



Energy Information and Analyzis Center in Hungary

www.e-isac.hu

Szabolcs Hallai

CISA, CISM, C|CISO, CITRM

Hungarian Energy and Public Utility Regulatory Agency

Agenda

- ISAC basics
- Chain of trust
- Architectural planning of e-isac.hu
- Implementation of e-isac.hu
- First impressions
- Expectations

10. PIES

24th of November 2017.



ISAC basics

- **Information Sharing and Analysis Center or (ISAC)** is a [nonprofit organization](#) that provides a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sector.

Information Sharing & Analysis Tools

Threat Data, Information Sharing

- ⊙ **Anonymous Submissions**
- ⊙ **CyberIntel Listserver**
- ⊙ Relevant/Actionable Cyber & Physical Alerts (Portal)
- ⊙ **Special Interest Group Email Listservers**
- ⊙ Document Repository
- ⊙ Member Contact Directory
- ⊙ Member Surveys
- ⊙ Risk Mitigation Toolkit
- ⊙ Threat Viewpoints

Ongoing Engagement

- ⊙ Bi-weekly Threat Calls
- ⊙ Emergency Member Calls
- ⊙ Semi-Annual Member Meetings and Conferences
- ⊙ Regional Outreach Program
- ⊙ Bi-Weekly Educational Webinars

Readiness Exercises

- ⊙ Government Sponsored Exercises
- ⊙ **Cyber Attack against Payment Processes (CAPP) Exercise**
- ⊙ Advanced Threat/DDoS Exercise
- ⊙ Industry exercises-Systemic Threat, Quantum Dawn Two, etc.

Chain of trust



Architectural planning of e-isac.hu

➤ Strategic plan

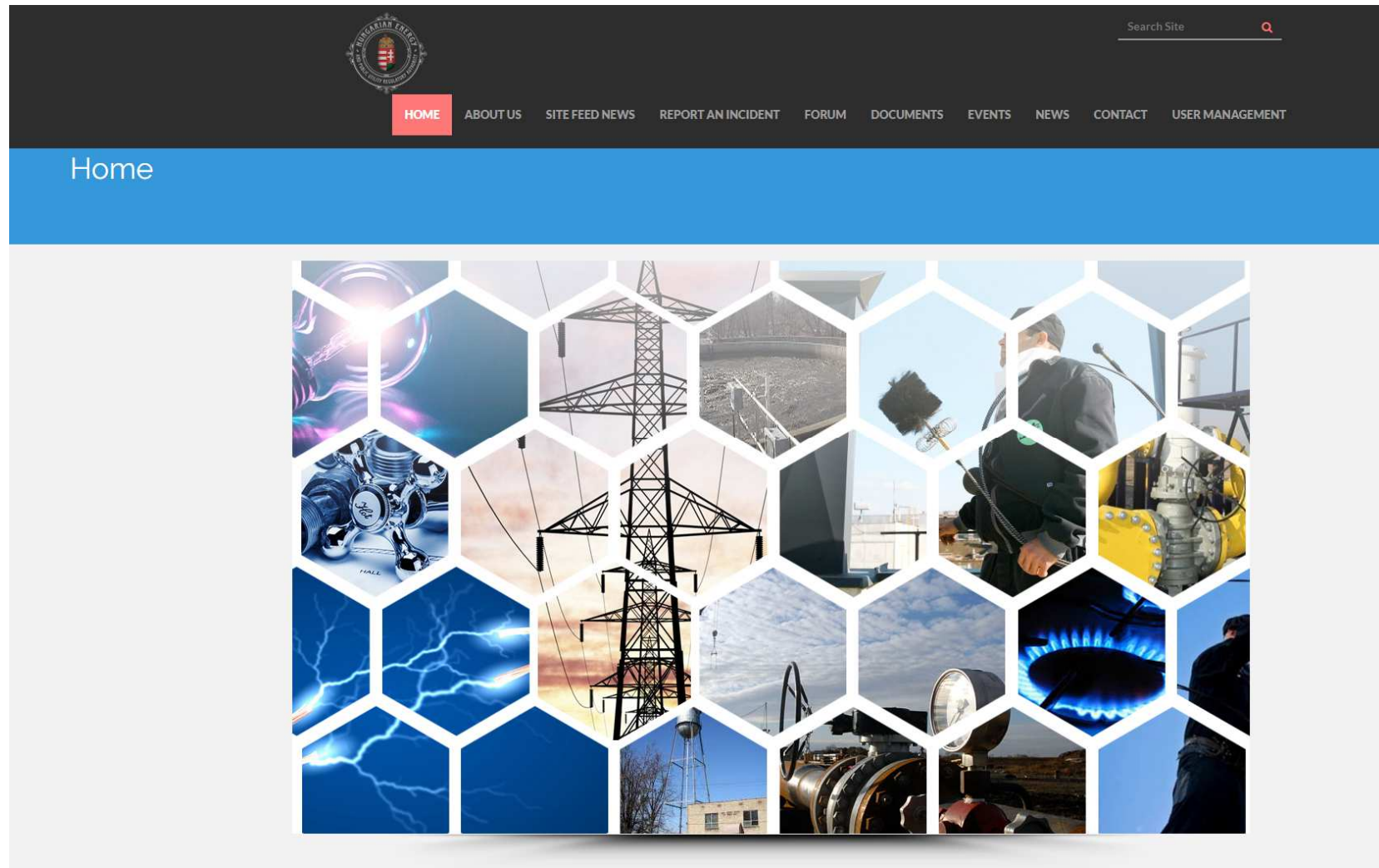
- ✓ ISAC independent from HEA infrastructure
- ✓ Highest security is to be implemented
- ✓ Reporting anonymity
- ✓ Forums
- ✓ Storage of several 1000s of documents
- ✓ CERT and other free Threat Report de-duplicated input (copy to fw)
- ✓ Threat statistics (World, Europe, Hungary)
- ✓ Hand made Vulnerability Report




- Private developer chosen (Black Cell Ltd.)
- 10 month long development cycle




Implementation of e-isac.hu



Implementation of e-isac.hu (documents)



Search Site 

HOMEABOUT USSITE FEED NEWSREPORT AN INCIDENTFORUMDOCUMENTSEVENTSNEWSCONTACTUSER MANAGEMENT

PUBLIC UTILITIES

CERT ALERTS

MCAFFEE THREAT REPORTS

MICROSOFT SECURITY BULLETIN SUMMARIES

SYMANTEC REPORTS

REGULATIONS AND OTHER RELATED DOCUMENTS


CISCO REPORTS

FIREEYE REPORTS


IBM REPORTS

ELECTRIC POWER


GUEST

 [CIS Microsoft Windows 7 Workstation Benchmark](#)
— by [admin](#) — last modified Oct 01, 2017 07:21 PM


This document provides prescriptive guidance for establishing a secure configuration posture for Microsoft Windows 7.

 [CIS Microsoft Windows 8.1 Workstation Benchmark](#)
— by [admin](#) — last modified Oct 01, 2017 07:21 PM


This document provides prescriptive guidance for establishing a secure configuration posture for Microsoft Windows 8.1.

 [CIS Microsoft Windows 10 Enterprise Release 1511 Benchmark](#)
— by [admin](#) — last modified Oct 01, 2017 07:21 PM


This document provides prescriptive guidance for establishing a secure configuration posture for Microsoft Windows 10 Enterprise Release.

 [ArborNetworks_Additional-Insights-Shamoon2\(02-21-2017\).pdf](#)
— by [Németh Ákos](#) — last modified Oct 01, 2017 07:21 PM


Information about Shamoon 2 malware

 [Badcyber_Polish-banks-hacked-information-stolen-unknown-attackers\(02-03-2017\).pdf](#)
— by [Németh Ákos](#) — last modified Oct 01, 2017 07:22 PM

Information about hacking several Polish Banks

 [BAESystems_Lazarus-FalseFlag-Malware\(02-20-2017\).pdf](#)
— by [Németh Ákos](#) — last modified Oct 01, 2017 07:22 PM

Information about Lazarus FalseFlag Malware

 [BAESystems_Lazarus-Watering-hole-attacks\(02-12-2017\).pdf](#)
— by [Németh Ákos](#) — last modified Oct 01, 2017 07:22 PM

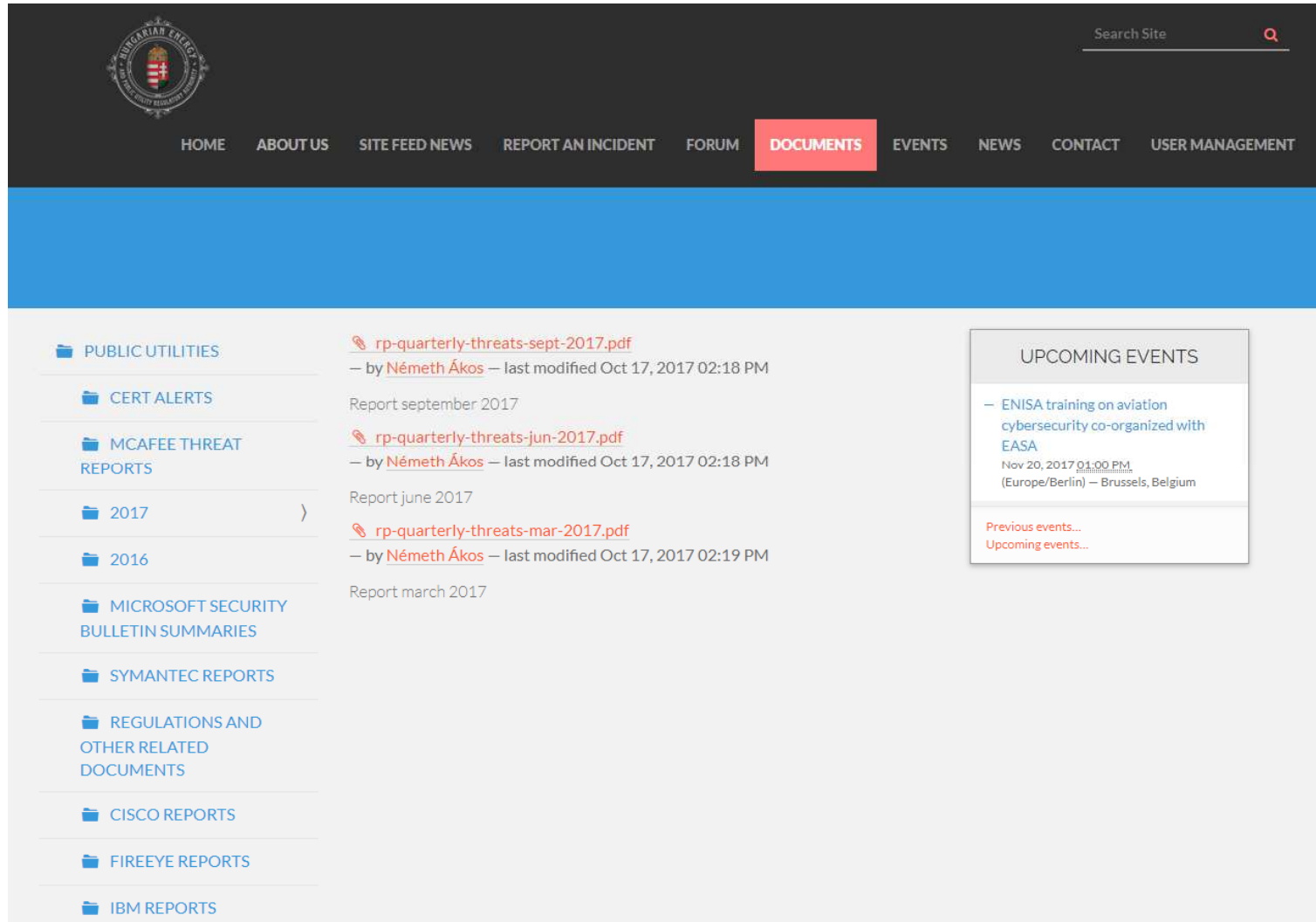
Information about a series of attacks directed at Polish financial institutions

UPCOMING EVENTS



— [ENISA training on aviation cybersecurity co-organized with EASA](#)
Nov 20, 2017 01:00 PM
(Europe/Berlin) — Brussels, Belgium

[Previous events...](#)
[Upcoming events...](#)


Implementation of e-isac.hu (threat reports)





The screenshot displays the e-isac.hu website interface. At the top, there is a dark navigation bar with the Hungarian Energy Regulatory Commission logo on the left and a search bar on the right. The main navigation menu includes links for HOME, ABOUT US, SITE FEED NEWS, REPORT AN INCIDENT, FORUM, DOCUMENTS (highlighted in red), EVENTS, NEWS, CONTACT, and USER MANAGEMENT. Below the navigation bar is a wide blue horizontal banner. The main content area is divided into three columns. The left column contains a sidebar with a list of document categories: PUBLIC UTILITIES, CERT ALERTS, MCAFFEE THREAT REPORTS, 2017 (selected), 2016, MICROSOFT SECURITY BULLETIN SUMMARIES, SYMANTEC REPORTS, REGULATIONS AND OTHER RELATED DOCUMENTS, CISCO REPORTS, FIREEYE REPORTS, and IBM REPORTS. The middle column displays three document entries, each with a red icon, a title, an author, and a modification date: 'rp-quarterly-threats-sept-2017.pdf' by Németh Ákos (Oct 17, 2017 02:18 PM), 'rp-quarterly-threats-jun-2017.pdf' by Németh Ákos (Oct 17, 2017 02:18 PM), and 'rp-quarterly-threats-mar-2017.pdf' by Németh Ákos (Oct 17, 2017 02:19 PM). The right column features a box titled 'UPCOMING EVENTS' which lists an event: 'ENISA training on aviation cybersecurity co-organized with EASA' on Nov 20, 2017 at 01:00 PM in Brussels, Belgium. It also includes links for 'Previous events...' and 'Upcoming events...'.


 Search Site 


HOME ABOUT US SITE FEED NEWS REPORT AN INCIDENT FORUM **DOCUMENTS** EVENTS NEWS CONTACT USER MANAGEMENT


 PUBLIC UTILITIES


 CERT ALERTS


 MCAFFEE THREAT REPORTS


 2017 >


 2016


 MICROSOFT SECURITY BULLETIN SUMMARIES


 SYMANTEC REPORTS


 REGULATIONS AND OTHER RELATED DOCUMENTS


 CISCO REPORTS

 FIREEYE REPORTS

 IBM REPORTS

 [rp-quarterly-threats-sept-2017.pdf](#)
— by [Németh Ákos](#) — last modified Oct 17, 2017 02:18 PM
Report september 2017

 [rp-quarterly-threats-jun-2017.pdf](#)
— by [Németh Ákos](#) — last modified Oct 17, 2017 02:18 PM
Report june 2017


 [rp-quarterly-threats-mar-2017.pdf](#)
— by [Németh Ákos](#) — last modified Oct 17, 2017 02:19 PM
Report march 2017


UPCOMING EVENTS

— ENISA training on aviation cybersecurity co-organized with EASA
Nov 20, 2017 01:00 PM
(Europe/Berlin) — Brussels, Belgium

[Previous events...](#)
[Upcoming events...](#)

Implementation of e-isac.hu (CERT alerts)



Search Site 

HOMEABOUT USSITE FEED NEWSREPORT AN INCIDENTFORUMDOCUMENTSEVENTSNEWSCONTACTUSER MANAGEMENT

PUBLIC UTILITIES

CERT ALERTS

2017

HUN

ENG

2016

2015

MCAFFEE THREAT REPORTS

MICROSOFT SECURITY BULLETIN SUMMARIES

SYMANTEC REPORTS


REGULATIONS AND OTHER RELATED DOCUMENTS

CISCO REPORTS


FIREEYE REPORTS

IBM REPORTS


CERT Alerts 2017 eng

 [ES-482_VMware vSphere Web Client_CH-14288_eng.pdf](#)
— by [Szilágyiszegi Zoltán](#) — last modified Nov 14, 2017 08:18 AM


VMware vSphere Web Client vulnerability

 [ES-481_VMware vCenter Server_CH-14287_eng.pdf](#)
— by [Szilágyiszegi Zoltán](#) — last modified Nov 14, 2017 08:16 AM


VMware vCenter Server vulnerability

 [ES-480_Symantec Endpoint Protection_CH-14286_eng.pdf](#)
— by [Szilágyiszegi Zoltán](#) — last modified Nov 14, 2017 08:18 AM


Symantec Endpoint Protection vulnerability

 [ES-479_Fortinet FortiOS_CH-14284_eng.pdf](#)
— by [Szilágyiszegi Zoltán](#) — last modified Nov 08, 2017 09:20 PM


Fortinet FortiOS vulnerability

 [ES-478_Siemens SIMATIC PCS 7_CH-14283_eng.pdf](#)
— by [Szilágyiszegi Zoltán](#) — last modified Nov 08, 2017 09:19 PM


Siemens SIMATIC PCS 7 vulnerability

 [ES-477_Red Hat Enterprise_CH-14282_eng.pdf](#)
— by [Szilágyiszegi Zoltán](#) — last modified Nov 08, 2017 09:18 PM

Red Hat Enterprise Virtualization vulnerability

 [ES-476_OpenSSL_CH-14281_eng.pdf](#)
— by [Szilágyiszegi Zoltán](#) — last modified Nov 08, 2017 09:17 PM

Open SSL vulnerability


 [ES-475_Cisco IOS XE_eng.pdf](#)
— by [Szilágyiszegi Zoltán](#) — last modified Nov 07, 2017 09:38 PM


UPCOMING EVENTS

— ENISA training on aviation cybersecurity co-organized with EASA
Nov 20, 2017 01:00 PM
(Europe/Berlin) — Brussels, Belgium

Previous events...
Upcoming events...

Implementation of e-isac.hu (incident reporting)





Search Site 


HOMEABOUT USSITE FEED NEWSREPORT AN INCIDENTFORUMDOCUMENTSEVENTSNEWSCONTACTUSER MANAGEMENT


Report an incident

Disclaimer: All incidents will be sent anonymously through this form.

Subject 

Comments 

INCIDENT 

☐ I'm not a robot

reCAPTCHA
Privacy - Terms

Submit

UPCOMING EVENTS

— ENISA training on aviation cybersecurity co-organized with EASA


Nov 20, 2017 01:00 PM
(Europe/Berlin) — Brussels, Belgium


Previous events...

Upcoming events...

The HUNGARIAN E-ISCAP® is © 2017-2017 Sponsored by MEKH, powered by the BlackCell Ltd.

Implementation of e-isac.hu (threat feed)



Search Site 


HOMEABOUT USSITE FEED NEWSREPORT AN INCIDENTFORUMDOCUMENTSEVENTSNEWSCONTACTUSER MANAGEMENT






Feed type



Hourly Feed

1,953,960

Hourly feed

Add a filter 

All Hungarian Mal ip 	Type 	Severity 	Date 	COUNT IPS 
ak.imgfarm.com	malware_distribution	high	May 8th 2017	7
195.184.191.147	malicious_ip	high	May 25th 2017	1
195.184.191.147	scanning	high	May 21st 2017	1
37.9.213.41	malicious_ip	high	November 17th 2017	1
37.9.213.41	scanning	high	September 19th 2017	1
79.172.208.97	malicious_ip	high	May 21st 2017	1
79.172.208.97	scanning	high	May 21st 2017	1
89.133.32.181	malicious_ip	high	May 2nd 2017	1
89.133.32.181	scanning	high	May 2nd 2017	1
com	malware_distribution	high	May 8th 2017	2

Exports: [Raw](#)  [Formatted](#) 

12345...51»

Implementation of e-isac.hu (vulnerability sheet)

Vulnerability datasheet	
Name vulnerability VMware vCenter Server	Severity Middle
Organisation GovCERT Hungary	Attack type Authentication
CERT ID CH-14287	Link http://tech.cert-hungary.hu/vulnerabilities/CH-14287
Release date 17. november 10.	ID ES-481
Summary A vulnerability in VMware vCenter Server could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.	
Description The vulnerability is due to improper handling of crafted LDAP packets by the affected software. An attacker could exploit this vulnerability by sending crafted LDAP packets to the targeted system. An exploit could cause the affected application on the system to crash or become unresponsive, resulting in a DoS condition.	
CVE reference: CVE-2017-4927	
Technical details	
Links https://tools.cisco.com/security/center/viewAlert.x?alertId=55877	
Affected systems VMware, Inc. vCenter Server 6.0 (Base, Update 1, Update 2, Update 2a, Update 3, Update 3a, Update 3b) 6.5 (.0, .0a, .0b, .0c, .0d, .0e)	
Solution VMware has confirmed the vulnerability and released software updates. https://my.vmware.com/web/vmware/details?downloadGroup=VC65U1&productId=614&rPId=17343 https://my.vmware.com/web/vmware/details?productId=491&downloadGroup=VC60U3	

Expectations

- If we manage to stop for the first year 1 attack
- Then the next year the double
- Then double again
- Then...



Questions?





Thank you for your kind attention!

Szabolcs Hallai

**CISA, CISM, C|CISO, CITRM
Hungarian Energy Agency - CISO
hallaisz@mekh.hu**