KASPERSKY lab

Industrial Cybersecurity 2018:
Opportunities and challenges in Digital Transformation

VLADIMIR KARANTAEV

Honeywell
Russia

- Has more than 16 year experience in IT and IS
- Authtor of a Smart Grid blog

smartgridib.blogspot.com

Managed Detection and Response (MDR) Delivery Models for Industrial Control Systems (ICS)

Karantaev Vladimir
Head of ICS Cyber Security
Ph.D. , IEC Expert, CIGRE Expert
v.karantaev@solarsecurity.ru
+79152211596

Sochi

September 20, 2018

Do we have anything to argue about? What about terminology? OT или ICS?

Gartner defines operational technology (OT) as: "hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in asset-centric enterprises, particularly in production and operations."

ICS is a complex of software and software hardware aimed at controlling technological and/or industrial equipment (control devices) and their processes as well as management of such equipment and processes;

Depending on the type of business we can speak about the following kinds of AS: Industrial Control Systems (ICS)…

Depending on the type of managed object (process) ICS can be, for example, ICS of Technological Processes (ICSTP), ICS of enterprise (MES) etc.

34.003-90

History in figures

5

Malware specifically designed for cyber attacks against Industrial Control Systems

- Stuxnet
- Havex
- Blackenergy
- Industroyer
- TRITON

1

Malware specifically designed for cyber attacks against safety instrumented system (SIS)

- TRITON

3

Malware specifically designed for industrial process disruption.

- Stuxnet
- Industroyer
- TRITON

History of methodology development

- **Reconnaissance:** research, identification and a selection of a cyber attacks target .
- **Weaponization.** coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool.
- **Delivery.** transmission of the weapon to the targeted environment.
- **Exploitation.** after the weapon is delivered to victim host, exploitation triggers intruders' code.
- **Installation.** installation of a remote access trojan or backdoor on the victim system and others actions.
- **Command and Control (C2).** intruders control the target environment..
- **Actions.** collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well

- **Develop:** identify target ICS type and develop malware.
- **Test:** ensure malware works as intended, likely off network in the adversary environment .
- **Delivery:** transfer malware to the ICS which contains the 'loader' module for the new logic and support binaries that provide the new logic.
- **Install/Modify:** execution and masking malicious code like a legal software
- **Attack:**

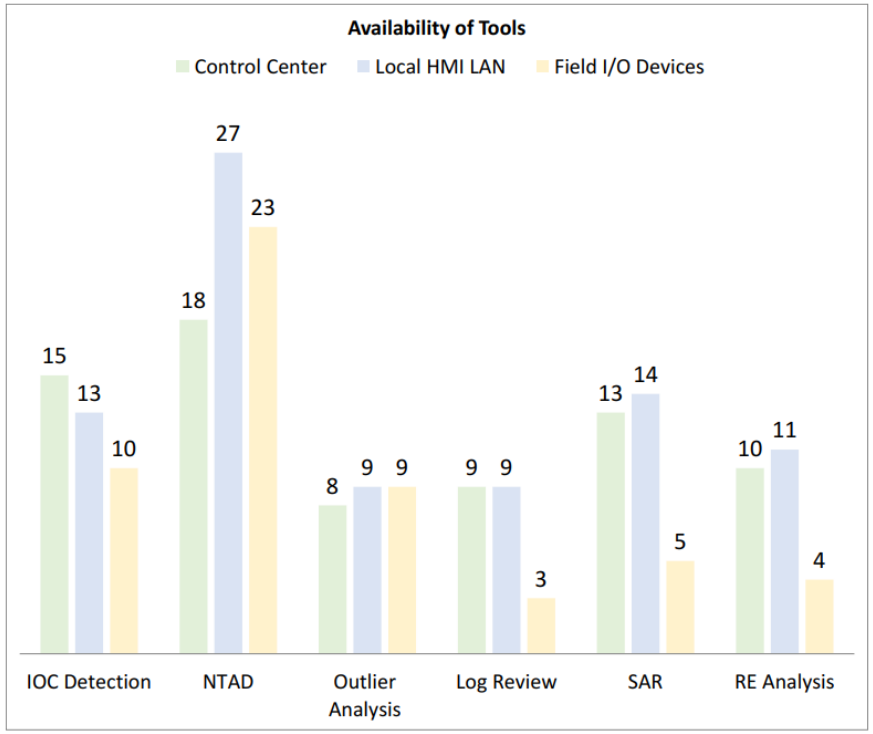
https://goo.gl/26VMMW

https://goo.gl/CYx6DN

https://goo.gl/utZSeJ

History of technology development

1. Multi-Purpose Tools
2. IOC Detection Tools
3. Network Traffic Anomaly Detection Tools
4. Outlier Analysis Tools
5. Log Review Tools
6. System Artifact Review Tools
7. Reverse Engineering Analysis Tools



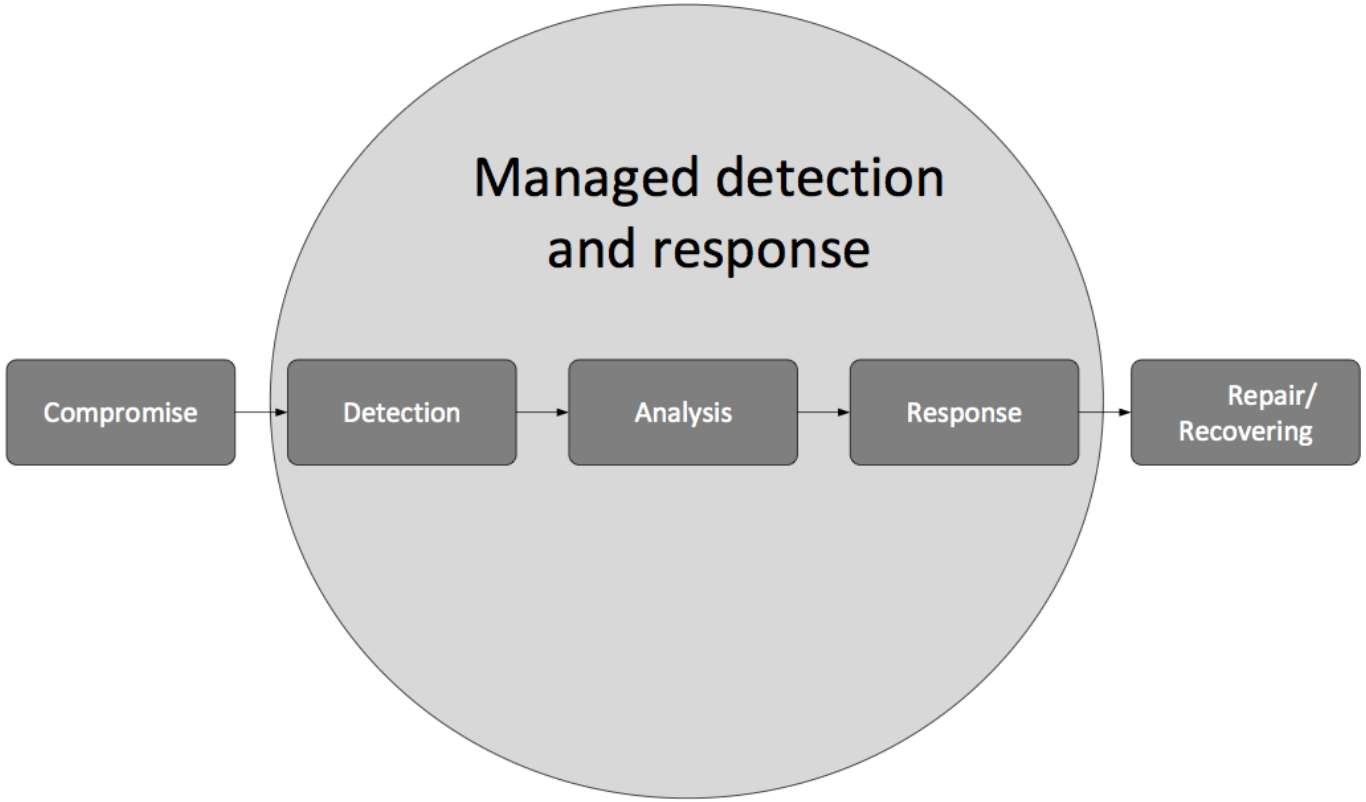
A Survey of Security Tools for the Industrial Control System Environment
The Idaho National Laboratory (INL) USA, 2017

Mature OT SOC is:

- 24/7/365 threat monitoring.
- High level of expertise.
- Well-defined processes.
- Analyst controlling infrastructure.
- Advanced analytics including

Threat Intelligence and Threat Hunting.

- Investigation of every security event.
- An individual plan for incident response.



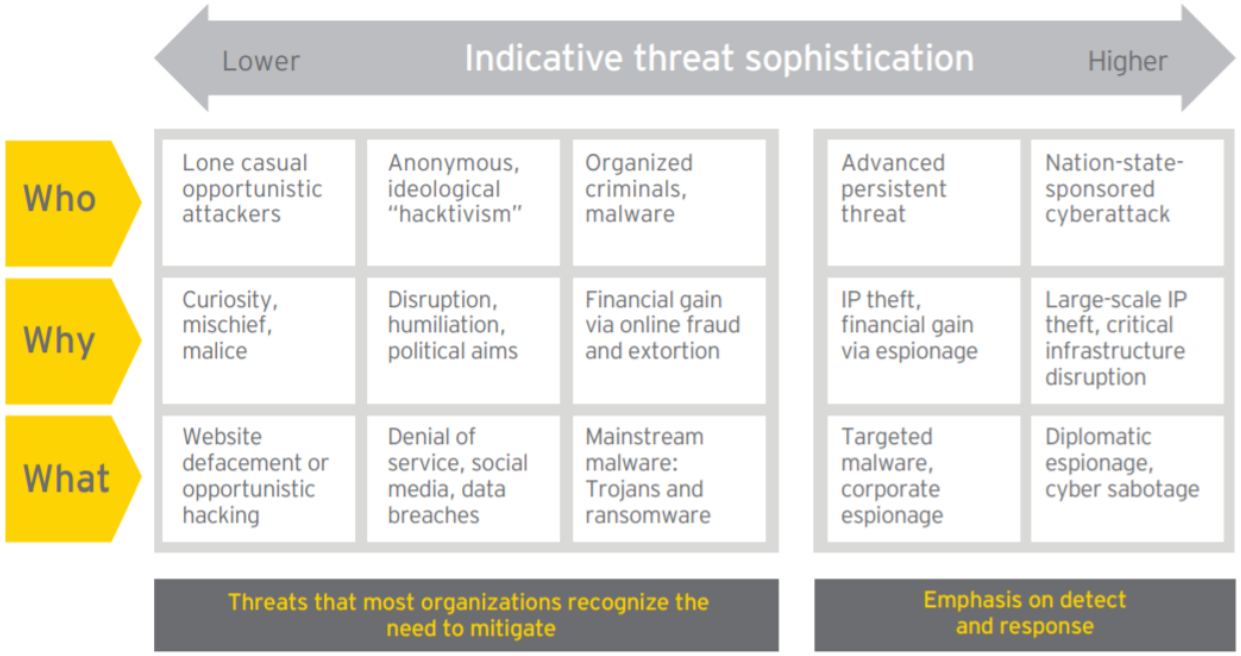
Why should we use MDR in ICS?

We start from the supposed level of ICS-related threat:

- APT-attacks.
- Nation-State sponsored cyberattack.

Therefore, emphasis should be made on detection and response.

SOC, built as MDR, intends to detect and response to advanced threats (APT-attacks).



EY:https://goo.gl/5qA8rN

Start conditions. Subsequent development.

Stage 1:

- Infrastructure of the protected object doesn’t have information security tools.

Stage 2:

- Infrastructure of the protected object has a fundamental security tools, e.g.

- Perimeter Security Gateway.
- Antivirus software.

Stage 3:

- Infrastructure of the protected object has ICS Security Tools:

- ICS Threat Detection Systems/ICS Asset Management System/ICS Network Intrusion Detection System (IDS).
- Industrial firewall.
- EndPoint Protection.
- EDR.

Stage 4:

- ICS includes a comprehensive built in security.

Basic architecture of the protected object

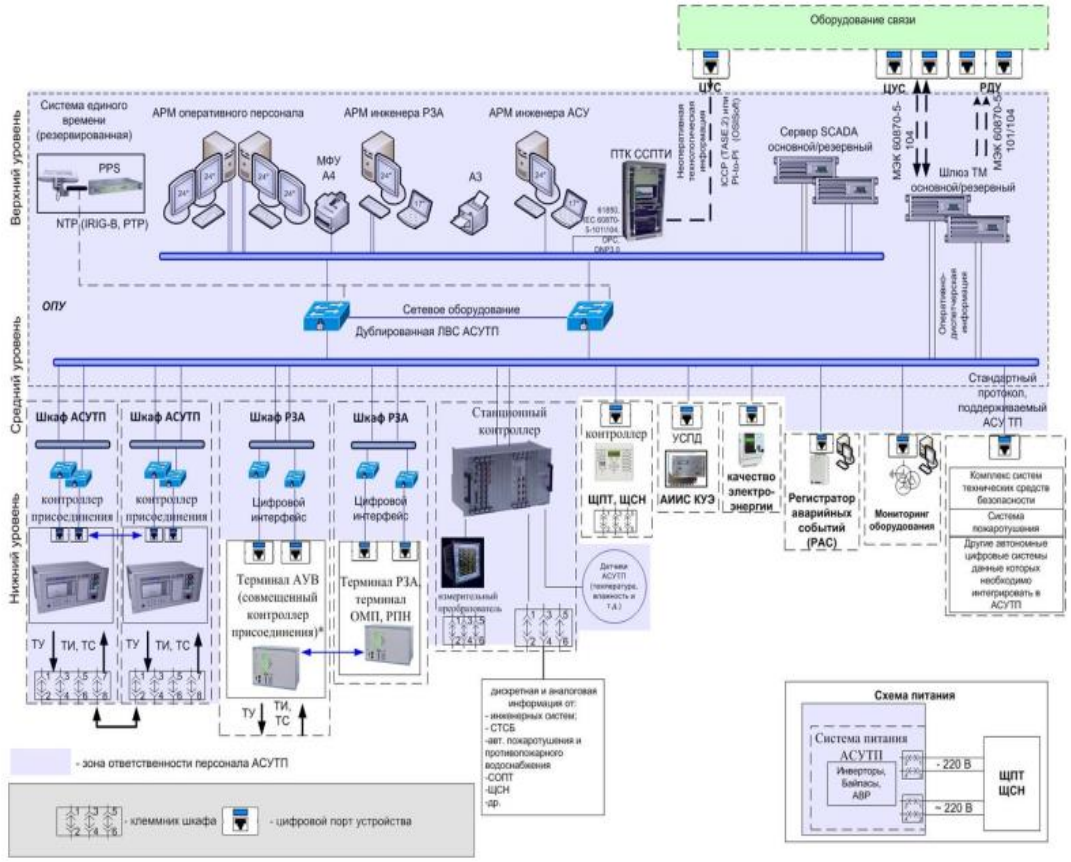
Detect network critical for protection nodes in the IT segment.

- IT workstation.

Detect network critical for protection nodes in the OT segment.

According to Russians and foreign standards at substation (digital substation) should be made:

- OT workstation.
- Workstation for configuration IED (PAC).
- ICS workstation.
- SCADA servers.
- ICS servers.
- AMI etc.



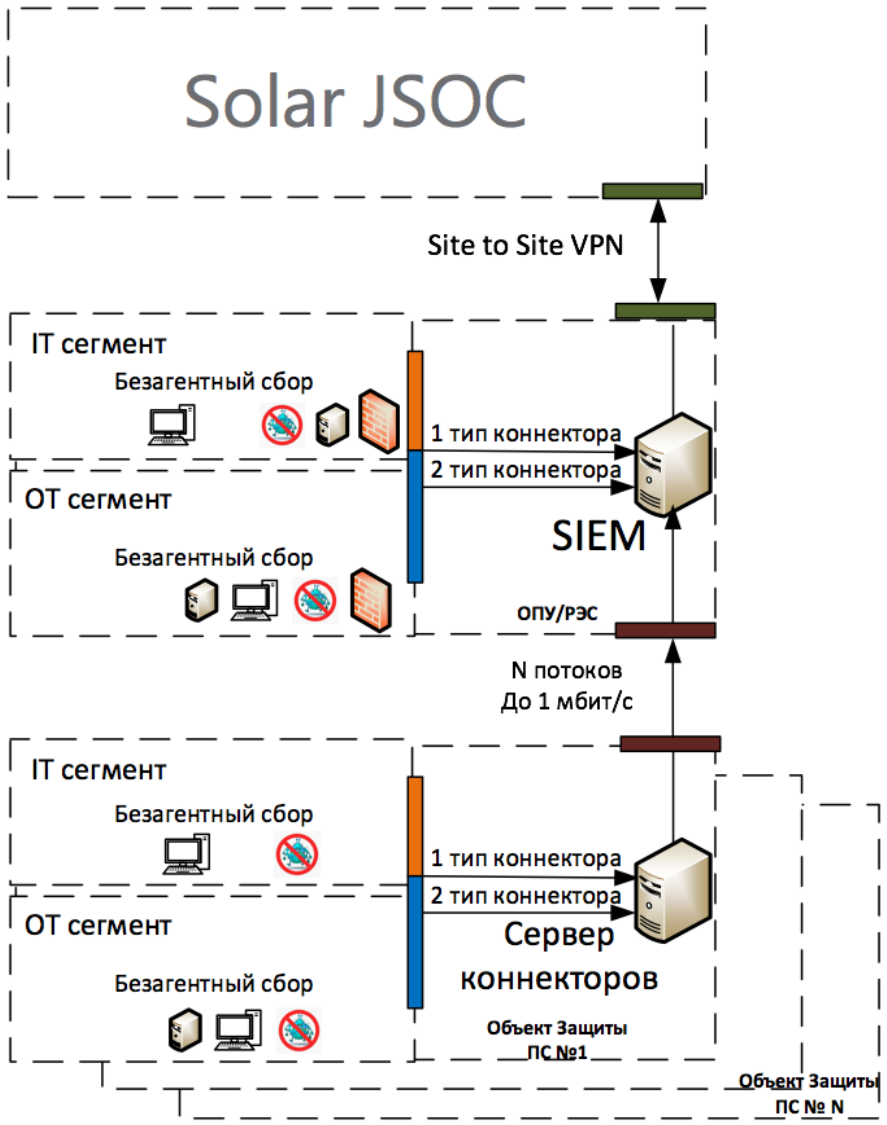
Basic architecture

Common Data Sources in IT Environments:

- Switches.
- Routers.
- IT workstation.
- Antivirus software.

Common Data Sources in IT Environments:

- Switches.
- OT workstation.
- Workstation for configuration IED (PAC).
- ICS workstation.
- SCADA servers.
- ICS servers.



Audit of workstation and servers under Windows System control

- Authentication;
- Account management;
- OS processes;
- Installation of OS services;
- Changes of file register: register criteria, file system objects;
- Network activity.

Security events audit in ICS

The following points are logged in the security log and forwarded to a connected syslog log server:

Actions:

- Successful log off of a user, even after a certain period of time.
- Successful log on of a user.
- Change or delete the connection password.
- Update or restore the firmware version in the device.
- Update the configuration in the device.
- Change the operating mode of the device.
- Change the date and time.
- Change or overwrite state value entries by the logged-on user.
- Switching operations by the registered user.

Potential errors:

- Number of entries with correct or incorrect passwords.
- Unsuccessful login attempt by typing 3 wrong passwords.
- Reboot or restart the device.

Basic control architecture should guarantee:

Intrusion into the technological process.

- Control, response and investigation into incidents of elements of the higher level of the ICS.
- 90% of tested SIEM scenarios of the IT-segment can be used to build a basic architecture of end-to-end monitoring.

Basic architecture should allow to:

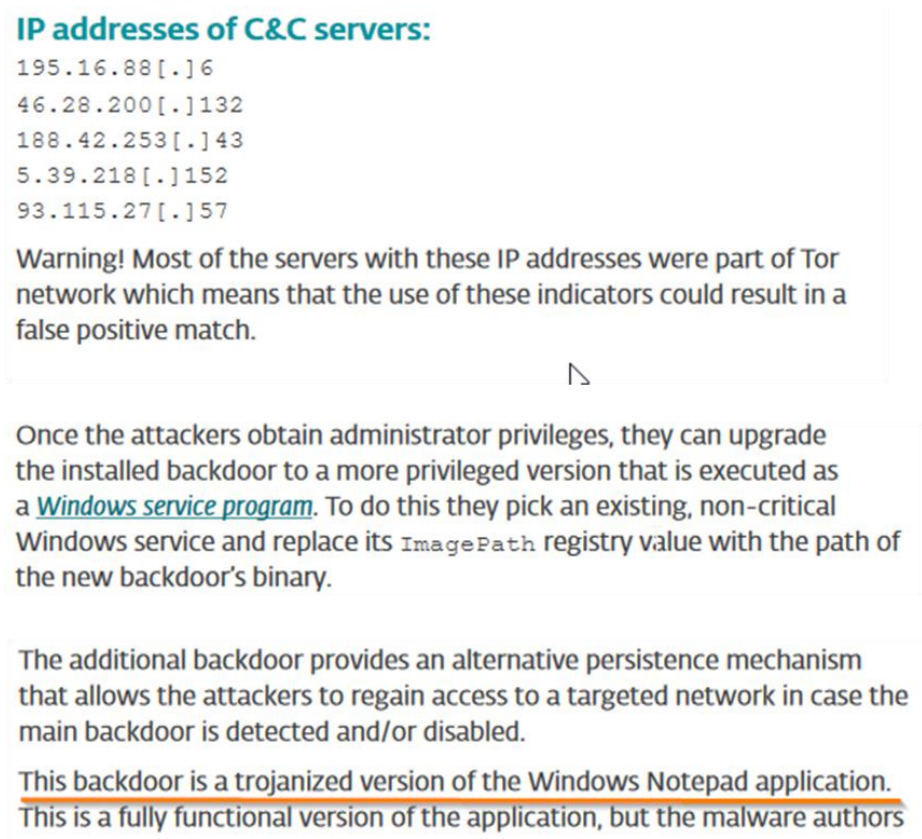
- Detect the attack development through kill chain stages.
- Detect suspicious traffic from the mission critical segment (Tor, etc).
- Detect changes brought into processes, structure of files of mission critical nodes.
- Detect attempts to escalate privileges.
- Detect new unknown nodes in the mission critical segment.
- Detect changes brought into the selection of services started in the mission critical segment.

Investigation into the suspected incident and fast response will come to the front.

How to detect Industroyer activity:

ESET document analysis:

- Main backdoor: the main module is connected to C&C servers with Tor.
- We should detect on outputs TOR feeds.
- We should detect changing a critical DLL in folders windows or system 32.
- We should detect a new system service start.
- We should detect changing a critical file.



IP addresses of C&C servers:

195.16.88[.]6
46.28.200[.]132
188.42.253[.]43
5.39.218[.]152
93.115.27[.]57

Warning! Most of the servers with these IP addresses were part of Tor network which means that the use of these indicators could result in a false positive match.

Once the attackers obtain administrator privileges, they can upgrade the installed backdoor to a more privileged version that is executed as a *Windows service program*. To do this they pick an existing, non-critical Windows service and replace its `ImagePath` registry value with the path of the new backdoor's binary.

The additional backdoor provides an alternative persistence mechanism that allows the attackers to regain access to a targeted network in case the main backdoor is detected and/or disabled.

This backdoor is a trojanized version of the Windows Notepad application. This is a fully functional version of the application, but the malware authors

https://goo.gl/DjaaCV

Advantages:

Possible predictable result:

Minimize the influence of the incident and business risk of malfunction of technological processes, which means keeping functioning of the protected object at the necessary integrity level.

- Earlier detection of incidents and stages of APT-attacks.
- Fast response in case of incident detection and analysis.
- High possibility of successful investigation of the incidents, which will allow to manage cyber security risks more effectively.

Easier compliance with the Regulator’s requirements and using of best practices.

Mature architecture of the protected object :

Common Data Sources in IT Environments:

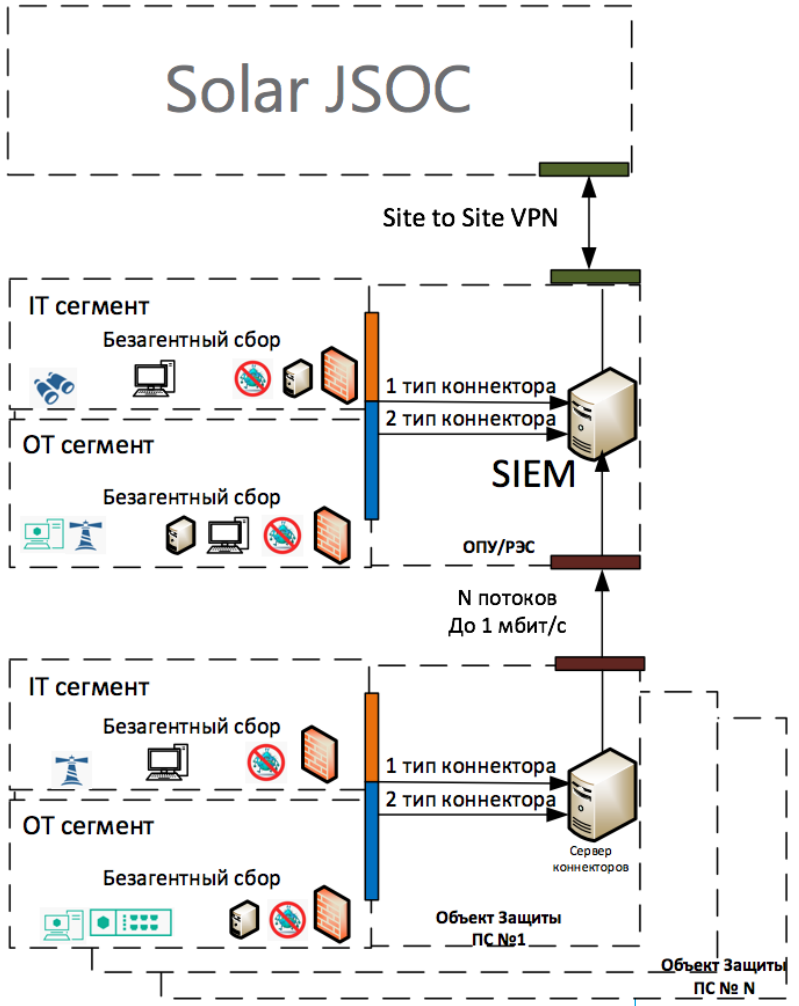
- Switches;
- Routers
- Endpoint Protection Software.
- IT workstation.
- Antivirus software.
- Perimeter Security Gateway.
- Intrusion Detection System (IDS).

Common Data Sources in OT Environments:

- IED, PLC – with Syslog:

Tailored ICS cyber security tools:

- ICS Threat Detection Systems/ICS Asset Management System/ICS Network Intrusion Detection System (IDS).
- Industrial firewall.
- Endpoint Protection Software.



Conclusion:

Implementation of SOC OT allows to:

- Raise a number of detected incidents.
- Detect aberrant behavior.
- Raise the possibility of ART-attack detection at the earlier stage.
- Minimize the influence of such incidents on the technological process.
- Minimize business risks which threaten the functioning of the company.

Implementation of solutions and services improving situational awareness allows:

- Suggest well-founded measures of reducing the influence of cyber attacks.
- Raise the quality of response to incidents.
- Make conclusions based on data.
- Develop a strategy of risk management at a whole new level.
- Easier compliance with the Regulators requirements and implementation of best practices.

Your questions…

Vladimir Karantaev
v.karantaev@solarsecurity.ru

Sochi September 20, 2018