kaspersky

Обзор источников сценариев атак для оценки эффективности систем защиты и мониторинга промышленных сетей

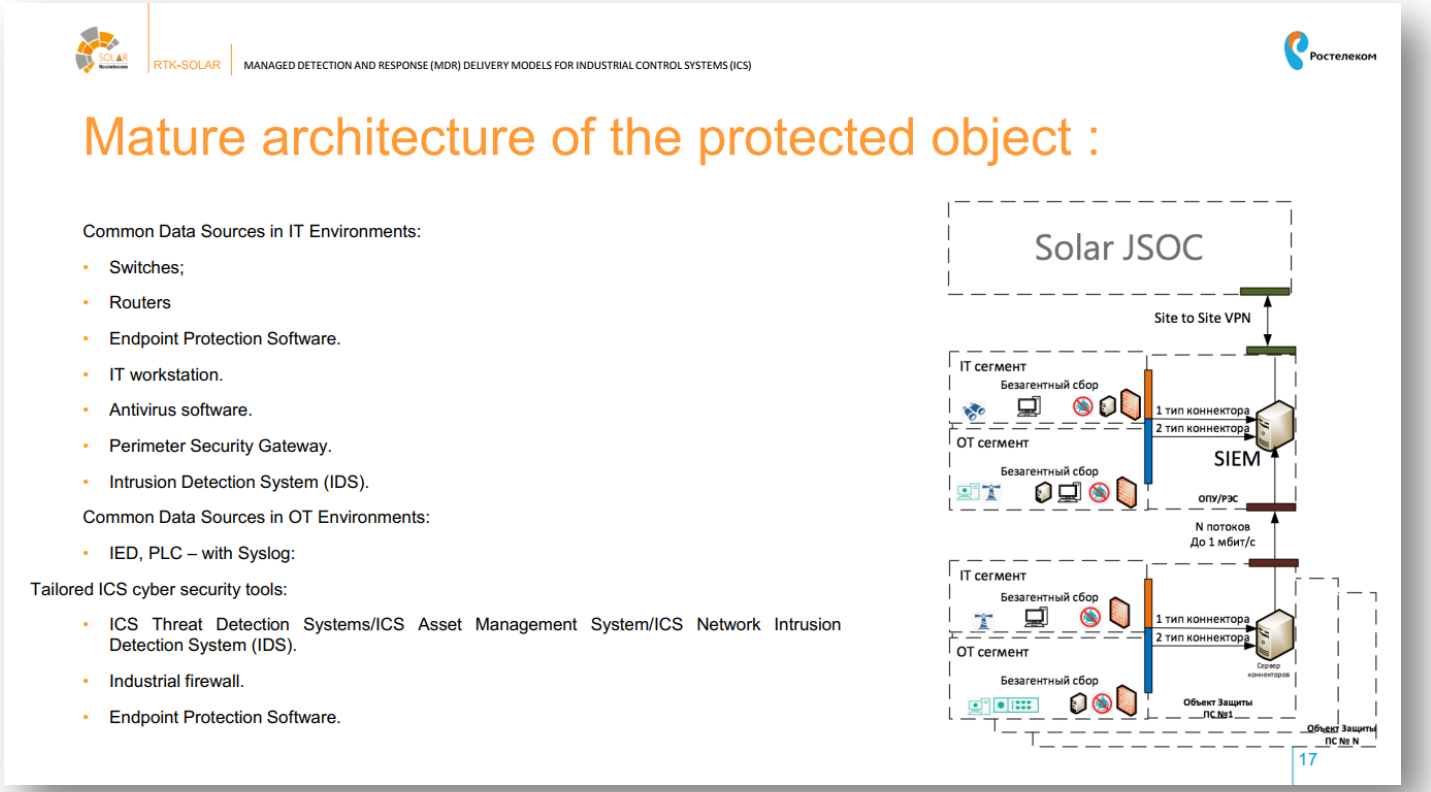
Антон Шипулин, CISSP, CEH, CSSA

Проблема

- Заказчикам нужны критерии для выбора эффективных систем кибербезопасности АСУ ТП

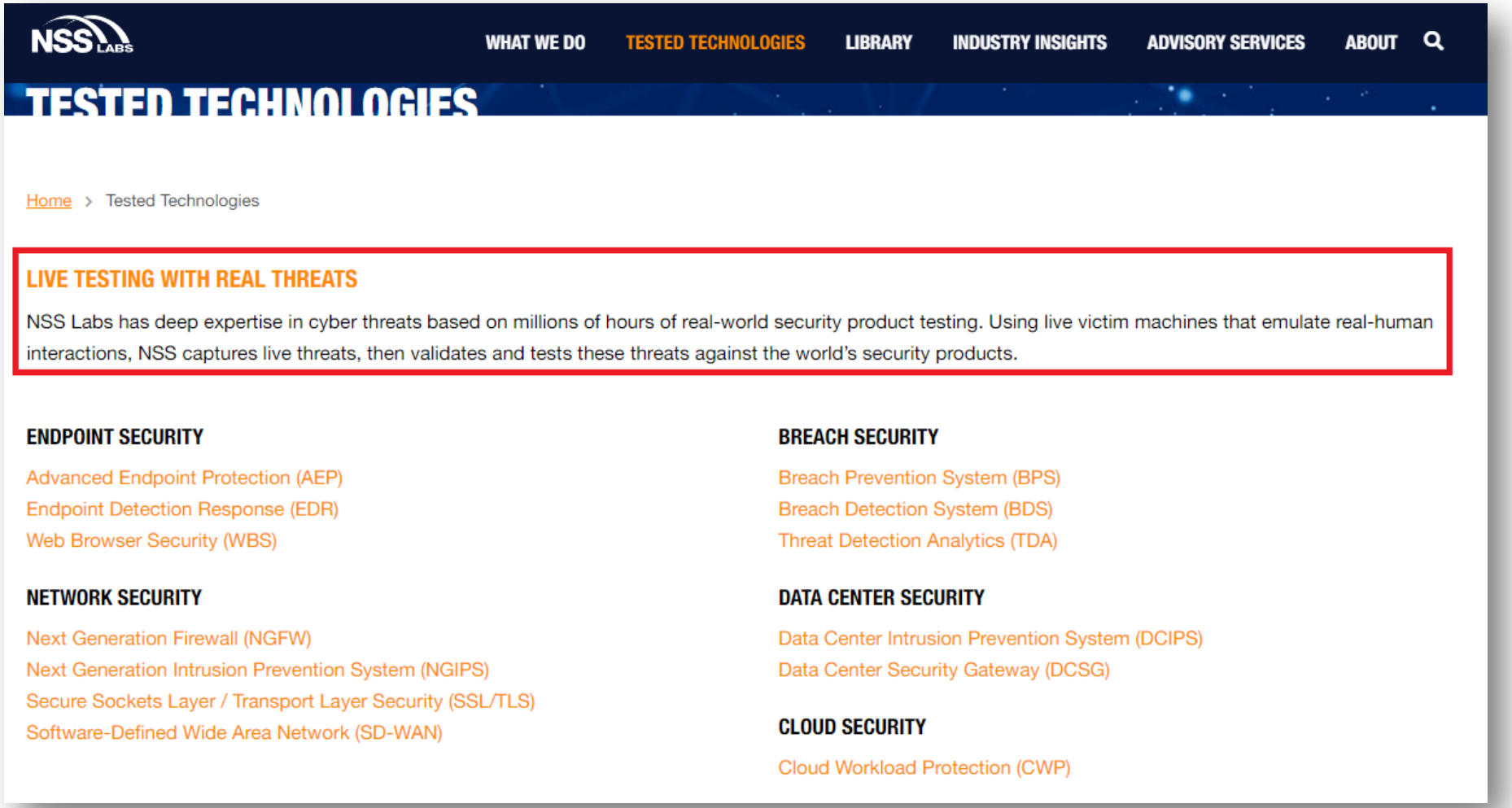
- Заказчикам нужны критерии для оценки эффективности возможности существующих систем кибербезопасности АСУ ТП и SOC целиком

- SOCам и вендорам систем кибербезопасности АСУ ТП нужны критерии для оценки эффективности своих возможностей



https://ics.kaspersky.com/media/ics-conference-2018/Vladimir-Karantaev-Managed-detection-and-response-MDR-delivery-models-for-industrial-control-systems-ICS-En.pdf

NSS Labs. Пока нет теста для решений **ICS Security**



https://www.nsslabs.com/tested-technologies/

Источники сценариев/техник атак

Intrusion Datasets/PCAPs

Techniques frameworks

- MITRE ATT&CK Enterprise
- MITRE ATT&CK ICS (in progress)
- CAT/CAFFEINE (in progress)

Промышленные полигоны/учения

- iTrust CISS, Singapore
- Kaspersky Industrial CTF
- The Standoff
- S4 ICS Detection Challenge
- Locked Shields

Реальные инциденты

- Industroyer
- Stuxnet
- Triton

Research papers

- arXiv.org
- GitHub/GitLab
- IEEE Xplore Library
- ScienceDirect
- ResearchGate
- ScienceOpen
- Google Scholar
- CREDC

Safety Studies / CCE

- PHA/HAZOP
- Accidents reports
- Safety/Hazard/Failure analysis

Practical Guides

- NISTIR 8219. BAD
- …

Intrusion Datasets

TABLE II
OVERVIEW OF NETWORK-BASED DATA SETS.

	General Information				Nature of the Data			Data Volume		Recording Environment			Evaluation		
Data Set	Year of Traffic Creation	Publicly Avail.	Normal Traffic	Attack Traffic	Meta-data	Format	Anonymity	Count	Duration	Kind of Traffic	Type of Network	Compl. Network	Predef. Splits	Balanced	Labeled
AWID [51]	2015	o.r.	yes	yes	yes	packet	none	37M packets	1 hour	emulated	small network	yes	yes	no	yes
Booters [52]	2013	yes	no	yes	no	packet	yes	250GB packets	2 days	real	small network	no	no	no	no
Botnet [5]	2014	yes	yes	yes	yes	packet	none	14GB packets	n.s.	emulated	diverse networks	yes	yes	no	yes
CIC DoS [53]	2017	yes	yes	yes	no	packet	none	4.6GB packets	24 hours	emulated	small network	yes	no	no	yes
CICIDS 2017 [25]	2017	yes	yes	yes	yes	packet, bi. flow	none	3.1M flows	5 days	emulated	small network	yes	no	no	yes
CIDDS-001 [24]	2017	yes	yes	yes	yes	uni. flow	yes (IPs)	32M flows	28 days	emulated and real	small network	yes	no	no	yes
CIDDS-002 [30]	2017	yes	yes	yes	yes	uni. flow	yes (IPs)	15M flows	14 days	emulated	small network	yes	no	no	yes
CDX [54]	2009	yes	yes	yes	yes	packet	none	14GB packets	4 days	real	small network	yes	no	no	no
CTU-13 [3]	2013	yes	yes	yes	yes	uni. and bi. flow, pcap	yes (payload)	81M flows	125 hours	real	university network	yes	no	no	yes with BG.
DARPA [55], [56]	1998/99	yes	yes	yes	yes	packet, logs	none	n.s.	7/5 weeks	emulated	small network	yes	yes	no	yes
DDoS 2016 [57]	2016	yes	yes	yes	no	packet	yes (IPs)	2.1M packets	n.s.	synthetic	n.s.	n.s.	no	no	yes
IRSC [58]	2015	no	yes	yes	no	packet, flow	n.s.	n.s.	n.s.	real	production network	yes	n.s.	n.s.	yes
ISCX 2012 [31]	2012	yes	yes	yes	yes	packet, bi. flow	none	2M flows	7 days	emulated	small network	yes	no	no	yes
ISOT [59]	2010	yes	yes	yes	yes	packet	none	11GB packets	n.s.	emulated	small network	yes	no	no	yes
KDD CUP 99 [45]	1998	yes	yes	yes	no	other	none	5M points	n.s.	emulated	small network	yes	yes	no	yes
Kent 2016 [60], [61]	2016	yes	yes	n.s.	no	uni. flow, logs	yes (IPs, Ports, date)	130M flows	58 days	real	enterprise network	yes	no	no	no
Koyto 2006+ [62]	2006 to 2009	yes	yes	yes	no	other	yes (IPs)	93M points	3 years	real	honeypots	no	no	no	yes
LBNL [63]	2004 / 2005	yes	yes	yes	no	packet	yes	160M packets	5 hours	real	enterprise network	yes	no	no	no
MAWI [64]	2007 to now	yes	yes	yes	no	packet	yes (IPs and payload)	100M packets per day	15 min each day	real	ISP	yes	no	no	yes (IDS)
NDSec-1 [65]	2016	o.r.	no	yes	no	packet, logs	none	3.5M packets	n.s.	emulated	small network	yes	no	no	yes
NGIDS-DS [22]	2016	yes	yes	yes	no	packet, logs	none	1M packets	5 days	emulated	small network	yes	no	no	yes
NSL-KDD [66]	1998	yes	yes	yes	no	other	none	150k points	n.s.	emulated	small network	yes	yes	no	yes
PU-IDS [67]	1998	n.i.f.	yes	yes	no	other	none	200k points	n.s.	synthetic	small network	yes	no	no	yes
PUF [68]	2018	yes*	yes	yes	no	uni. flow	yes (IPs)	300k flows	3 days	real	university network	no	no	no	yes (IDS)
SANTA [38]	2014	no	yes	yes	no	other	yes (payload)	n.s.	n.s.	real	ISP	yes	n.s.	no	yes
SSENET-2011 [50]	2011	n.i.f.	yes	yes	no	other	none	n.s.	4 hours	emulated	small network	yes	no	no	yes
SSENET-2014 [69]	2011	n.i.f.	yes	yes	no	other	none	200k points	4 hours	emulated	small network	yes	yes	yes	yes
SSHCure [70]	2013 / 2014	yes	yes	yes	no	uni. and bi. flow, logs	yes (IPs)	2.4GB flows (compressed)	2 months	real	university network	yes	no	no	indirect
TRAbID [71]	2017	yes	yes	yes	no	packet	yes (IPs)	460M packets	8 hours	emulated	small network	yes	yes	no	yes
TUIDS [72], [73]	2011 / 2012	o.r.	yes	yes	no	packet, bi. flow	none	250k flows	21 days	emulated	medium network	yes	yes	no	yes
Twente [74]	2008	yes	no	yes	yes	uni. flow	yes (IPs)	14M flows	6 days	real	honeypot	no	no	no	yes
UGR 16 [32]	2016	yes	yes	yes	some	uni. flows	yes (IPs)	16900M flows	4 months	real	ISP	yes	yes	no	yes with BG.
UNIBS [75]	2009	o.r.	yes	no	no	flow	yes (IPs)	79k flows	3 days	real	university network	yes	no	no	no
Unified Host and Network [76]	2017	yes	yes	n.s.	no	bi. flows, logs	yes (IPs and date)	150GB flows (compressed)	90 days	real	enterprise network	yes	no	no	no
UNSW-NB15 [23]	2015	yes	yes	yes	yes	packet, other	none	2M points	31 hours	emulated	small network	yes	yes	no	yes

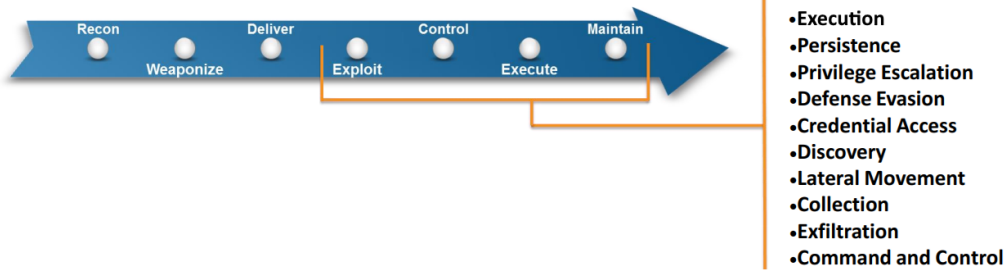
yes* = but not found under the given link, n.s. = not specified, n.i.f. = no information found, uni. flow = unidirectional flow, bi. flow = bidirectional flow, with BG. = with background labels

https://arxiv.org/abs/1903.02460v2

https://lukatsky.blogspot.com/2019/02/blog-post_26.html

MITRE ATT&CK. Что это?

ATT&CK – база знаний и классификация техник атакующих на различных этапах жизненного цикла



- **Initial Access**
- **Execution**
- **Persistence**
- **Privilege Escalation**
- **Defense Evasion**
- **Credential Access**
- **Discovery**
- **Lateral Movement**
- **Collection**
- **Exfiltration**
- **Command and Control**

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Image File Execution Options Injection			Forced Authentication	Network Share Discovery	AppleScript		Man in the Browser	Exfiltration Over Physical Medium	Multi-hop Proxy
Plist Modification			Hooking	System Time Discovery	Third-party Software		Browser Extensions		Domain Fronting
Valid Accounts			Password Filter DLL	Peripheral Device Discovery	Windows Remote Management		Video Capture	Exfiltration Over Command and Control Channel	Data Encoding
DLL Search Order Hijacking			LLMNR/NBT-NS Poisoning	Account Discovery	SSH Hijacking	LSASS Driver	Audio Capture		Remote File Copy
AppCert DLLs		Process Doppelgänging	Securityd Memory	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Automated Collection	Scheduled Transfer	Multi-Stage Channels
Hooking		Mshta	Private Keys	System Information Discovery	Pass the Ticket	Mshta	Clipboard Data	Data Encrypted	Web Service
Startup Items		Hidden Files and Directories	Keychain		Replication Through Removable Media	Local Job Scheduling	Email Collection	Automated Exfiltration	Standard Non-Application Layer Protocol
Launch Daemon		Launchctl	Input Prompt	Security Software Discovery		Trap	Screen Capture	Exfiltration Over Other Network Medium	
Dylib Hijacking		Space after Filename	Bash History			Source	Data Staged		Communication Through Removable Media
Application Shimming		LC_MAIN Hijacking	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Launchctl	Input Capture	Exfiltration Over Alternative Protocol	
AppInit DLLs		HISTCONTROL			Remote Desktop Protocol	Space after Filename	Data from Network Shared Drive		Multilayer Encryption
Web Shell		Hidden Users	Account Manipulation	System Owner/User Discovery	Pass the Hash	Execution through Module Load		Data Transfer Size Limits	Standard Application Layer Protocol
Service Registry Permissions Weakness		Clear Command History	Replication Through Removable Media		Exploitation of Vulnerability		Data from Local System	Data Compressed	
Scheduled Task		Gatekeeper Bypass		System Network Configuration Discovery	Shared Webroot	Regsvcs/Regasm	Data from Removable Media		Commonly Used Port
New Service		Hidden Window	Input Capture		Logon Scripts	InstallUtil			Standard Cryptographic Protocol
File System Permissions Weakness		Deobfuscate/Decode Files or Information	Network Sniffing	Application Window Discovery	Remote Services	Regsvr32			
Path Interception			Credential Dumping		Application Deployment Software	Execution through API			Custom Cryptographic Protocol
Accessibility Features		Trusted Developer Utilities	Brute Force	Network Service Scanning		PowerShell			Data Obfuscation
Port Monitors		Regsvcs/Regasm	Credentials in Files	Query Registry	Remote File Copy	Rundll32			Custom Command and Control Protocol
Screensaver	Exploitation of Vulnerability			Remote System Discovery	Taint Shared Content	Scripting			Connection Proxy
LSASS Driver	Extra Window Memory Injection			Permission Groups Discovery		Graphical User Interface			Uncommonly Used Port
Browser Extensions	Access Token Manipulation			Process Discovery		Command-Line Interface			Multiband Communication
Local Job Scheduling	Bypass User Account Control			System Service Discovery		Scheduled Task			Fallback Channels
Re-opened Applications	Process Injection					Windows Management Instrumentation			
Rc.common	SID-History Injection	Component Object Model Hijacking				Trusted Developer Utilities			
Login Item	Sudo	InstallUtil				Service Execution			
LC_LOAD_DYLIB Addition	Setuid and Setgid	Regsvr32							
Launch Agent		Code Signing							
Hidden Files and Directories		Modify Registry							
.bash_profile and .bashrc		Component Firmware							
Trap		Redundant Access							
Launchctl		File Deletion							
Office Application Startup		Timestomp							
Create Account		NTFS Extended Attributes							
External Remote Services		Process Hollowing							
Authentication Package		Disabling Security Tools							
Netsh Helper DLL		Rundll32							
Component Object Model Hijacking		DLL Side-Loading							
Redundant Access		Indicator Removal on Host							
Security Support Provider		Indicator Removal from Tools							
Windows Management Instrumentation Event Subscription		Indicator Blocking							
		Software Packing							
Registry Run Keys / Start Folder		Masquerading							
		Obfuscated Files or Information							
Change Default File Association		Binary Padding							
Component Firmware		Install Root Certificate							
Bootkit		Network Share Connection Removal							
Hypervisor		Rootkit							
Logon Scripts		Scripting							
Modify Existing Service									

https://attack.mitre.org

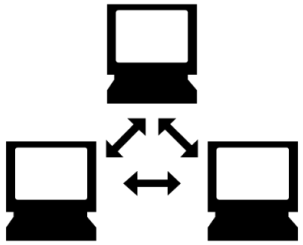
MITRE ATT&CK. Что проверять?

Endpoint Data

- ☑ Access Tokens
- ☑ Anti-virus
- ☑ API monitoring
- ☑ Application Logs
- ☑ Asset Management
- ☑ Authentication logs
- ☑ Binary file metadata
- ☑ BIOS
- ☑ Browser extensions
- ☑ Data loss prevention
- ☑ Detonation chamber
- ☑ Digital Certificate Logs
- ☑ DLL monitoring
- ☑ DNS records
- ☑ EFI
- ☑ Email gateway
- ☑ Environment variable
- ☑ File monitoring
- ☑ Host network interface
- ☑ Kernel drivers
- ☑ Loaded DLLs
- ☑ Mail server
- ☑ Malware reverse engineering
- ☑ MBR
- ☑ Named Pipes
- ☑ PowerShell logs
- ☑ Process command-line parameters
- ☑ Process monitoring
- ☑ Process use of network
- ☑ Sensor health and status
- ☑ Services
- ☑ SSL/TLS inspection
- ☑ System calls
- ☑ Third-party application logs
- ☑ User interface
- ☑ VBR
- ☑ Web application firewall logs
- ☑ Web logs
- ☑ Web proxy
- ☑ Windows Error Reporting
- ☑ Windows event logs
- ☑ Windows Registry
- ☑ WMI Objects

- ☑ Netflow/Enclave netflow
- ☑ Network device logs
- ☑ Network intrusion detection system
- ☑ Network protocol analysis
- ☑ Packet capture

Network Data



https://public.tableau.com/profile/cyb3rpanda#!/vizhome/MITREATTCKMatrixforEnterpriseV2/ATTCK

MITRE ATT&CK. Как проверять

BAS tools моделируют вредоносную активность (включая техники которые обходили бы текущую защиту) позволяя SOCам определять текущее состояние системы защиты

https://attackevals.mitre.org

Commercial

- AttackIQ
- Circumventive
- Cymulate
- Pcysys
- Picus
- SafeBreach
- ThreatCare
- Verodin
- XM Cyber
- SCYTHE

Open Source

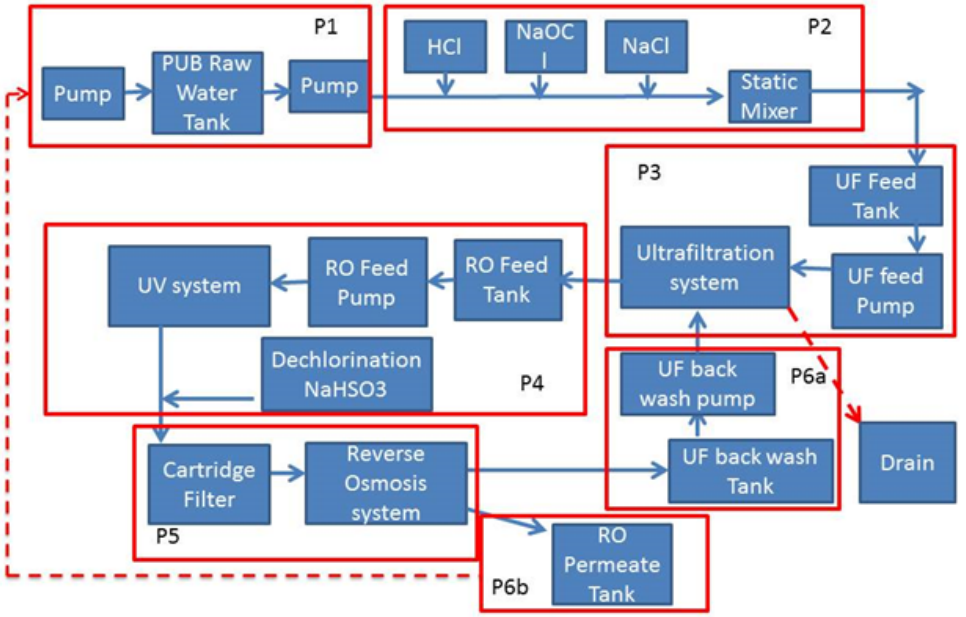
- Red Team Automation (RTA)
- Infection Monkey
- Network Flight Simulator
- Metta
- Atomic Red Team
- MITRE CALDERA
- APT Simulator

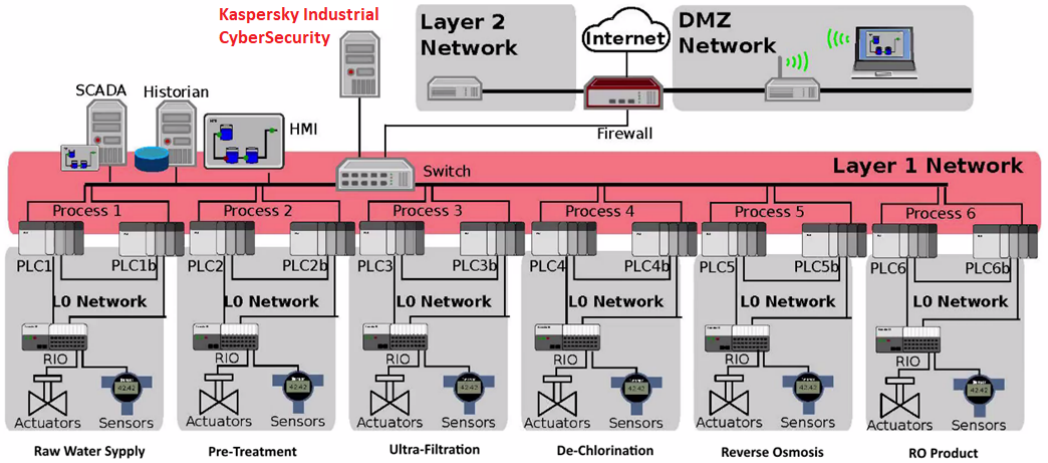
https://github.com/redhuntlabs/RedHunt-OS/
https://www.gartner.com/en/documents/3875421
https://blogs.gartner.com/augusto-barros/2018/04/17/threat-simulation-open-source-projects/

Промышленные полигоны/учения: **Kaspersky Industrial CTF**

https://ctf.kaspersky.com

Промышленные полигоны/учения: **SUTD,** Сингапур





6 stages:

- P1: RAW water Supply and storage
- P2: Pre-treatment
- P3: Ultrafiltration and backwash
- P4: De-Chlorination System
- P5: Reverse Osmosis (RO)
- P6: RO Permeate Transfer, UF Backwash and Cleaning

Full details on the testbed
https://itrust.sutd.edu.sg/testbeds/secure-water-treatment-swat/

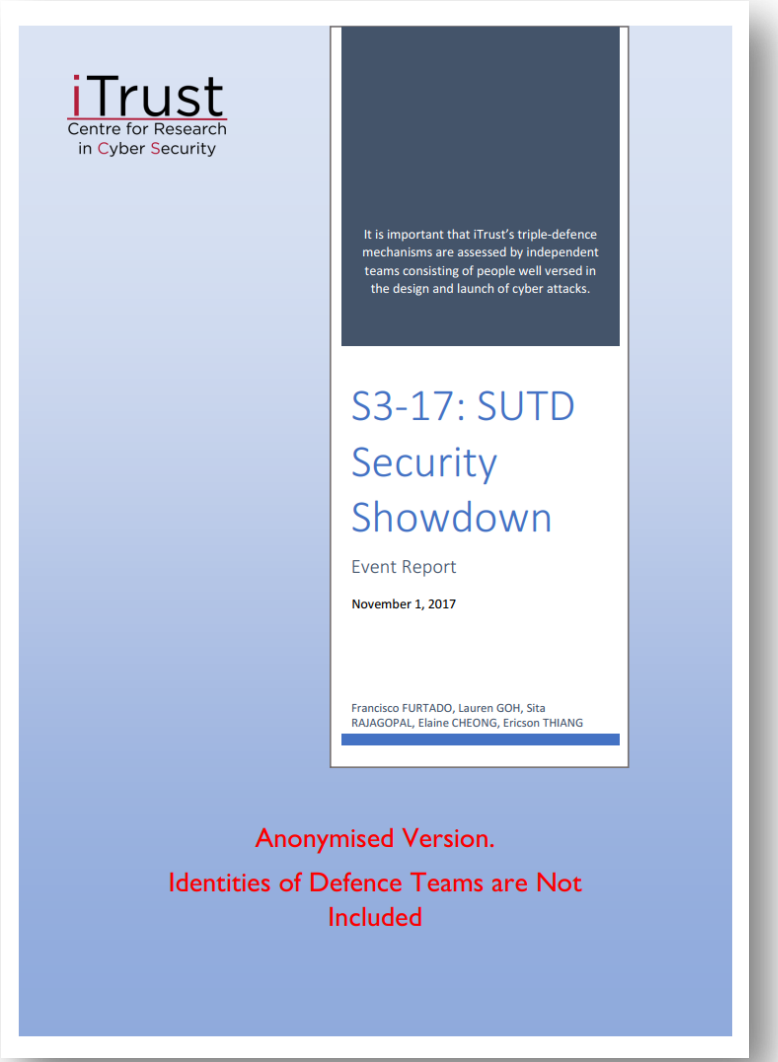
Промышленные полигоны/учения: **SUTD,** Сингапур**, 2017**

Cybercriminal Attacker Model

- Control of the PLC through the Bridged Man-in-the-Middle (MiTM) at Level 0
- Control of the chemical dosing system through a Python script (pycomm)
- Control of the Historian through the Aircrack WiFi
- Control of the pressure through the Server Message Block (SMB)
- Control of the water level in the tank through the Metasploit VNC Scanner
- Control of the pump through a rogue router
- Control of the pump through the FactoryTalk and password vulnerability
- Control of the pressure pump through Python script (pycomm)
- Control of the pump through the compromised HMI
- Overwriting data stored at Historian
- Control of the Historian through MiTM using ARP

Insider Attacker Model

- Control of the Motorised Valve through Manual Intervention
- Control of the RIO/Display through manual configuration on the sensor
- Control of the water pump P101 through the Python script (pycomm)
- Control of the water pump P101 through manual operation of the HMI
- Control of the pressure pump through Python script (pycomm)
- Control of the water tank level LIT101 through Python script (pycomm)
- Control of chemical dosing through modified PLC Logic
- Control of the RIO through disconnecting Analogue Input/Output pin
- Control of the amount of chemical dosing through Python script
- Control of the PLC through the modification of PLC logic in Studio 5000
- Control of the motorised valve through modification of PLC logic in Studio 5000
- Control of the motorised valve MV201 through the modification of PLC logic
- Control of the water tank level LIT301 through adjusting alarm levels
- Control of the chemical dosing pump P205 through manual operation of the dosing meter
- Control of the HMI/SCADA through simulation control
- Control of the PLC through disconnected network cables



Details: https://goo.gl/y1Pxre

Промышленные полигоны/учения: **SUTD,** Сингапур**, 2019**

2:23 - Scanning both Zycron and SWaT network concurrently.
2:30 - Discovered the VNC service.
2:38 - Attack: Attempting to do MITM attack on PLC1
2:50 - Attack: Attempting to do Layer 0 MITM attack on LIT101.
2:23 - Scanning both Zycron and SWaT network concurrently.
2:30 - Discovered the VNC service.
2:38 - Attack: Attempting to do MITM attack on PLC1 Attempt to do bridge in primary plc to RIO
2:50 - Attack: Attempting to do Layer 0 MITM attack on LIT101. Spoof water level to 390
2:54 - Attack Successful! 2:59 - Attack: Download modified P2 PLC code.
3:01 - Attack Unsuccessful! 3:18 - Attack: Downloading modified P2 PLC code. Attack Unsuccessful!
3:19 - Attack: Trying to breach the firewall.
3:22 - Attack: Overwriting PLC code. Attack Unsuccessful!
3:38 - Attack: Attempting to set LIT101 to 300. Attack Unsuccessful!
4:16 - Spoofing attack LIT101 at HMI Successful!
4:45 - Download of PLC code failed!
5:07 - Launch on DPIT pressure successful!
5:18 - Attempt to change plant to manual mode.
5:19 - Attempt successful!
5:20 - Attempt to stop plant process.
5:23 - Attempt to stop/start plant successful!
5:28 - Attack : Attempt to do DoS attack on historian for all values. Attack unsuccessful!
5:36 - Attack : Attempt to do DoS attack on historian for all values. Attack unsuccessful!
6:18 - Attack: Attempt to do DoS attack on historian for all values. Attack unsuccessful!
6:20 - Eternal Blue attack: Time Out!

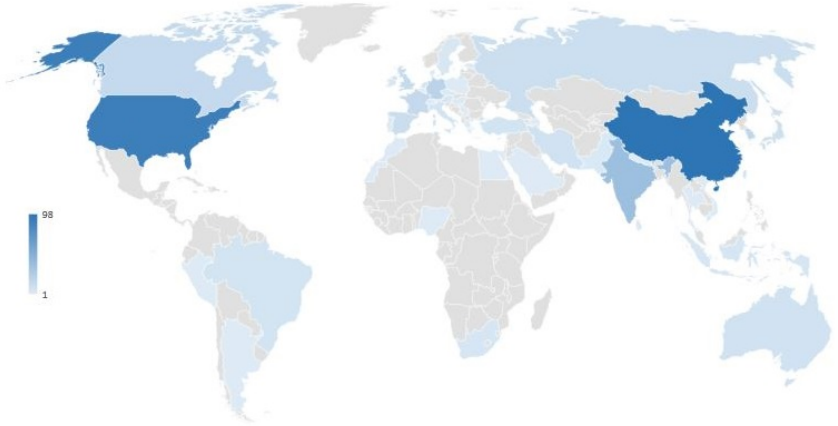
https://itrust.sutd.edu.sg/ciss-2019/

Промышленные полигоны/учения: **SUTD,** Сингапур

https://itrust.sutd.edu.sg/research/dataset/

- Secure Water Treatment (SWaT)
- SWaT Security Showdown (S317)
- Water Distribution (WADI)
- BATtle of Attack Detection Algorithms (BATADAL)
- Electric Power and Intelligent Control (EPIC)
- Blaq_0

Overview of dataset requests by country (left) and year (right)

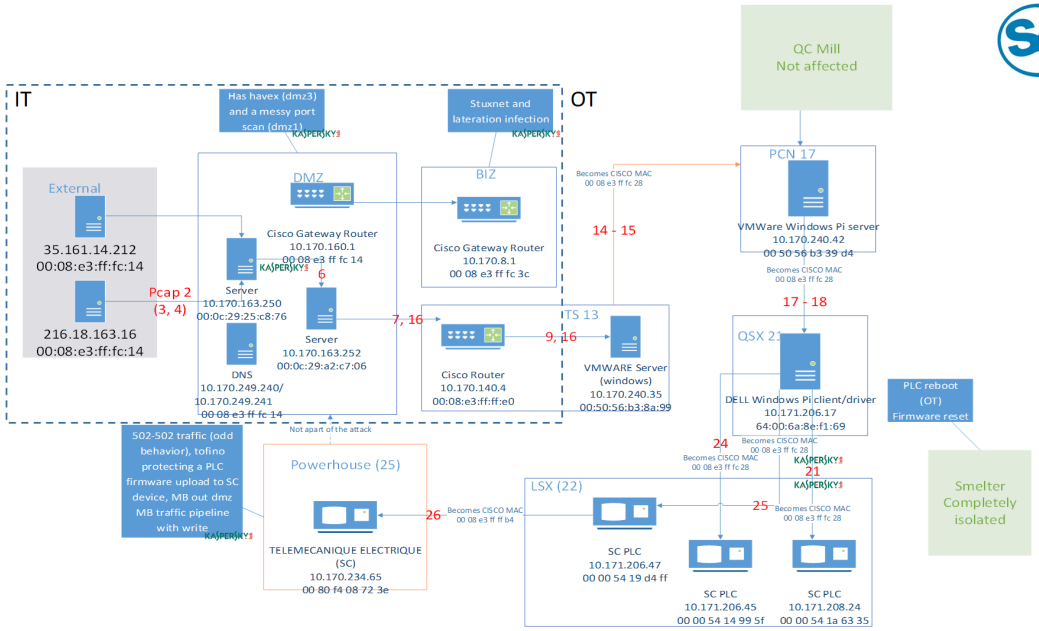


Исследователи из России

- Institute of Control Sciences
- Moscow Institute of Physics and Technology
- National Research University
- Saint Petersburg State University
- Peter the Great St. Petersburg Polytechnic University
- South Ural State University
- Innopolis University
- **Kaspersky Lab**

Промышленные полигоны/учения: **S4x19 ICS Detection Challenge**

- WMI Lateral Movement
- Reconnaissance / Network Scan
- Reconnaissance / Reading Project from PLC / Modbus
- Reconnaissance / Modbus Scan
- Transfer Malicious Firmware to Rockwell Automation PLC
- Modbus Write Attempt from an Internet address
- “Stuxnet” Malware Network Activity
- “Havex” Malware Network Activity
- “Greyenergy” Malware Network Activity



https://www.youtube.com/watch?v=A2tQo4t4ibo

https://www.youtube.com/watch?v=vSd8hoRqnF4&list=PLPmbqO785Hlt3yFvW-EZhvRq53EcCjmZc

Реальные инциденты, **Industroyer**

The 2016 Ukraine attack occurred at the transmission-level with an attack against a regional SCADA system generally focused on a single 330 kV-to-110 kV-to-10 kV substation, resulting in a distribution-level outage.

	2015	2016
Substations	50+	1
Customers	225K	Portion of Capital region
MW Impact	135 MW	200 MW

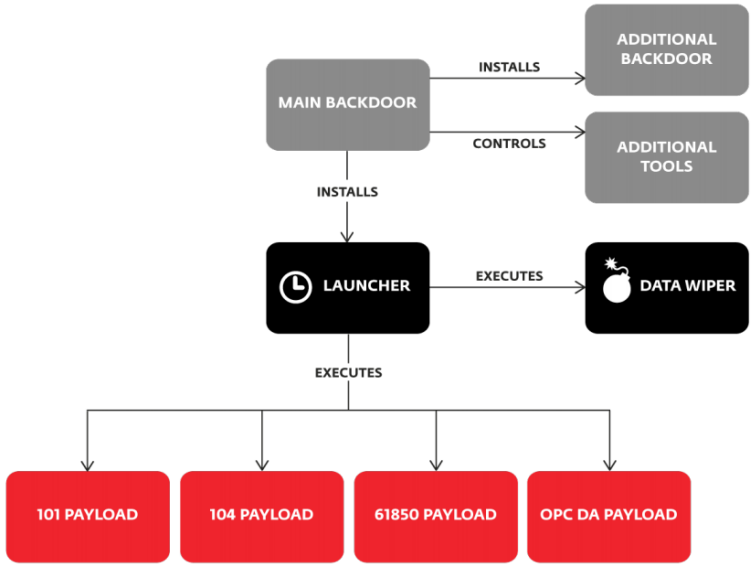


Figure 1. Simplified schematic of Win32/Industroyer components.

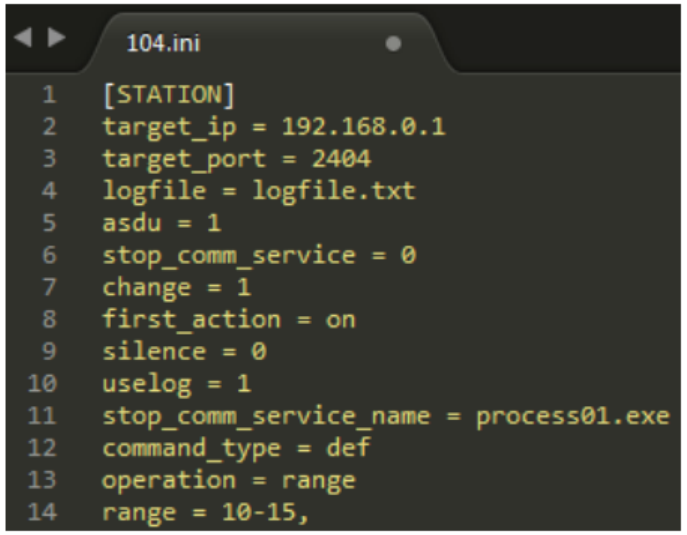
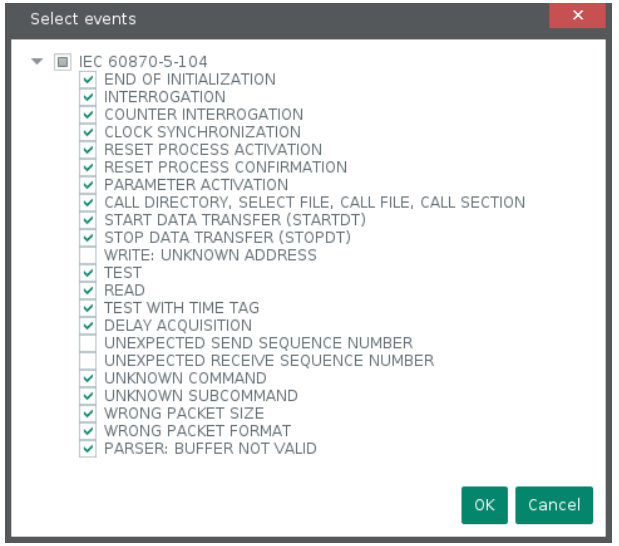


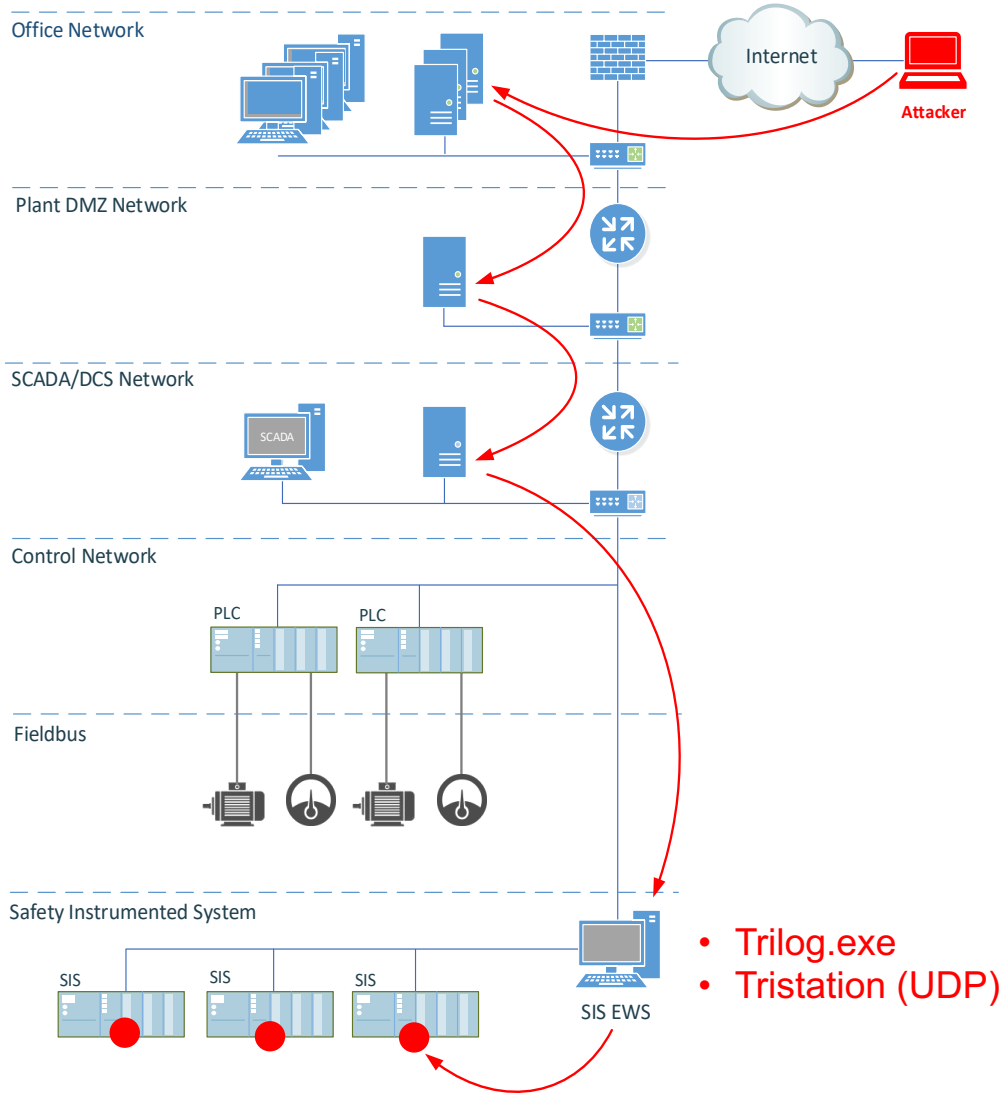
Figure 8. An example of 104 payload DLL configuration.



KICS 60870-5-104 Protocol Events

https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Реальные инциденты, **Triton**



Endpoint activities at different levels and stages

Powershell, Python
SSH clients (Putty/Plinks)
Netcat/Cryptocat
Mmikatz, PsExec
AdExplorer, ShareEnum, PsGetSid
Nmap, iPerf
Trilog.exe

Network activities at different levels and stages

DNS
SSH
RDP
RPC/SMB (PsExec)
HTTP (Webshell)
TCP/UDP (Nmap, iPerf)
VPN
Tristation (UDP)

Реальные инциденты, **Triton**

TRISIS / TRITON / HatMan Malware Repository

Description

This repository contains original samples and decompiled sources of malware attacking commonly used in Industrial Control Systems (ICS) *Triconex* Safety Instrumented System (SIS) controllers. For more information scroll to "*Learn More*".

Each organization describing this malware in reports used a different name (TRISIS/TRITON/HatMan). For that reason, there is no one, common name for it.

https://github.com/MDudek-ICS/TRISIS-TRITON-HATMAN

Practical Guides. NISTIR. Behavioral Anomaly Detection

- plaintext passwords
- user authentication failures
- new network devices
- abnormal network traffic between devices
- internet connectivity
- data exfiltration
- unauthorized software installations
- PLC firmware modifications
- unauthorized PLC logic modifications
- file transfers between devices
- abnormal ICS protocol communications
- malware
- denial of service (DoS)
- abnormal manufacturing system operations
- port scans/probes
- environmental changes


NISTIR 8219

Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection

James McCarthy
Michael Powell
Keith Stouffer
CheeYee Tang
Timothy Zimmerman
William Barker
Titilayo Ogunyale
Devin Wynne
Johnathan Wiltberger

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

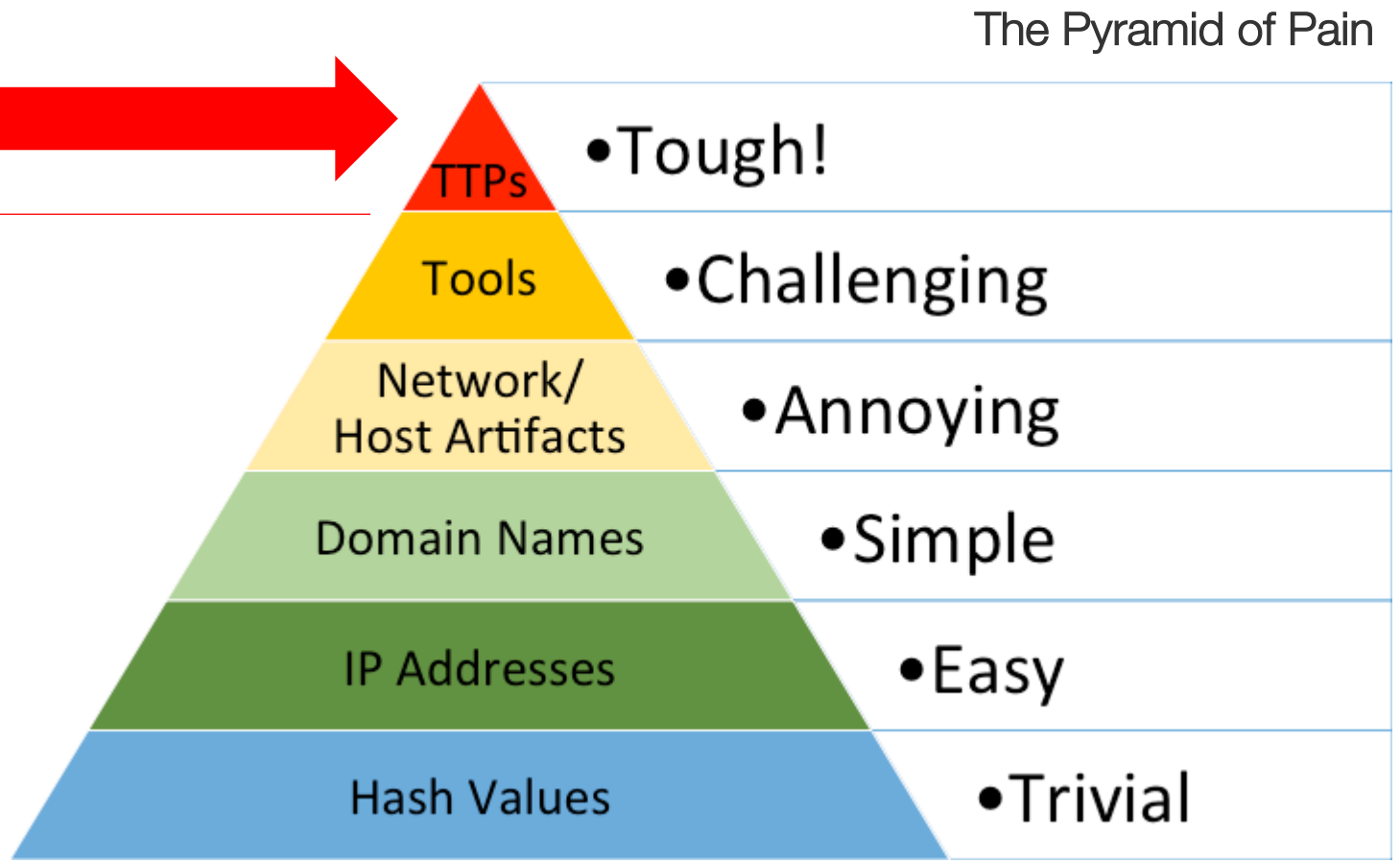
NISTIR 8219

https://csrc.nist.gov/publications/detail/nistir/8219/draft

Эффективный **Threat Intelligence**

Сценарии Атак
и детекты для них

Частные атрибуты



https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Источники сценариев/техник атак

Intrusion Datasets/PCAPs

Techniques frameworks

- MITRE ATT&CK Enterprise
- MITRE ATT&CK ICS (in progress)
- CAT/CAFFEINE (in progress)

Промышленные полигоны/учения

- iTrust CISS, Singapore
- Kaspersky Industrial CTF
- The Standoff
- S4 ICS Detection Challenge
- Locked Shields

Реальные инциденты

- Industroyer
- Stuxnet
- Triton

Research papers

- arXiv.org
- GitHub/GitLab
- IEEE Xplore Library
- ScienceDirect
- ResearchGate
- ScienceOpen
- Google Scholar
- CREDC

Safety Studies / CCE

- PHA/HAZOP
- Accidents reports
- Safety/Hazard/Failure analysis

Practical Guides

- NISTIR 8219. BAD
- …

kaspersky

Спасибо!

Антон Шипулин

CISSP, CEH, CSSA

Менеджер по развитию решений по безопасности критической инфраструктуры

Kaspersky HQ

39A/3 Leningradskoe Shosse, Moscow

T: +7 (495) 797 8700 #1746

Anton.Shipulin@kaspersky.com

@shipulin_anton

ics.kaspersky.com