WAZUH

OSSEC Ruleset			
Rule	**Description**	**Source**	**Updated by Wazuh**
amazon_rules	Amazon main rules.	Created by Wazuh	✔
amazon-ec2_rules	Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define.	Created by Wazuh	✔
amazon-iam_rules	AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources for your users. You use IAM to control who can use your AWS resources (authentication) and what resources they can use and in what ways (authorization).	Created by Wazuh	✔
apache_rules	Apache is the world's most used web server software.	Out of the box	✔
apparmor_rules	AppArmor is a Linux kernel security module that allows the system administrator to restrict programs's capabilities with per-program profiles.	Out of the box	✔
arpwatch_rules	ARPWatch is a computer software tool for monitoring Address Resolution Protocol traffic on a computer network.	Out of the box	✔
asterisk_rules	Asterisk is a software implementation of a telephone private branch exchange (PBX).	Out of the box	✔
attack_rules	Signatures of different attacks detected by OSSEC	Created by Wazuh	✔
auditd_rules	The Linux Audit system provides a way to track security-relevant information on your system. Based on pre-configured rules, Audit generates log entries to record as much information about the events that are happening on your system as possible.	Created by Wazuh	✔
cimserver_rules	Compaq Insight Manager Server	Out of the box	✔
cisco-estreamer_rules	The FireSIGHT System Event Streamer (eStreamer) uses a message-oriented protocol to stream events and host profile information to the client application.	Created by Wazuh	✔
cisco-ios_rules	Cisco IOS is a software used on most Cisco Systems routers and current Cisco network switches.	Out of the box	✔
clam_av_rules	Clam AntiVirus (ClamAV) is a free and open-source, cross-platform antivirus software tool-kit able to detect many types of malicious software.	Out of the box	✔
courier_rules	IMAP/POP3 server	Out of the box	✔
docker_rules	Docker is an open-source project that automates the deployment of applications inside software containers.	Created by Wazuh	✔
dovecot_rules	Dovecot is an open-source IMAP and POP3 server for Linux/UNIX-like systems, written primarily with security in mind.	Out of the box	✔
dropbear_rules	Dropbear is a software package that provides a Secure Shell-compatible server and client. It is designed as a replacement for standard OpenSSH for environments with low memory and processor resources, such as embedded systems.	Out of the box	✔
firewall_rules	FirewallD provides a dynamically managed firewall with support for network/firewall zones to define the trust level of network connections or interfaces. Default firewall management tool RHEL and Fedora.	Out of the box	✔
firewalld_rules	Firewall events detected by OSSEC	Out of the box	✔
fortigate_rules	Fortigate (Fortinet) firewalls.	Created by Wazuh	✔
freeipa_rules	Open source project for identity management.	Created by Wazuh	✔
ftpd_rules	Simple FTP server.	Out of the box	✔
hordeimp_rules	IMP is the Internet Messaging Program and provides webmail access to IMAP and POP3 accounts.	Created by Wazuh	✔
hp_rules	HP Switch rules	Created by Wazuh	✔
identity_guard_rules	Identity Guard is an identity theft protection service	Created by Wazuh	✔
ids_rules	IDS events detected by OSSEC	Out of the box	✔
imapd_rules	imapd is the Courier IMAP server that provides IMAP access to Maildir mailboxes	Out of the box	✔
imperva_rules	Cyber security software and services to protect companies' sensitive data and application software from attacks.	Created by Wazuh	✔
jenkins_rules	Jenkins is an open source automation server written in Java. The project was forked from Hudson.	Created by Wazuh	✔
mailscanner_rules	MailScanner is a highly respected open source email security system design for Linux-based email gateways	Out of the box	✔
mcafee_av_rules	McAfee is an antivirus program.	Out of the box	✔
mongodb_rules	MongoDB is a free and open-source cross-platform document-oriented database program.	Created by Wazuh	✔
ms_dhcp_rules	Microsoft DHCP rules.	Out of the box	✔
ms_ftpd_rules	Microsoft FTP rules.	Out of the box	✔
ms_logs_rules	Microsoft Windows logs rules.	Created by Wazuh	✔
ms_sqlserver_rules	Microsoft SQL Server is a relational database management system developed by Microsoft.	Created by Wazuh	✔

WAZUH

OSSEC Ruleset			
Rule	**Description**	**Source**	**Updated by Wazuh**
ms_wdefender_rules	Windows Defender is an anti-malware component of Microsoft Windows.	Created by Wazuh	✔
msauth_rules	Microsoft Windows events deteced by OSSEC.	Out of the box	✔
ms-exchange_rules	Microsoft Exchange Server is a calendaring and mail server developed by Microsoft	Out of the box	✔
ms-se_rules	Microsoft Security Essentials (MSE) is an antivirus software (AV) product that provides protection against different types of malicious software	Out of the box	✔
mysql_rules	MySQL is an open-source relational database management system (RDBMS).	Out of the box	✔
named_rules	named is a Domain Name System (DNS) server.	Out of the box	✔
netscaler_rules	NetScaler is a hardware device (or network appliance) manufactured by Citrix, which primary role is to provide Level 4 Load Balancing. It also supports Firewall, proxy and VPN functions	Created by Wazuh	✔
netscreenfw_rules	Netscreen is a high performance firewall.	Out of the box	✔
nginx_rules	Nginx is a web server with a strong focus on high concurrency, performance and low memory usage.	Out of the box	✔
openbsd_rules	OpenBSD is a Unix-like computer operating system descended from BSD.	Out of the box	✔
opensmtpd_rules	OpenSMTPD is a FREE implementation of the server-side SMTP protocol as defined by RFC 5321, with some additional standard extensions.	Created by Wazuh	✔
openvpn_rules	OpenVPN is an open-source software application that implements virtual private network (VPN) techniques.	Created by Wazuh	✔
oscap_rules	OpenSCAP is an open-source software that provides assessment, measurement and enforcement of security baselines.	Created by Wazuh	✔
ossec_rules	Main rules	Out of the box	✔
pam_rules	A pluggable authentication module (PAM) is a mechanism to integrate multiple low-level authentication schemes into a high-level application programming interface (API).	Out of the box	✔
php_rules	PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language.	Out of the box	✔
pix_rules	Cisco PIX (Private Internet eXchange) is a popular IP firewall and network address translation (NAT) appliance.	Out of the box	✔
policy_rules	Policy rules (login during weekends, non-business hours)	Out of the box	✔
postfix_rules	Postfix is a free and open-source mail transfer agent (MTA) that routes and delivers electronic mail.	Out of the box	✔
postgresql_rules	PostgreSQL is an object-relational database management system (ORDBMS) with an emphasis on extensibility and on standards-compliance.	Out of the box	✔
proftpd_rules	ProFTPD is an FTP serve	Out of the box	✔
puppet_rules	Puppet is an open-source configuration management utility.	Created by Wazuh	✔
pure-ftpd_rules	Pure-FTPd is a free (BSD license) FTP Server	Out of the box	✔
racoon_rules	Racoon is a key management daemon used for VPN connections.	Out of the box	✔
redis_rules	Redis is an open source (BSD licensed), in-memory data structure store, used as database, cache and message broker.	Created by Wazuh	✔
roundcube_rules	Roundcube is a web-based IMAP email client.	Out of the box	✔
rsa-auth-manager_rules	RSA Authentication Manager is a platform behind RSA SecurID that allows for centralized management of the RSA SecurID environment.	Created by Wazuh	✔
rules_config	Main rules	Out of the box	✖
sendmail_rules	Sendmail is a general purpose internetwork email routing facility that supports many kinds of mail-transfer and delivery methods, including SMTP used for email transport over the Internet.	Out of the box	✔
serv-u_rules	FTP Server software (FTP, FTPS, SFTP, Web & mobile) for secure file transfer and file sharing on Windows & Linux.	Created by Wazuh	✔
smbd_rules	SMBD is a server that can provide most SMB services. The server provides filespace and printer services to clients using the SMB protocol.	Out of the box	✔
solaris_bsm_rules	Solaris Basic Security Module (BSM) can create an extremely detailed audit trail for all processes on the system.	Out of the box	✔
sonicwall_rules	SonicWall is a network firewall.	Out of the box	✔
sophos_rules	Sophos Anti-Virus.	Created by Wazuh	✔
spamd_rules	spamd is a ISC-licensed lightweight spam-deferral daemon written under the umbrella of the OpenBSD project. spamd works directly with smtp connections, and supports features such as greylisting, minimising false positives compared to a system that does full-body analysis.	Out of the box	✖
squid_rules	Squid is a caching and forwarding web proxy.	Out of the box	✔

OSSEC Ruleset			
Rule	**Description**	**Source**	**Updated by Wazuh**
sshd_rules	sshd (SSH Daemon) is the daemon program for ssh.	Out of the box	✔
symantec-av_rules	Symantec is an antivirus program.	Out of the box	✔
symantec-ws_rules	Symantec Web Security	Out of the box	✔
syslog_rules	Rules to analyze syslog messages	Out of the box	✔
sysmon_rules	Rules to detect Windows Process Anomalies	Out of the box	✔
systemd_rules	Systemd is a software suite for central management and configuration of the GNU/Linux operating system.	Out of the box	✖
telnetd_rules	Telnet protocol daemon	Out of the box	✖
trend-osce_rules	Trend Micro OSCE (Office Scan) rules	Out of the box	✔
unbound_rules	Unbound is a validating, recursive, and caching DNS server software.	Out of the box	✖
usb_rules	Rules to track usb devices.	Created by Wazuh	✔
vmpop3d_rules	vm-pop3d is a POP3 server.	Out of the box	✔
vmware_rules	VMware is a virtualization software .	Out of the box	✔
vpn_concentrator_rules	Cisco VPN Concentrator	Out of the box	✔
vpopmail_rules	vpopmail is a free GPL software package, to provide a way to manage virtual e-mail domains and non /etc/passwd e-mail accounts on qmail mail servers.	Out of the box	✔
vsftpd_rules	vsftpd is an FTP server for Unix-like systems, including Linux.	Out of the box	✔
web_appsec_rules	Rules for vulnerabilities and attacks related with web	Out of the box	✔
web_rules	Web access rules	Out of the box	✔
wordpress_rules	WordPress is a free and open-source content management system (CMS) based on PHP and MySQL.	Out of the box	✔
zeus_rules	Zeus is a lite Web Server	Out of the box	✔