Cyber Defense and Situational Awareness Software Solutions Portfolio

Every day organizations are exposed to cyber attacks. Information security teams do their best, but it is very difficult to monitor the current situation, pinpoint leading indicators, respond to issues, and stay informed about latest attack vectors, methods and threats – and it is overwhelming to do all of this at the same time.



Automatic Event Correlation for Incident Detection



Continuously discover anomalies caused by advanced attacks and get informed about emerging issues in real time.



Cooperative Analysis Engine for SA and Incident Response



AUSTRIAN INSTITUTE

- ÆCID is built on AIT's patented solution for adaptive network log stream processing, which is inspired by approaches from the domain of bio informatics. This approach enables ÆCID to detect, classify and cluster frequently occurring patterns in log files and eventually distinguish the known good from unknown malicious activities specifically in your custom IT infrastructure – self-learning with minimal manual configuration effort.
- ÆCID relies on a central log store and verbose logging activated. It operates on top of raw logs and alerts findings seamlessly and directly to your existing SIEM solution via syslog connectors for further investigations. ÆCID is designed to complement your existing security solutions in place.

Friedberg I., Skopik F., Settanni G., Fiedler R. (2015): Combating Advanced Persistent Threats: From Network Event Correlation to Incident Detection. *Elsevier Computers & Security Journal*, Volume 48, pp. 35-57. Elsevier.

Skopik F., Fiedler R. (2013): A50292/2013 (AT 514.215) - Verfahren zur Feststellung von Abweichungen von einem vorgegebenen Normalzustand (Method to detect deviations from a given normal state), patent, April 2013

Figure 1 - Systemconce

Figure 1 - ÆCID Application Concept

- CÆSAIR continuously imports security feeds in standard formats, such as STIX, IODEF and CVE, into its sophisticated knowledge store and discovers relations between recent issue reports and knowledge artifacts, including vulnerabilities, emerging threats and previous incident reports. For a given issue report, it identifies relevant past events and documents and provides classification, thus assistis to to handle the issue.
- CÆSAIR is designed as a standalone Web-based help and support solution for security incident teams. With its multitude of importers, CÆSAIR can be connected to numerous different information sources, being internal or external ones from peers and partners, to establish situational awareness (SA), and enable the effective investigation and mitigation of incidents.
- Settanni G., Skopik F., Shovgenya Y., Fiedler R., et al. (2015): A Blueprint for a Pan-European Cyber Incident Analysis System. 3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015), September 17-18, 2015, Ingolstadt, Germany. BCS

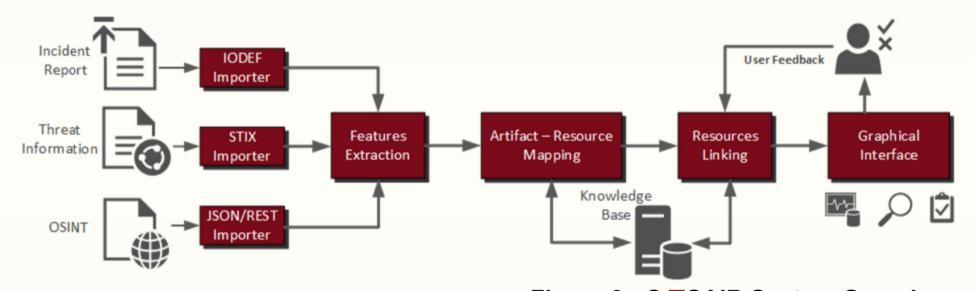
nd

Re

S

0

Skopik F., Wurzenberger M., Settanni G., Fiedler R. (2015): Establishing National Cyber Situational Awareness through Incident Information Clustering. International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2015), June 8-9, 2015, London, UK. C-MRIC.



Distributed Anomaly Detection Engine Perfor-IDS/IPS Firewall Application mance Logs Server Logs Logs Logs

Figure 2 - CÆSAIR System Overview

	Resources & Artifacts								
Incor	ning issues			Rela	ated r	esources			
Туре	Date	Summary	Actions	Туре	Score	Date	Summary		Action
cve	16.07.2015 08:45	Unspecified vulnerability in the Oracle Applications Framework component in Oracle E- Business Suite 12.2.4 allows remote authenticated users to affect integrity via unknown vectors related to Dialog popup.	۹.1	cve	350	09.09.2015 08:12	and R2 allow	tory in Microsoft Windows Server 2008 SP2 and R2 SP1 and Server 2012 Gold ws remote authenticated users to cause a denial of service (service outage) by titple machine accounts, aka "Active Directory Denial of Service Vulnerability."	+.' © •
cve	20.07.2015 05:07	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45, and Java SE Embedded 7u75 and 8u33 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries, a different vulnerability than CVE-2015-2590.	۹.1	cve	350	24.03.2015 03:01	and R2 SP1 configured,	IGON service in Microsoft Windows Server 2003 SP2, Windows Server 2008 SP2 , and Windows Server 2012 Gold and R2, when a Domain Controller is allows remote attackers to spoof the computer name of a secure channel's of bable secure channels and the secure channels and the secure channel's	+.0
cve	16.07.2015 08:41	Unspecified vulnerability in the Oracle Sourcing component in Oracle E-Business Suite 12.1.1, 12.1.2, 12.1.3, 12.2.3, and 12.2.4 allows remote authenticated users to affect confidentiality via unknown vectors related to Bid/Quote creation.	۹.1	Det	leveraging the ability to sniff network traffic, aka "NETLOGON Spoofing Vulnerability."				
cve	18.07.2015 12:09	Unspecified vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager component in Oracle Commerce Platform 3.1.1, 3.1.2, 11.0, and 11.1 allows remote attackers to affect confidentiality and integrity via unknown vectors related to Content Acquisition System.	۹./	Res	Vetails for resource: AVDuqm_6kCSfqDJI9CSy tesource ID in Index: AVDuqm_6kCSfqDJI9CSy ast modified date: 09.09 2015 08.12				
cve	16.07.2015 05:36	Unspecified vulnerability in the Application Express component in Oracle Database Server before 5.0 allows remote authenticated users to affect availability via unknown vectors.	۹,4		s: Windo mmai	ws Server Active	Directory Dos	Edit tags	
cve	40.07.0045.07.44					· j			
	16.07.2015 07:44	Unspecified vulnerability in the Data Store component in Oracle Berkeley DB 11.2.5.1.29, 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability of vulnerability of vulnerability integrability integrability of vulnerability.						008 SP2 and R2 SP1 and Server 2012 Gold and R2 allows remote authenticated u: eating multiple machine accounts, aka "Active Directory Denial of Service Vulnerab	
	16.07.2015 07.44	11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2624, CVE- 2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE-	۹.*	caus					
	16.07.2015 07.44	11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2624, CVE- 2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE- 2015-4754, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE- 2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-	٩.4	caus	e a denia ribute			reating multiple machine accounts, aka "Active Directory Denial of Service Vulnerab	
	16.07.2015 07.44	11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2624, CVE- 2015-2626, CVE-2015-4640, CVE-2015-4656, CVE-2015-4656, CVE-2015-4754, CVE- 2015-4764, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE-	۹.4	Att	e a denia ribute			reating multiple machine accounts, aka "Active Directory Denial of Service Vuherab Value cve cVC-2015-2535	
cve	16.07.2015 06:17	11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2624, CVE- 2015-2626, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4754, CVE- 2015-4754, CVE-2015-4775, CVE-2015-4776, CVE-2015-4777, CVE-2015-4778, CVE- 2015-4780, CVE-2015-4781, CVE-2015-4782, CVE-2015-4783, CVE-2015-4784, CVE-	_	Att	e a denia ribute pe rnal_id	al of service (servic	e outage) by cr	reating multiple machine accounts, aka "Active Directory Denial of Service Vuherab Value cve	
cve		11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2624, CVE- 2015-2626, CVE-2015-2640, CVE-2015-2656, CVE-2015-2656, CVE-2015-4754, CVE- 2015-4764, CVE-2015-4776, CVE-2015-4776, CVE-2015-4778, CVE-2015-4778, CVE- 2015-4780, CVE-2015-47761, CVE-2015-4776, CVE-2015-4783, CVE-2015-47784, CVE- 2015-4785, CVE-2015-4786, CVE-2015-4787, CVE-2015-4788, and CVE-2015-4789. Unspecified vulnerability in the Oracle Data Integrator component in Oracle Fusion	۹.» ۹.»	Att _tyl inte _so _so	e a denia ribute be rnal_id urce.vuln operator	al of service (servic	e outage) by cr	reating multiple machine accounts, aka "Active Directory Denial of Service Vuherab Value cve cVC-2015-2535	
cve		11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2624, CVE-2015-264, CVE-2015-2654, CVE-2015-2656, CVE-2015-4756, CVE-2015-4758, CVE-2015-4756, CVE-2015-4756, CVE-2015-4756, CVE-2015-4758, CVE-2015-4758, CVE-2015-4758, CVE-2015-4758, CVE-2015-4758, CVE-2015-4758, CVE-2015-4756, CVE-2015-4758, CVE-2015-4759, CVE-2015-4758, CVE-2015-4758, CVE-2015-4758, CVE-2015-4758, CVE-2015-4758, CVE-2015-2638, CVE-2015-2638, CVE-2015-4758, and CVE-2015-4759, CVE-2015-2638, CVE-2015-2638, CVE-2015-4758, and CVE-2015-4758, CVE-2015-2638, CVE-2015-2638, CVE-2015-4758, and CVE-2015-4758, CVE-20	_	Ltyl	e a denia ribute De rnal_id urce.vuln .operator urce.vuln .negate	of service (service) erable-configuration erable-configuration erable-configuration	e outage) by cri on.logical- on.logical-	eating multiple machine accounts, aka "Active Directory Denial of Service Vuherab Value cve CVC-2015-2535 OR	
	16.07.2015.06:17	 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2624, CVE-2015-2640, CVE-2015-2654, CVE-2015-2656, CVE-2015-4756, CVE-2015-4750, CVE-2015-4760, CVE-2015-2636, CVE-2015-4760, and CVE-2015-4760. 	_	Att _tvi _tvi _sc _sc _sc _sc _sc _scs _scsscssc	e a denia ribute De rnal_id urce.vuln .operator urce.vuln .negate urce.vuln .fact-ref.r	i of service (servic erable-configuratic erable-configuratic erable-configuratic ame erable-configuratic	e outage) by cri on logical- on logical- on logical-	eating multiple machine accounts, aka "Active Directory Denial of Service Vuherab Value cve CVC-2015-2535 OR false	
cve	16.07.2015 06:17 15.07.2015 05:23	 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2624, CVE-2015-400, CVE-2015-400, CVE-2015-4766, CVE-2015-4766, CVE-2015-4768, CVE-2015-2015, CVE-2015-2015, CVE-2015-2015, CVE-2015-2015, CVE-2015-2015, CVE-2015-2015, CVE-2015-4768, and CVE-2015-4759. win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Sits SP2, Windows Server 2005 SP2 and R2 SP1, Windows R1, Windows R, Windows R,	Q.2	Att _tyl nte _sc tesi _sc tesi _sc tesi _sc tesi _sc tesi _sc tesi _sc tesi _sc tesi	e a denia ribute be mal_id urce.vuln .operator urce.vuln .fact-ref.r urce.vuln .fact-ref.r	i of service (servic erable-configuratic erable-configuratic name erable-configuratic name erable-configuratic name	e outage) by cri on logical- on logical- on logical- on logical-	eating multiple machine accounts, aka "Active Directory Denial of Service Vuherab Value cve cvC-2015-2535 OR false cpe/o.microsoft.windows_server_2008 (2:sp1	
	16.07.2015.06:17	 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-2624, CVE-2015-400, CVE-2015-2634, CVE-2015-2656, CVE-2015-4756, CVE-2015-4758, CVE-2015-2635, CVE-2015-2636, CVE-2015-0448, CVE-2015-0458, CVE-2015-2635, CVE-2015-2636, CVE-2015-0448, CVE-2015-4759, win32k sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Sista SP2, Windows Server 2015 SP2, Windows Server 2015 SP2, Windows Sista SP2, Windows Server 2015 SP2, Windows Sista SP2, Windows Sista SP2, Windows Server 2015 SP2, Windows Sista SP2, Windows Sista SP2, Windows Sista SP2, Windows Sista SP3, Windows Sista SP3, Windows Sista SP3, Windows Sista SP4, Wi	Q.2	Att 	e a denia ribute pe rnal_id urce.vuln .negate urce.vuln .fact-ref.r urce.vuln .fact-ref.r	i of service (servic erable-configuratic erable-configuratic ame erable-configuratic name erable-configuratic name erable-configuratic name	e outage) by cr in logical- in logical- in logical- in logical- in logical-	eating multiple machine accounts, aka "Active Directory Denial of Service Vulnerab Value cve cVC-2015-2535 OR false cpe/o:microsoft:windows_server_2008 j2:sp1 cpe/o:microsoft:windows_server_2008:sp2	
cve	16.07.2015 06:17 15.07.2015 05:23	 11.2.5.2.42, 11.2.5.3.28, and 12.1.6.0.35 allows local users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-4264, CVE-2015-4264, CVE-2015-4264, CVE-2015-4766, CVE-2015-4766, CVE-2015-4766, CVE-2015-4776, CVE-2015-2015, CVE-2015, CVE-2	a	Att VVI VVI scs}	e a denia ribute be rnal_id urce.vuln .operator urce.vuln .fact-ref.r urce.vuln .fact-ref.r urce.vuln .fact-ref.r	erable-configuration erable-configuration erable-configuration erable-configuration erable-configuration erable-configuration erable-configuration erable-configuration erable-configuration erable-configuration erable-configuration	e outage) by on on logical- on logical- on logical- on logical- on logical- on logical- on logical-	eating multiple machine accounts, aka "Active Directory Denial of Service Yuherab Value cve cVC-2015-2505 OR false cpe/o.microsoft.windows_server_2008.ip2 cpe/o.microsoft.windows_server_2008.isp2 cpe/o.microsoft.windows_server_2012	

Figure 3 - CÆSAIR Dashboard



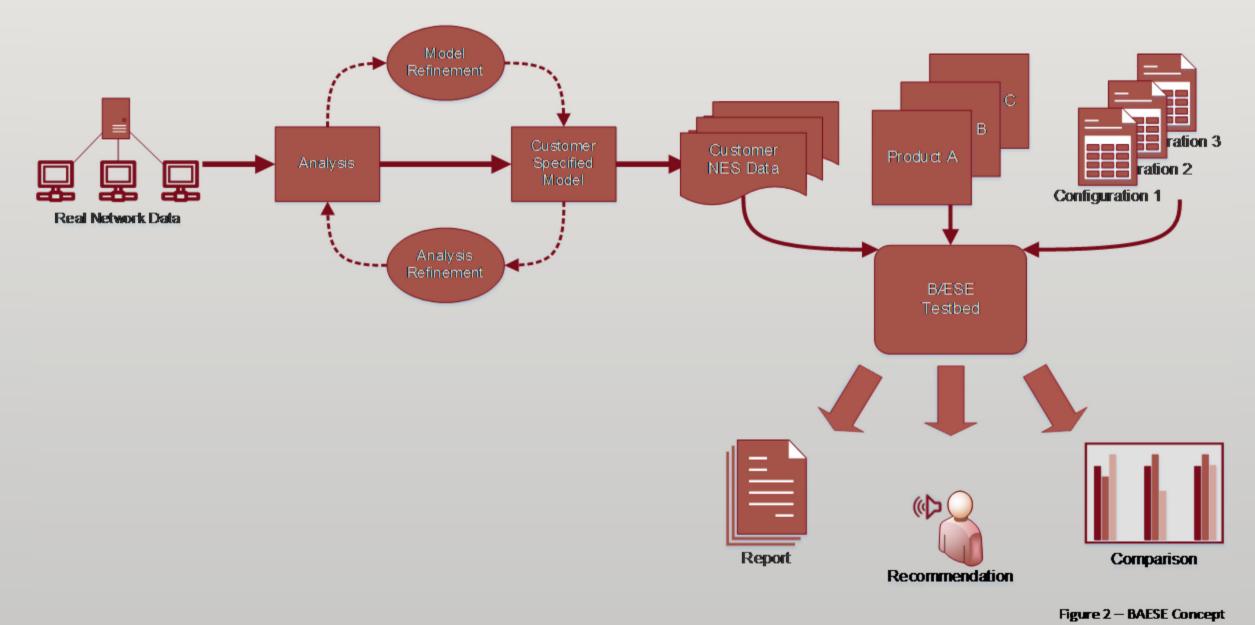
d Aler.

Fullye and Prep?

Discove

Benchmarking and Analytic Evaluation of IDSs in Specified Environments

- Challenge your IDS with newest attack vectors, tune its configuration and periodically (\mathbf{i}) verify its effectiveness.
- BÆSE takes short snippets of your central log store to create an event-based behavior model of your infrastructure. With this model it can create synthetic stimuli to challenge state-of-the-art security solutions in a realistic and customer-specific way. The output of this action is used to fine-tune configurations and thus increase



detection capabilities with respect to newest attack vectors and at the same time decrease false positive rates.

BÆSE enables you to verify the detection capabilities of your network log-based IDS and SIEM solution and tune their configurations offline without negative side effects on your monitored ICT infrastructure - however, still shaped to your specific environment. It requires access to a central log store to understand how the monitored infrastructure works and to create realistic stimuli to the challenged IDS or SIEM.



Wurzenberger M., Skopik F., Settanni G., Fiedler R. (2015): Beyond Gut Instincts: Understanding, Rating and Comparing Self-Learning IDSs Int'I Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2015), June 8-9, 2015, London, UK. C-MRIC.

Skopik F., Settanni G., Fiedler R., Friedberg I. (2014): Semi-Synthetic Data Set Generation for Security Software Evaluation. 12th International Conference on Privacy, Security and Trust, July 23-14, 2014, Toronto, Canada. IEEE.

Figure 4 - BÆSE System Overview

For further questions, please contact:

Florian Skopik, florian.skopik@ait.ac.at, www.ait.ac.at/ict-security AIT Austrian Institute of Technology GmbH, Digital Safety and Security Department, Austria. Solutions make use of:

