alienvault	**AlienVault 3.1**	
	Security Information & Event Management (SIEM)	
	Systeemvereisten: Min. 4GB RAM. Geen besturingssysteem. Systeemvereisten afhankelijk van omgeving.	
	Ontwikkeld door:	AlienVault
GPLv3 / Commerciële licentie	**Contactpersoon:**	kristof.verslype@smals.be

Functionaliteiten

AlienVault is een typisch SIEM product. Veiligheidsgerelateerde logs worden dus door de verschillende apparaten in de IT-infrastructuur (endpoint systemen, firewalls, application servers, IDS, etc.) naar een centrale SIEM server gestuurd voor analyse om kwetsbaarheden en veligheidsincidenten te detecteren. Een belangrijk aspect hierbij is de correlatie, waarbij verbanden tussen logs, die mogelijks op verschillende plaatsen en verschillende tijdstippen gegenereerd werden, gezocht worden.

De voornaamste functionaliteiten in *OSSIM*, de gratis open source component, zijn:

- Het overzichtelijk weergeven van de kwetsbaarheden in de IT-infrastructuur.
- Het oplijsten van de verdachte gebeurtenissen (vb. brute-force password attack). Elke dergelijke gebeurtenis krijgt een prioriteit van AlienVault.
- Het genereren van een alarm wanneer de prioriteit van een gebeurtenis een drempelwaarde overschrijdt. Dergelijke alarmen worden op AlienVault dashboards getoond en kunnen per e-Mail verstuurd worden.
- Tonen van de beschikbaarheden van de verschillende systemen en services.
- Het doorzoekbaar maken van de recent binnengekomen gebeurtenissen.
- De mogelijkheid om bij elke gebeurtenis door te klikken tot op het niveau van de individuele logs.
- Het weergeven van de evolutie van de hoeveelheid netwerkverkeer. Er kan geselecteerd worden op netwerksegement, op ip-adres, op type pakketjes (vb. torrents), etc.

De voornaamste extra SIEM functionaliteit in de betalende versie is:

- De generatie van rapporten die een overzicht geven van de incidenten, kwetsbaarheden, etc., Door SIEM systemen gegenereerde rapporten worden veelal gebruikt om compliancy met regelgevingen na te gaan.
- Het vinden van specifieke, potentieel minder recente gebeurtenissen en logs. Dit is bijzonder nuttig bij onder meer forensisch onderzoek.

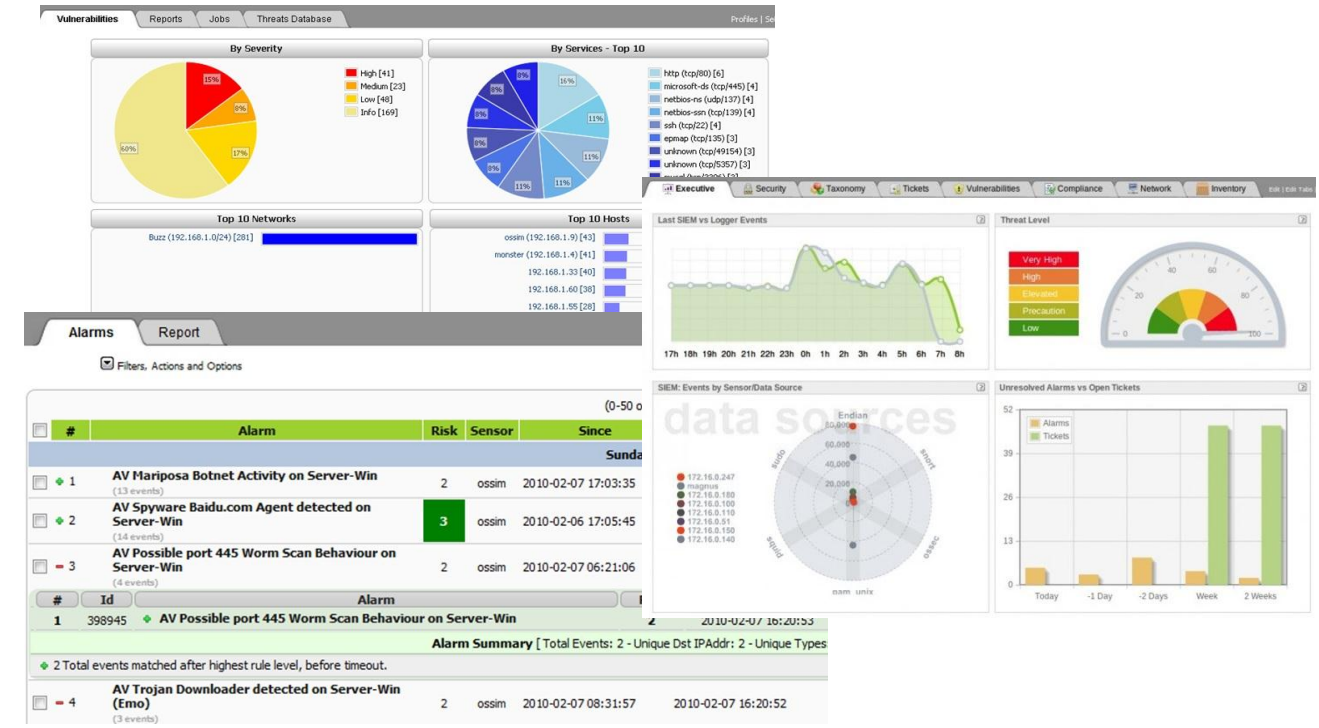
Conclusies en Aanbevelingen

AlienVault is een waardevolle tool die erin geslaagd is heel wat reeds bestaande open source software (Nessus, Snort, Nagios, etc.) netjes te integreren in een SIEM tool die vrij overzichtelijke dashboards aanbiedt. Desondanks kan het niet tippen aan de top SIEM producten.
Een vaak onderschatte inspanning is nodig om AlienVault te configureren, alsook de verschillende applicaties en toestellen die hun logs voortaan moeten doorsturen naar de AlienVault server.
Ondanks de uitgebreide documentatie is er toch wat tijd nodig om AlienVault te doorgronden, maar gelukkig is er ook nog de uitgebreide community.

Testen en Resultaten

De testen werden uitgevoerd in een virtuele omgeving gebruikmakend van VirtualBox. De virtuele omgeving bestond uit een firewall, een applicatieserver, twee end-point systemen, de AlienVault server en een externe aanvaller. AlienVault heeft zijn eigen Debian-gebaseerde besturingssysteem, de aanvaller gebruikte BackTrack en de andere systemen Ubuntu. Verschillende services zoals DNS, e-Mail en SSH werden geïnstalleerd op de applicatieserver.

Het installeren van AlienVault verliep vlot en probleemloos. Gezien de volledige testomgeving op linux gebaseerd is, werd van Syslog gebruik gemaakt om de logs naar de AlienVault server te sturen. Als je met Syslog vertrouwd bent, is dit vrij snel te doen voor één systeem. Standaardapplicaties zoals Bind en OpenSSH worden door AlienVault goed ondersteund. De ondersteuning voor andere besturingssystemen en wat exotischere toepassingen werd niet getest. Indien deze ondersteuning nog niet aanwezig is, kunnen wel zogenaamde plugins en directives daartoe gecreëerd worden. De gesimuleerde aanvallen (DoS aanval, brute-force SSH aanval, reconnaissance, etc.) werden vlot gedetecteerd, maar vele hedendaagse aanvallen zijn uiteraard complexer. De vraag blijft dus in zekere zin in hoeverre AlienVault voldoet aan de verwachtingen in een reële productieomgeving.



Voorbeelden van de web-based dashboards in AlienVault

Gebruiksvoorwaarden

Het basispakket OSSIM is vrij beschikbaar onder de GPLv3 open source licentie. Om gebruik te maken van de volledige kracht en functionaliteit van AlienVault SIEM, wat aangeraden wordt voor bedrijfscontexten, moet $32.000 op tafel gelegd worden. Bijkomende support is mogelijk en kan voor 24/7 support oplopen tot $50.000 per jaar (bron: scmagazine.com).