MDR SOC services practice in Russia
Real-life cases and collaboration with CERTs

Anton Yudakov
CISSP, CISM

Head of Operations - Rostelecom-Solar JSOC

BAKU Sep 05, 2018

Agenda

- A few words about Rostelecom-Solar JSOC
- Security Operations: how we operate, a few real-life cases
- Security Operations: how we use TI (Threat Intelligence) and partners info exchange

Rostelecom-Solar

#1

Cybersecurity
service provider in Russia

350+

Cybersecurity experts

Our Business

- Cybersecurity service provider
- Information security vendor
- Information security systems integrator

SOLAR JSOC

The first and the largest commercial MDR SOC service provider in Russia and CIS

Enterprise clients

>60

Cybersecurity experts

>110

Years of Detection and Response

6+

JSOC clients

Банк Санкт-Петербург

МТС Банк

NSPK National Payment Card System MIR

Башкомснаббанк

Тинькофф

media

Уральский Банк реконструкции и развития

Почта Банк

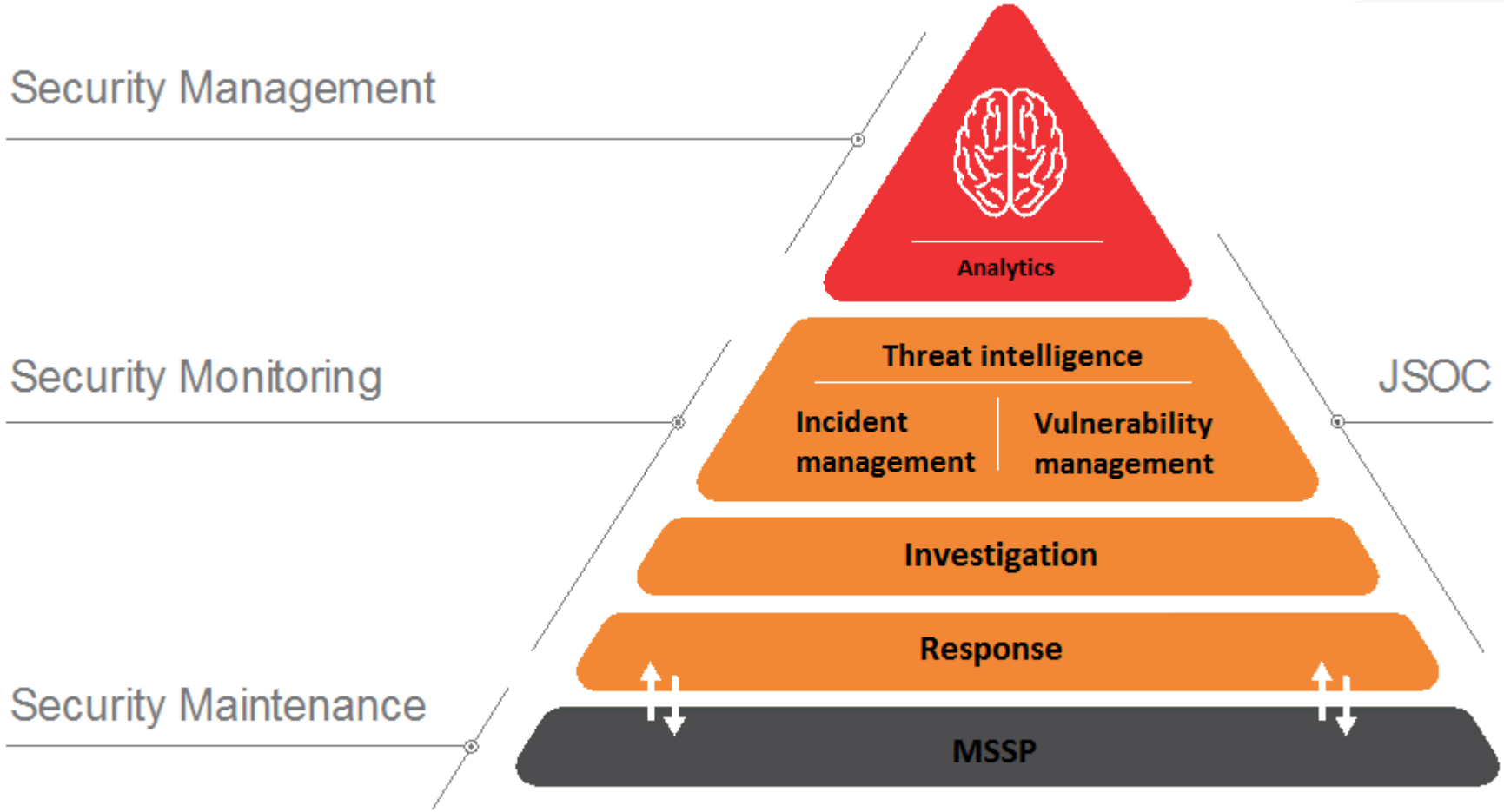
Юнипро

Росфинмониторинг

Министерство информационных технологий и связи Хабаровского края

LEROY MERLIN

Our SOC\service model



Rostelecom-Solar JSOC team

Heads

JSOC architect and development teams

Forensics, malware analysis and pentest teams

Service managers

MDR

Analysts (experts)

2nd line

2nd line

1st line

1st line

MSSP

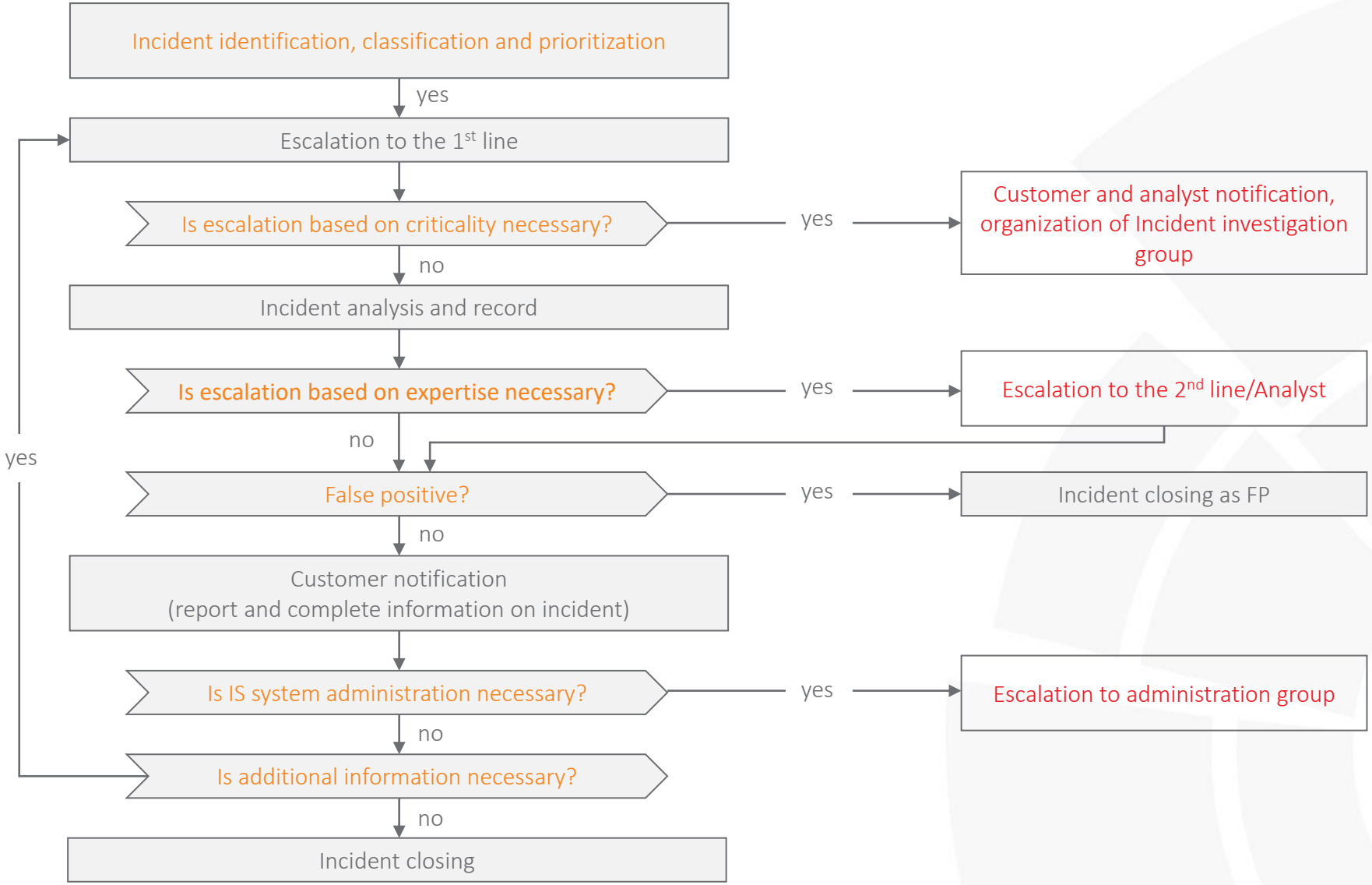
IS Admins (experts)

2nd line

1st line

JSOC Security Operations Center

JSOC incident workflow

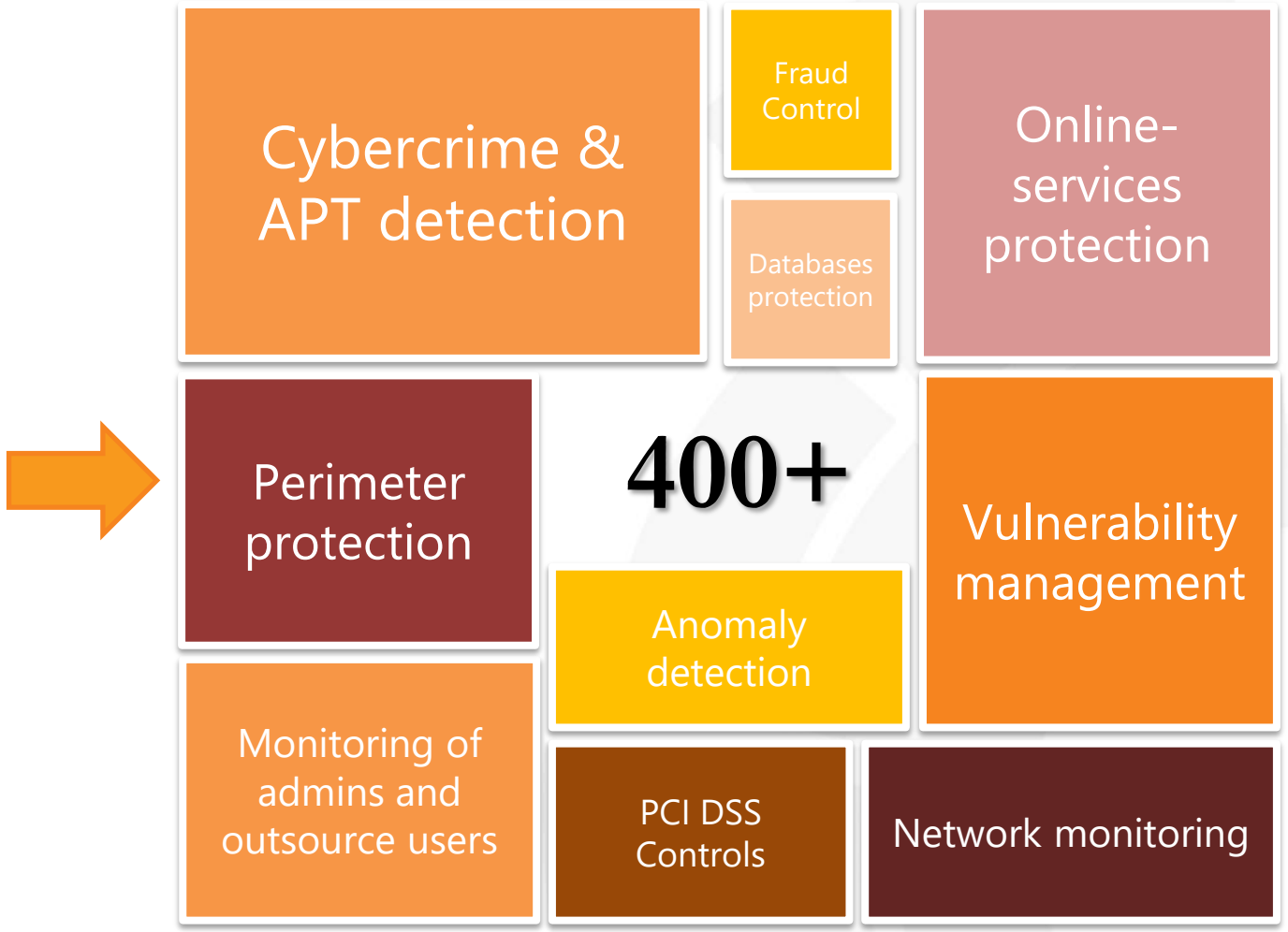


SLA

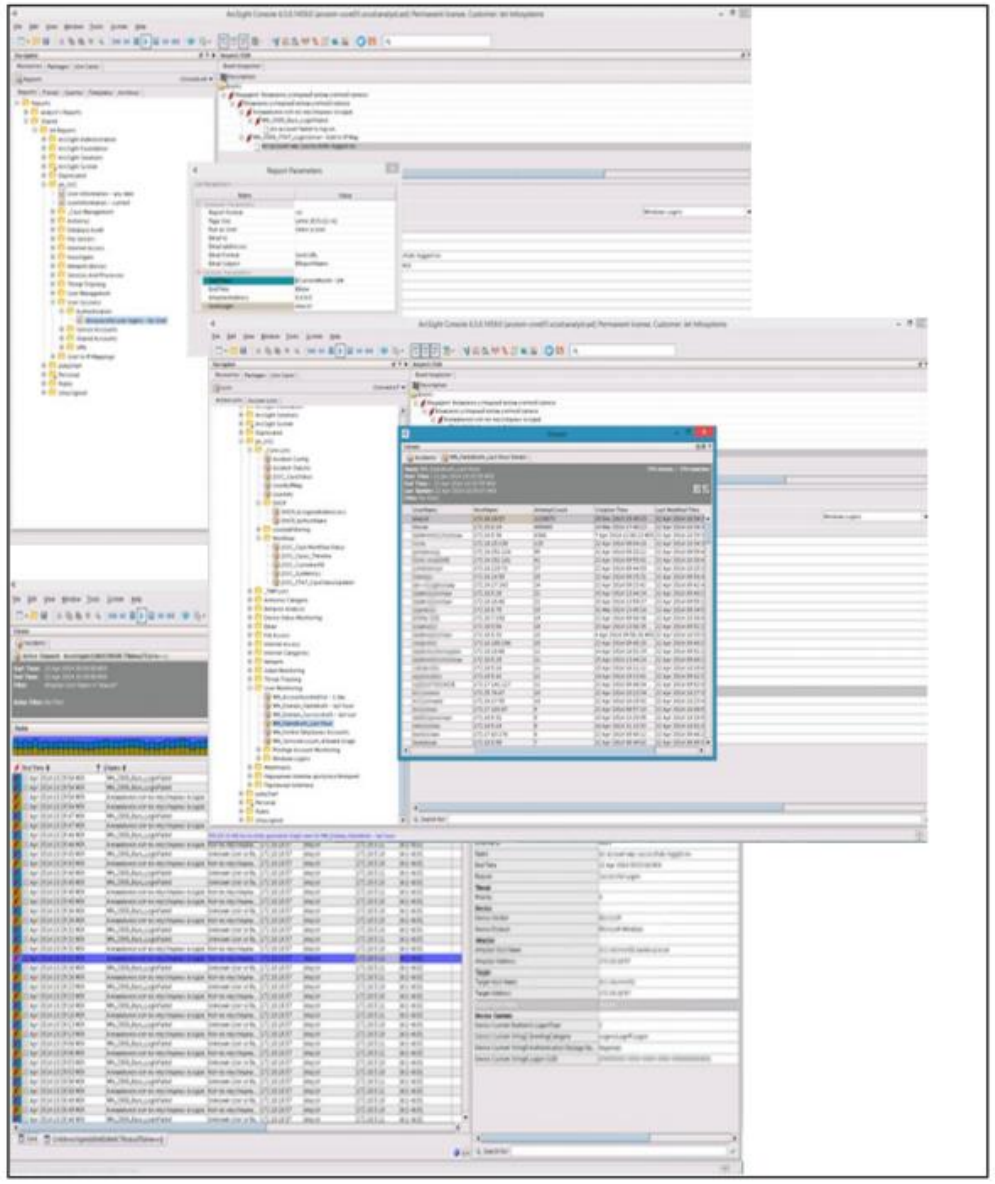
99,4%	10 min	30 min
Service availability	Time to detect	Time to respond

Use cases

6+ Years of
Detection and Response



Incident monitoring: SIEM vs SOC



1.	Incident name:	RemoteAdminTools outgoing host activity
2.	Date and time:	18 Jul 2017 03:08:02 MSK
3.	Detailed incident description:	Remote administration tool vuupc (bluecoat categorization) launch is detected on _____ host (ip address - _____) Log in attempts to ip address 173.193.202.79 are blocked by ACL Current activity is detected for the first time on this host. Active user on the host isn't identified Last activity was registred 17 Jul 18:59:03, User account ____
4.	How incident was detected:	Bluecoat log analysis
5.	Cause of incident:	Remote administration tool launch on the host
6.	Information about log source:	===== Information about system ===== Source host name: _____ Zone name: ___user1_vlan100_10.0.0.0 ===== Information about user ===== Name: _____ Position: Head of department Company: _____ Department: Law department Phone: _____ E-mail: _____
7.	Information about target:	Inetnum: 173.193.202.79 Netname: vuupc.com Country: Brazil
8.	Recommend ations:	To check if remote administration tool launch on the host is legitimate. If it is not, then remove prohibited software
9.	Additional information:	VuuPC is a siftware for Remote administration from other computer or mobile device, connected to the Internet. Several resources categorize this software as malware

Working with SIEM content: from suspected incident to a real one

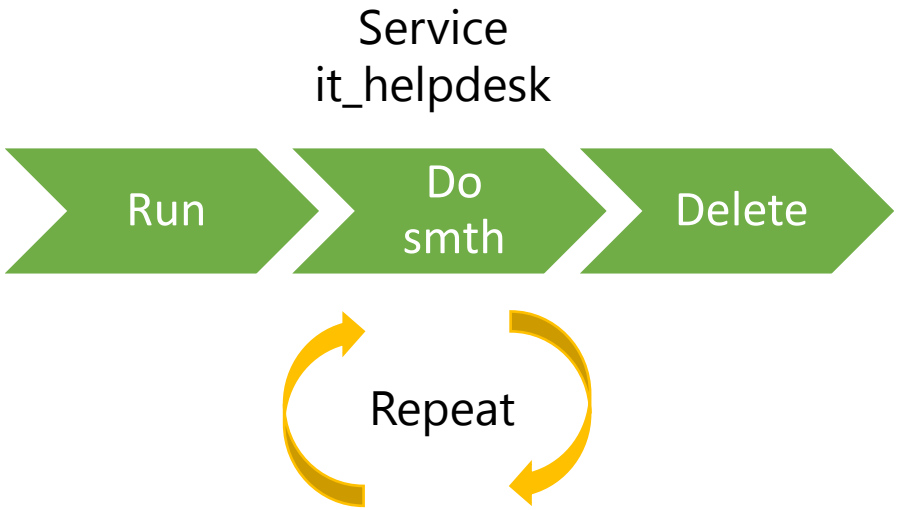
Basic scenarios (indirect indicators)	A potential Incident
Incoming e-mail from an unknown sender	Almost 100% probability of an infected host. A possible targeted attack on a host.
Non-legitimate process (software) started on a host	
Remote Access Tools/TOR/Feeds activity from host	
New local Administrator account created on a host	
Registry modification according to RDP limitations on a host	
A lot of unsuccessful connections from an internal host to an external network (Internet)	A possible botnet / unknown malware.
Internet activity to known malwared-hosts (Feeds / Proxy categorization)	
Remote access activity from an internal host to outside network (Internet)	

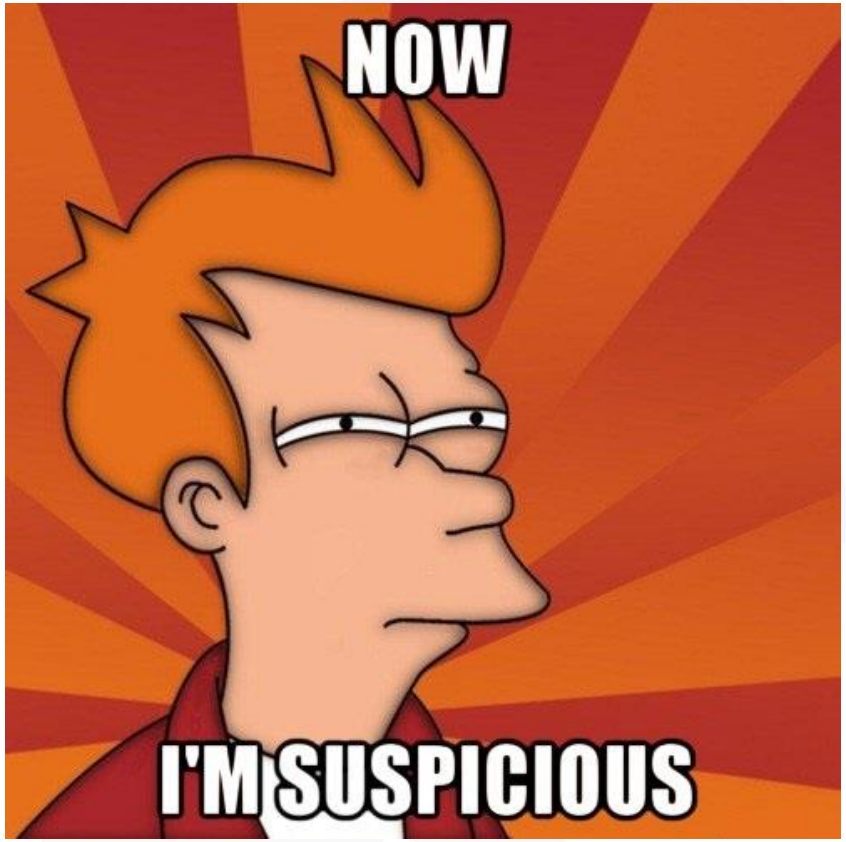
JSOC APT detection approach

- Identifying APT at early stages – aggregation of Threat Intelligence and Threat Hunting
- >90% of typical deployment vectors can be controlled by our general monitoring scenarios
- Maximum control on critical hosts and possible targets – profiling of critical systems

JSOC case #1 – APT

- Print manager server

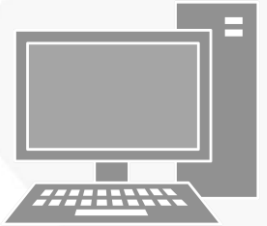




JSOC case #1 – Investigation

- Service was detected on:

19 Servers



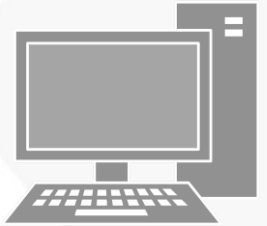
20 Workstations

And it was …somewhat like PSExec

JSOC case #1 – Investigation

- Service was detected on:

19 Servers



20 Workstations

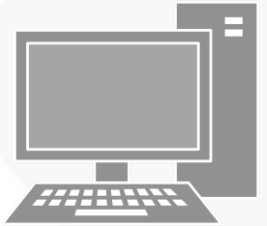
And it was …somewhat like PSExec

- C&C connection through DNS tunnel
- Keylogger

JSOC case #1 – Investigation

- Service was detected on:

19 Servers



20 Workstations

And it was …somewhat like PSExec

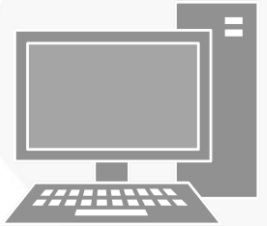
- C&C connection through DNS tunnel
- Keylogger

Compromised accounts

JSOC case #1 – Investigation

- Service was detected on:

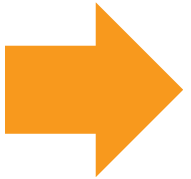
19 Servers



20 Workstations

And it was …somewhat like PSExec

- C&C connection through DNS tunnel
- Keylogger

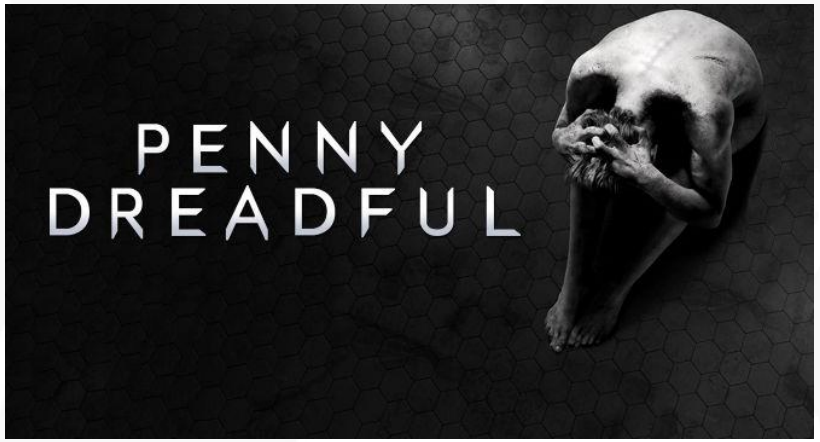


Compromised accounts

Transfer through DNS tunnel

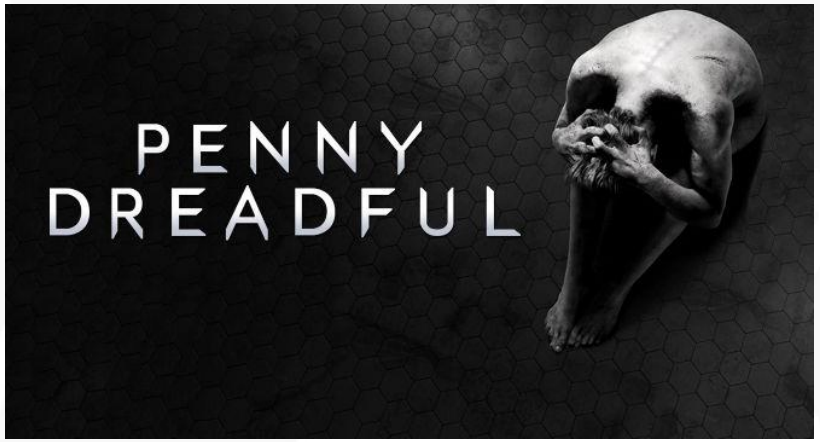
JSOC case #2

- What happened
  - Accountant connected USB flash drive to the workstation
  - That contained 0-day malware … here we go again
  - 0-day incorporated itself to a system processes
- Outcome:
  - It was hidden for 1 year
  - Saved screenshots and gathered passwords
  - Without financial damage … fortunately



JSOC case #2

- What happened
  - Accountant connected USB flash drive to the workstation
  - That contained 0-day malware … here we go again
  - 0-day incorporated itself to a system processes
- Outcome:
  - It was hidden for 1 year
  - Saved screenshots and gathered passwords
  - Without financial damage … fortunately
- How to detect:
  - Monitoring of critical hosts
  - Monitoring of activities to C&C centers



How we detected this incident: anomaly activity on a critical host

JSOC case #3

- What happened
  - IT administrator downloaded warez for work
  - That contained 0-day malware …
  - That deleted anti-virus agent and created a fake agent
- Outcome:
  - 10 infected hosts
  - Attempt to infect chief accountant machine
  - Without financial damage … fortunately

JSOC case #3

- What happened
  - IT administrator downloaded warez for work
  - That contained 0-day malware …
  - That deleted anti-virus agent and created a fake agent
- Outcome:
  - 10 infected hosts
  - Attempt to infect chief accountant machine
  - Without financial damage … fortunately
- How to detect:
  - Monitoring of critical hosts
  - Monitoring of attempts to communicate with C&C servers

How we detected this incident: communication with C&C servers

JSOC case #3

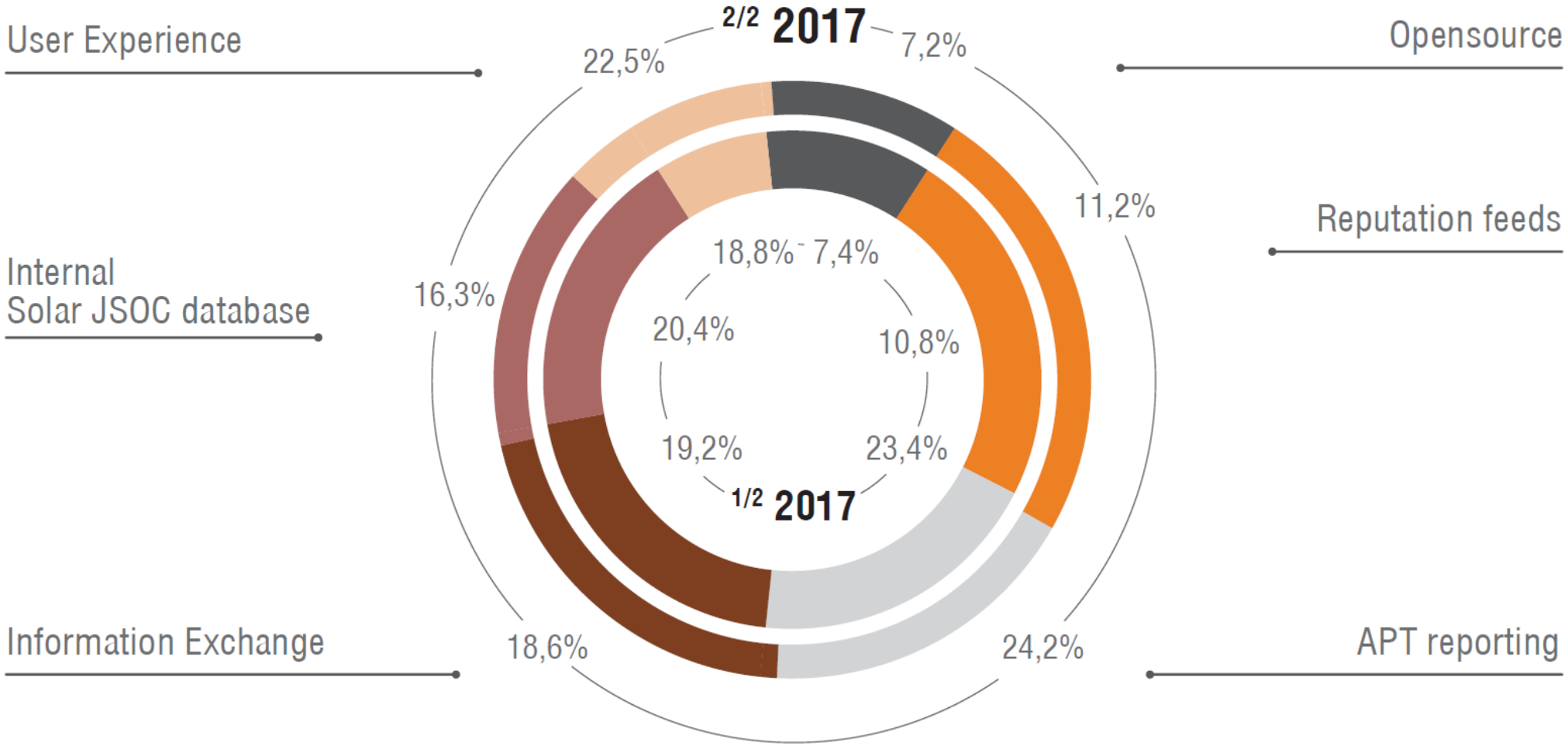
- What happened
  - IT administrator downloaded warez for work
  - That contained 0-day malware …
  - That deleted anti-virus agent and created a fake agent
- Outcome:
  - 10 infected hosts
  - Attempt to infect chief accountant machine
  - Without financial damage … fortunately
- How to detect:
  - Monitoring of critical hosts
  - Monitoring of **attempts to communicate with C&C servers**

How we detected this incident: **communication with C&C servers**

Threat Intelligence – looks simple…

- Threat Intelligence sources:
  - Paid subscriptions (broadcasting) – feeds from Antivirus, Network security and other security vendors.
  - Paid subscriptions (targeted) – feeds and IOCs from CERTs, research labs, etc.
  - Partners info exchange – Russian CERTs (FinCERT, GOV-CERT), SOC club, etc.
  - Your own research – if possible
  - Users requests – are priceless

JSOC Threat Intelligence sources according to incidents detected



Threat Intelligence case #1

- The Silence group/campaign:
  - Sep 21, 2017 – some info and IOCs from an APT campaigns report provider including winexe tool service
  - Oct 13, 2017 – the first mass email campaign on banks, first samples from our clients, so we have our own IOCs and we send them to our partners
  - Oct 13, 2017 a few hours later – the first FinCERT bulletin on the case with some IOCs
  - Oct 17, 2017 – the second mass email campaign on banks, first samples from our clients, so we have our own IOCs and we send them to our partners
  - Oct 17, 2017 – an additional info and IOCs from an APT campaigns report provider
  - Oct 20, 2017 – the second FinCERT bulletin on the case with some IOC including the new ones

  …
  - Aug, 2018 – info and a lot of IOCs on the Silence group and their instruments and TTPs from one of security vendors.

Threat Intelligence case #2

- A new 0-day published for OS Windows – local privilege escalation vuln

Threat Intelligence case #2

- A new 0-day published for OS Windows – local privilege escalation vuln

Threat Intelligence case #2

- But is that so important and critical to our infrastructure?
- Do we need to apply any workarounds immediately?
- If so – which one and why?

- BTW …in a plenty of companies all around the world Windows Task Scheduler is used to run scripts using admin user accounts. It's also a local privilege escalation vulnerability which in fact is a security misconfiguration. And in fact you don't need any exploits to download and run for privilege escalation.

Threat Intelligence – …is not simple in fact

- But TI is a need
- And here is some advice:
  - Don’t use all of Feeds and IOCs you may find, analyze their quality
  - While analyzing look if there any additional context info and description (ex.: winexe/psexec could be used by both adversaries and IT system administrators)
  - While using TI use it right:
    - Analyze IOCs relevance
    - Add verified IOCs to real-time monitoring and at the same time run a background retrospective check
    - Preventively block critical and definitely dangerous IOCs
    - What you can’t monitor – check periodically

Thank you!

Anton Yudakov
CISSP, CISM

Head of Operations - Rostelecom-Solar JSOC

a.yudakov@solarsecurity.ru
www.solarsecurity.ru