

RSA Envision cursus

Bijgedragen door Steph
Wednesday 23 September 2009

Ik heb deze week cursus van RSA Envision. Dit is een behoorlijk mooie en complexe oplossing. Het is een passief apparaat dat logs van zo'n beetje alle apparatuur en applicaties kan verwerken. Welke logs hij niet kan, kan je zelf fixen.

De theorie achter de applicatie is simpel: Een beetje bedrijf heeft een aantal logs per minuut, misschien zelfs een tiental per seconde. Deze hoort de admin te controleren, maar in het beste geval gebeurt dit enkel bij problemen. Envision helpt hierbij: het schift de logs voor je. Envision sorteert ze op belangrijkheid, bewaart alles en heeft alerts of zelfs de mogelijkheid automatisch een call te registreren wanneer er iets mis is. Deze alerts zijn zo goed in te stellen dat je zelfs correlatie kan toepassen: Wanneer dit gebeurt, gevolgd door dat, dan hebben we pas een reden om er een punt van te maken: Wanneer een ip onze firewall scant is dat niet interessant, wanneer ditzelfde ip daarna een succesvolle connectie opzet (op zichzelf ook niet vreemd) dan is 1 en 1 een hele goede reden om hier een alert bij te genereren!

Op deze manier til je security en ook waarschuwingen naar een heel nieuw niveau. Een niveau dat zelfs automatisch met zich meebrengt dat je aan een hoop certificeringen (sox etc.) voldoet. Dus voor bedrijven interessant!

Het is een zeer complex maar super interessant geheel waarvan ik dus echt wel onder de indruk ben. De architectuur is indrukwekkend maar begrijpelijk en open. Het is vrij makkelijk om te beredeneren waar dingen mis gaan en er zijn behoorlijk bizarre limieten aan de hardware.

Ik krijg de les van Hap Waters, een RSA leraar uit Boston. Hij geeft geweldige cursus, is bijzonder grappig en onderhoudend. Hij weet dingen boeiend te linken en de klas echt mee te nemen in de materie. Ik geniet er dus echt van. De man heeft een zeer grappige en extreem humoristische cynische kant, hij zeikt de cursisten continue af op zeer grappige manieren. Je kan er echt niet boos van worden :). Morgen de laatste dag, ik vind het nu al jammer!

Technorati: ((RSA)), ((Envision))