

RE: Securty Audit Correlating

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2004-12/0070.html>

From: Jose Costa (josepcosta_at_yahoo.com.br)

Date: 12/20/04

Date: Mon, 20 Dec 2004 09:07:08 -0300 (ART)

To: John Bankes <jbanks@netforensics.com>, "'SecurIT Informatique Inc.'" <securit@iquebec.com>

Thanks for the information but I need to do it offline because I just need to do it every 3 months to create a report to our CSO.

I'll start working on it this week. I'll test exporting both(events and tickets) to a SQL/Access DB and figure out how to correlate them.

Any sample or idea will be appreciated.

Tks,

JL

----- John Bankes <jbanks@netforensics.com> escreveu:

- > *We also provide most of what you are looking for.*
- > *Check out*
- > *www.netforensics.com for more information. Sorry*
- > *for the commercial, but it*
- > *might be what you're looking for. JB*
- >
- > -----Original Message-----
- > *From: SecurIT Informatique Inc.*
- > *[mailto:securit@iquebec.com]*
- > *Sent: Thursday, December 16, 2004 6:47 PM*
- > *To: Jose Costa*
- > *Cc: focus-ms@securityfocus.com*
- > *Subject: Re: Securty Audit Correlating*
- >
- > *Hello Jose,*
- >
- > *I am not sure if this will fit all your bill, but*
- > *you may want to look at my*
- > *log centralising and analysis software LogAgent*
- > *(<http://securit.iquebec.com>). It will analyse in*
- > *real time your event*
- > *viewer logs, so you can set filters for specific*

SecurityFocus Microsoft: RE: Securty Audit Correlating

> *object access, accounts*
> *usage or event type, and it will convert your event*
> *viewer logs in ascii at*
> *the same time.*
>
> *As for the correlating, it is probably possible to*
> *use one of the consoles I*
> *designed (LogIDS or LogMonitor) by converting your*
> *tickets in ascii. Or*
> *maybe that the extractor side-tool I wrote with*
> *these consoles is better*
> *suited for your needs. If you think that these*
> *things could help you, but*
> *the correlating does not exactly satisfy you, let me*
> *know and I can probably*
> *write you something customized to your needs, that*
> *is if you cannot find*
> *anything else around.*
>
> *Feel free to contact me if you have any questions*
> *regarding these tools.*
>
> *Adam Richard*
> *SecurIT Informatique Inc.*
>
> *At 02:54 PM 16/12/2004, Jose Costa wrote:*
> *>Hi all,*
> >
> *>Currently we are outsourcing our account creation,*
> *password*
> *>unlock/modify, folder creation/access control and*
> *Internet/Applications*
> *>Access Control to a third company and we need some*
> *audit and reports.*
> *>We use AD running on W2K Server.*
> >
> *>Basically what we want to do is to activate GPO*
> *Account Management and*
> *>Object Access and create some users with*
> *Admin/Account Operators rights*
> *>and log their object access on File Servers top*
> *folders and account*
> *>management tasks.*
> >
> *>After that,we need to do some correlating with Help*
> *Desk Tickets, based*
> *>on time. We will audit that with samples, not all*
> *logs or tickets.*
> >
> *>The target is to discover if these accounts were*
> *used without a help*

RE: Securty Audit Correlating

SecurityFocus Microsoft: RE: Securty Audit Correlating

Yahoo! Acesso Grátis – Instale o discador do Yahoo! agora. <http://br.acesso.yahoo.com/> – Internet rápida e grátis
