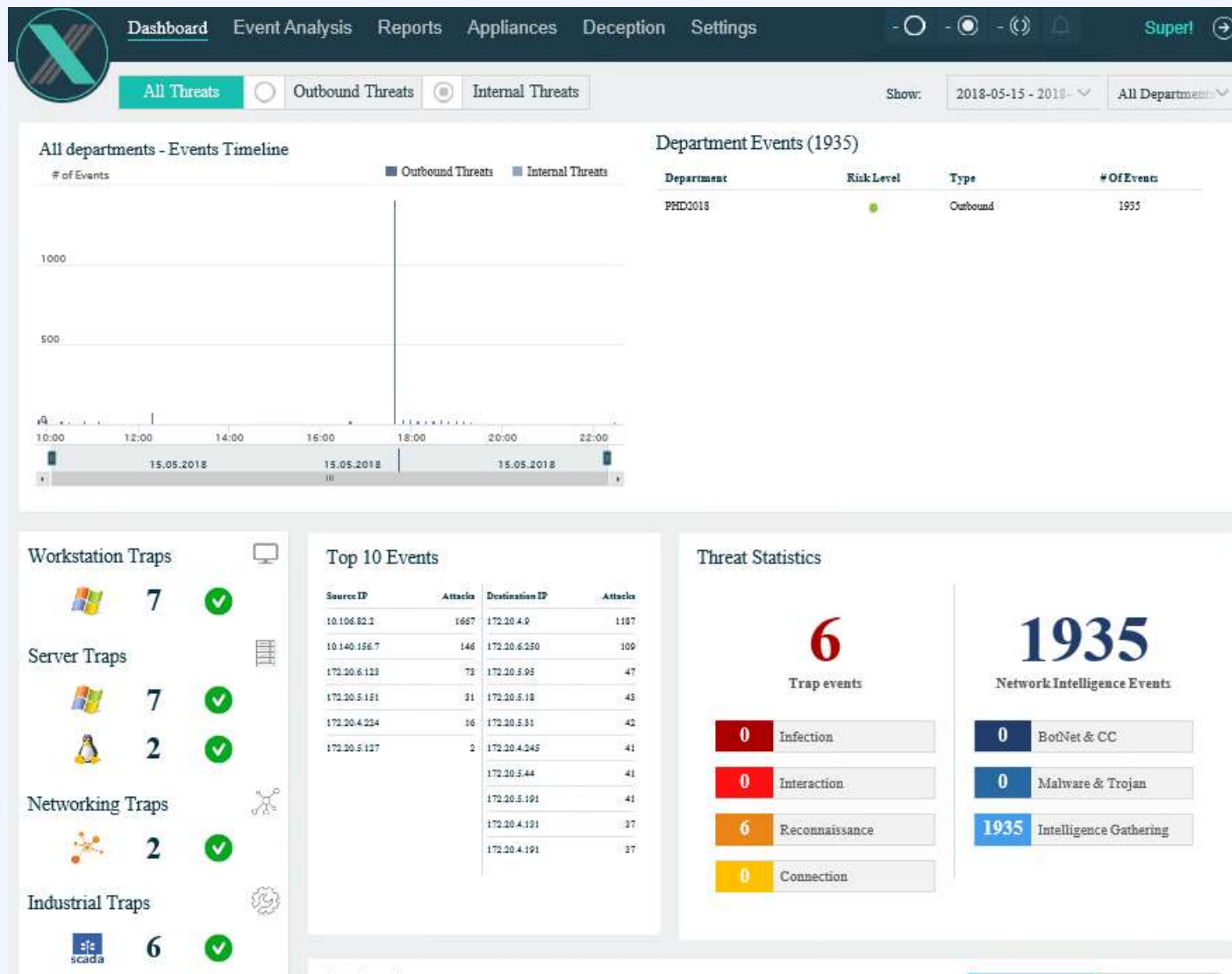
Full OS Clones



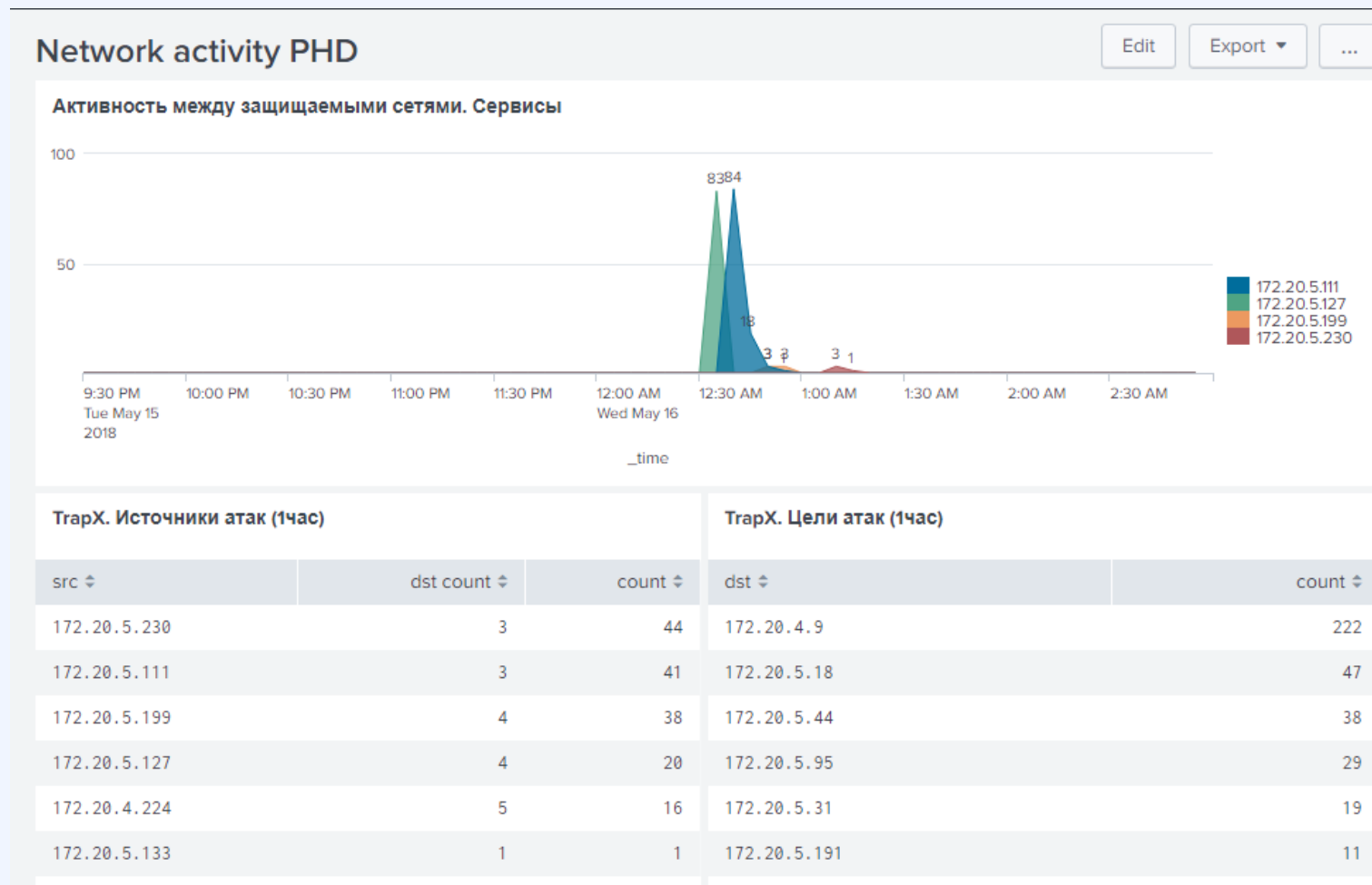
ТРАПХ ДЛЯ ЗАЩИТЫ SCADA НА PHDAYS



ТРАПХ ДЛЯ ЗАЩИТЫ SCADA НА PHDAYS



TRAPX ДЛЯ ЗАЩИТЫ SCADA НА PHDAYS



ТРАПХ ДЛЯ ЗАЩИТЫ SCADA НА PHDAYS



111 Infection 172.20.5.230 172.20.5.230 805_95_win SMB 445 16.05.2018 01:11:08 00:12 min

Attack Highlights

Host name: 172.20.5.230
IP Address: 172.20.5.230
Port: 41467
Login: Domain: Username: (SMB1)
Start Timestamp: 16/05/2018 01:11:08
End Timestamp: 16/05/2018 01:11:20

SMB 445
Name: 805_95_win
IP address: 172.20.5.95
Emulation type: Windows Server
OS: Microsoft Windows Server 2003

- Establish Connection 1
- Logon 1
- Tree Connect 1
- Exploit 1
- Disconnected 1

Attack Details

Contains text 5/5 Events

01:11:08	Establish Connection: from port 41467
01:11:09	Logon: Domain: Username: (SMB1)
01:11:09	Tree Connect: \\172.20.5.95\IPC\$
01:11:09	Exploit: Exploit: EternalBlue exploit detected
01:11:20	Disconnected

20180516-011108_SMB_117.pcap

No.	Time	Source	Destination	Prot
1	0.000000	172.20.5.230	172.20.5.95	SMB
2	0.000288	172.20.5.95	172.20.5.230	SMB
3	0.034963	172.20.5.230	172.20.5.95	SMB
4	0.035079	172.20.5.95	172.20.5.230	SMB
5	0.152001	172.20.5.230	172.20.5.95	SMB
6	0.152375	172.20.5.95	172.20.5.230	SMB

TRAPX ДЛЯ ЗАЩИТЫ SCADA НА PHDAYS



ID	Svr	Type	Attacker hostname	Attacker IP	Trap name	Protocol	Port	Proxy	Start	Duration
118		Interaction	10.140.156.14	10.140.156.14	809_191_win	SSH	22		24.05.2018 11:19:23	03:00 min

Attack Highlights

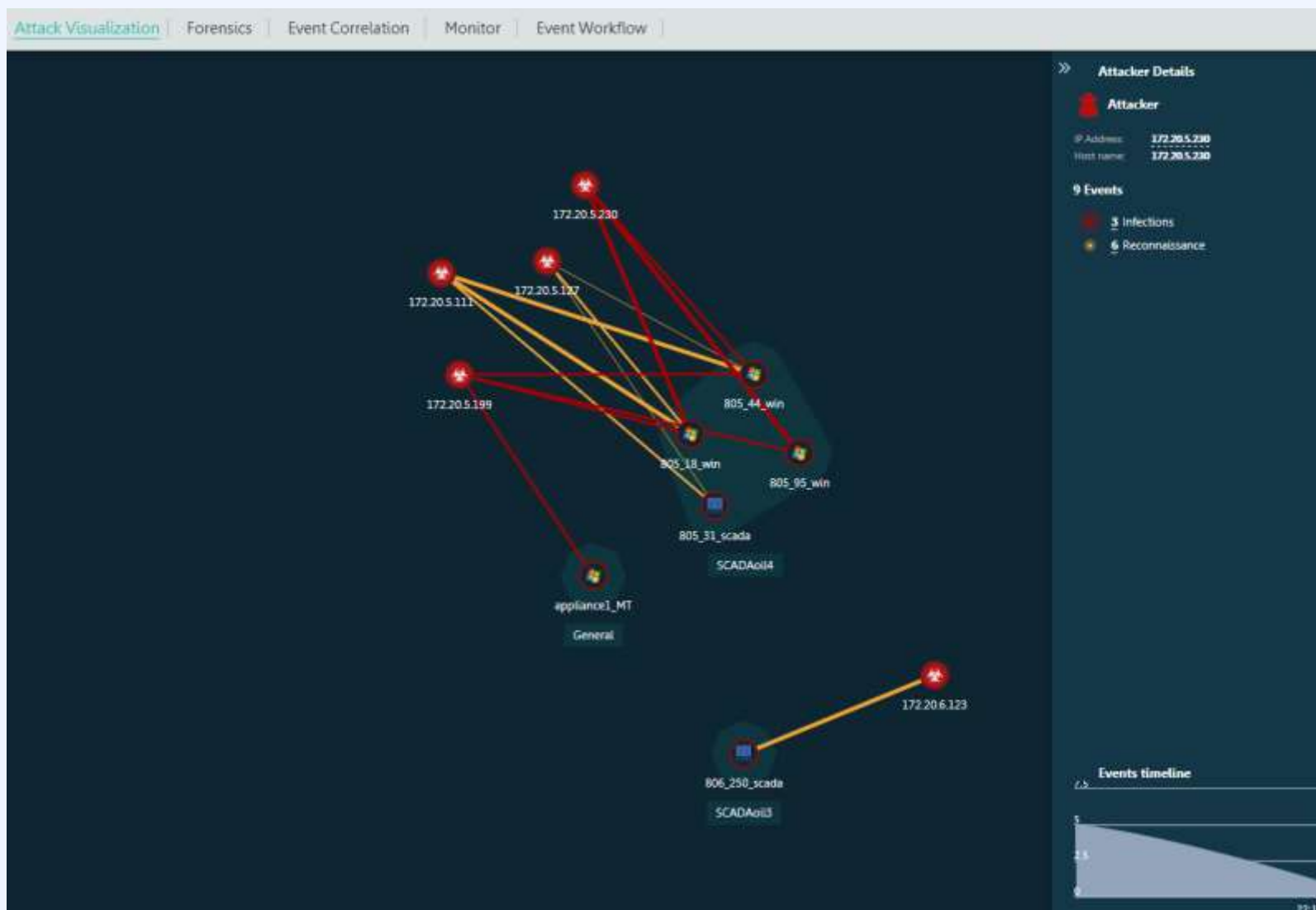
Host name: 10.140.156.14	SSH 22 Name: 809_191_win IP address: 10.140.156.191 Emulation type: Linux Server OS: Linux 3.7	Establish Connection: 1
IP Address: 10.140.156.14		Authentication Result: 1
Port: 46726		Shell: 1
Login: N/A		Command: 6
Start Timestamp: 24/05/2018 11:19:23		Disconnected: 1
End Timestamp: 24/05/2018 11:22:23		

Attack Details

Contains text 10/10 Events

11:19:23	Establish Connection: from port 46726
11:19:32	Authentication Result: true User: root Password: qwerty Login Attempts: 1
11:19:32	Shell: Opening shell Username: root
11:19:38	Command: uname -a
11:19:42	Command: cd /etc
11:19:44	Command: ls -l
11:19:48	Command: cat yum
11:19:52	Command: cat yum.conf

ТРАПХ ДЛЯ ЗАЩИТЫ SCADA НА PHDAYS



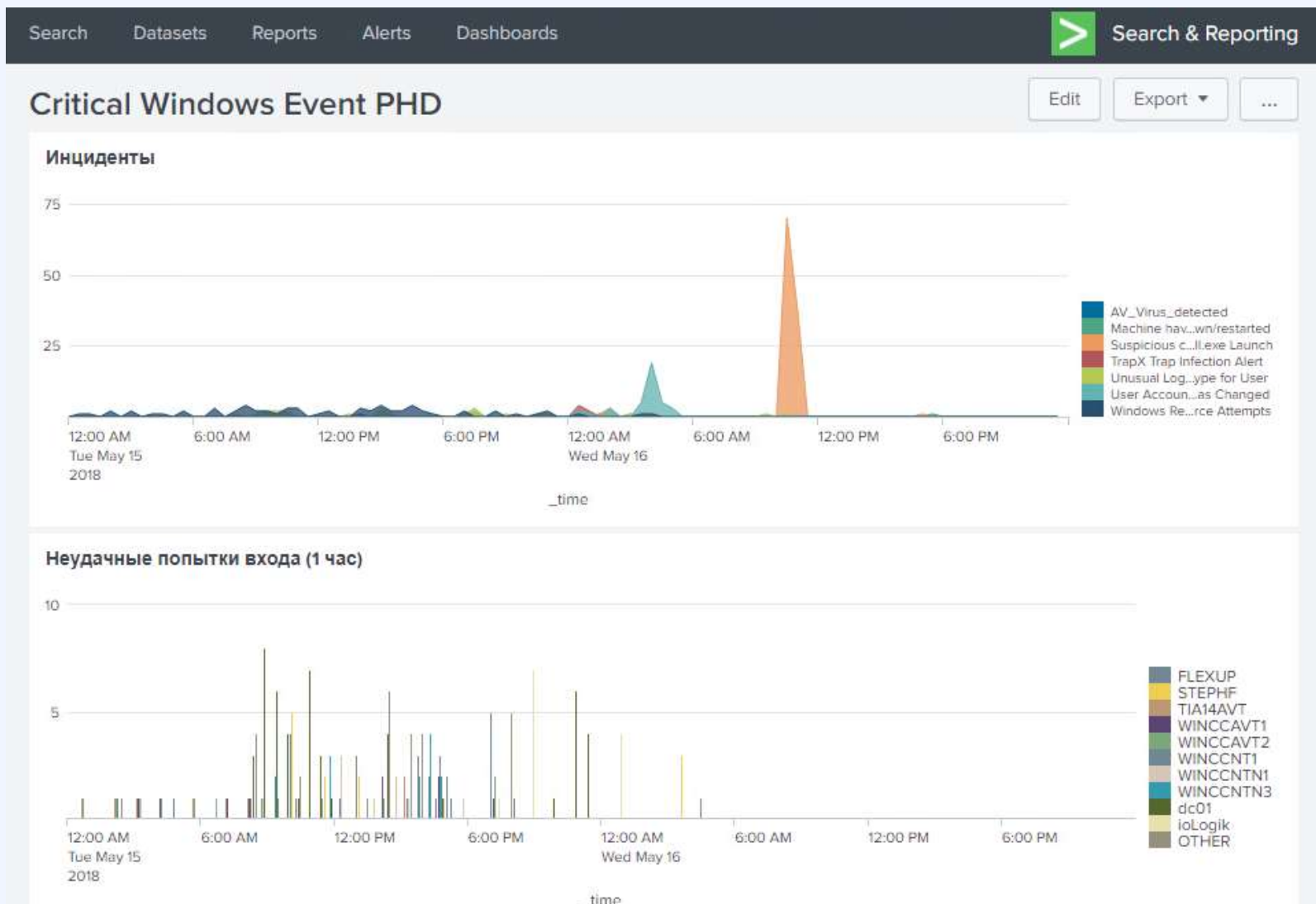
TRAPX ДЛЯ ЗАЩИТЫ SCADA НА PHDAYS



The screenshot shows the JetSec web interface. The top navigation bar includes 'Dashboard', 'Event Analysis', 'Reports', 'Appliances', 'Deception', and 'Settings'. Below this is a secondary navigation bar with 'Event Analyzer', 'Attack Visualization', 'Forensics', 'Event Correlation', 'Monitor', and 'Event Workflow'. The main content area displays a table titled 'Binaries list' with the following data:

<input type="checkbox"/>	<u>Trap name</u>	<u>MD5 hash</u>	<u>File size</u>	<u>Timestamp</u>	<u>Analysis Report</u>
<input type="checkbox"/>	MyNewTrap	1f73402c644002a7ea3c9532e8ba4139	3 (0.00 KB)	13.05.2018 00:53:54	
<input type="checkbox"/>	MyNewTrap	a8f5f167f44f4964e6c998dee827110c	6 (0.01 KB)	12.05.2018 23:28:46	
<input type="checkbox"/>	appliance1_MT	d41d8cd98f00b204e9800998ecf8427e	0 (0.00 KB)	11.05.2018 17:22:21	
<input type="checkbox"/>	MyNewTrap	d41d8cd98f00b204e9800998ecf8427e	0 (0.00 KB)	11.05.2018 17:22:21	

TRAPX ДЛЯ ЗАЩИТЫ SCADA НА PHDAYS



HONEY POT ДЛЯ ЗАЩИТЫ БАНКА НА PHDAYS



PHDays Bank Pro CMS

Administrators Panel

Login

Password

Sign in

© 2017 PHDays Bank





СПАСИБО ЗА ВНИМАНИЕ!

31/05/2018

**Анна
Богданова**

Руководитель направления SOC ЦИБ АО «Инфосистемы Джет»
av.bogdanova@jet.msk.su / +7 916 784-70-95