



About AutoTrader.com

AutoTrader.com, created in 1997 and headquartered in Atlanta, Ga., is the Internet's leading auto classifieds marketplace and consumer information website. AutoTrader.com aggregates in a single location more than 2.5 million vehicle listings from 40,000 dealers and 250,000 private owners, which provide the largest selection of vehicles attracting more than 9 million unique visitors every month. Through innovative merchandising products such as multiple photos and comprehensive search functionality, AutoTrader.com unites buyer and seller online - dramatically improving the way people research, locate and advertise vehicles.

About Matthew Keogler

Matthew Keogler serves as Senior Security and Network Engineer. His primary responsibility is to manage security, but he also led the team that built the company's



network and continues to provide help with the system architecture for Autotrader.com. For the past three years he's also been a guest speaker covering topics of Intrusion Detection Systems and Security Event Monitors for The Institute for Applied Network Security.

AutoTrader.com

SANS What Works in Vulnerability Management

Autotrader.com designed an effective security process to prioritize the most important security events and vulnerabilities so that the right things get fixed first.

INTERVIEW

Q. What was the challenge you were facing that led you to look for an improved solution?

A. The biggest challenge was the sheer number of security events coming in from our IDS. I needed to filter out the noise, get rid of false positives, and make decisions about what actually mattered.

My concern was that the false positives were camouflaging the real attacks. I wanted to find out what was really important. I am not nearly as worried about ping floods as I am about an attack on a vulnerability in my Apache server.

Q. How did you go about solving the problem?

A. I created a list of business and technical requirements. One of the main technical requirements was for an IDS event to automatically go through a validation/verification process before being displayed to the screen. I had been running open-source Snort but even after customization it was constantly flooded with false positive events. The key piece of data that was missing was whether the targets of the attacks were vulnerable. If they were, then the attack mattered. If they were not, then the attack wasn't important.

Q. Wouldn't a scanner have told you what was vulnerable?

A. Yes, but it wouldn't connect the attacks with vulnerabilities. It wouldn't tell me which vulnerabilities outsiders were trying to exploit.

Q. How did you go about looking for a better solution?

A. I started from the ground up -- reading the latest trade magazines that covered IDS vendors, gathering information, and documenting my findings. I then matched my business and technical requirements with the information gathered, which helped boil the list of IDS vendors down to two. I then created an in-house bake-off placing the machines in a production environment. My experience has shown that one product always sells itself and in my case, it was Sourcefire.

Q. What is it?

A. A whole different way of approaching the problem called passive network discovery, behavioral profiling and vulnerability analysis technology. This tool gave me a good vulnerability test, although not quite as good as a stand-alone scanner. In addition this data was correlated with the IDS data. The combination showed me which events really mattered. When Sourcefire merged the passive monitoring technology with the IDS, it opened a whole new set of opportunities for vulnerability management based on actual threats.

Q. How well does it work?

A. It eliminated the problem of being inundated by events. Now I can marry the vulnerability status of the server and application to an event and target the ones that matter.

"When Sourcefire merged the passive monitoring technology with the IDS, it opened a whole new set of opportunities for vulnerability management based on actual threats."

"It all came together really well. I could see an event that was rated with an impact flag because I knew the system being targeted was vulnerable. I could pick which vulnerability levels I wanted to view and have the events prioritized."

"[Sourcefire] eliminated the problem of being inundated by events."

Q. How do you know it works?

A. One of the ways it helps us improve security is that it gives us a centralized place to view vulnerability status of our applications, per server. That way we know whether the patch management system missed anything and what versions of things are running and what the server vulnerabilities have. We can really see what's going on in our infrastructure and we now have data to support doing forensics and looking deeper into our applications. And we can fix the important things very quickly.

Q. Before we go deeper into what it does for you, can you help us understand just what a passive system does and how it is different, for example, from a scanner?

A. Sure. The passive technology watches and interprets all network traffic. Since every system on the network talks with other systems, the passive monitoring provides up-to-the-minute information on what is and isn't running on our network.

Q. Why is that better than a regular scanner?

A. It is much better than the vulnerability scanners. Most of the active vulnerability scanners are used once a month or once a quarter. The passive technology is continuous. So if someone adds a vulnerable system to our network, the passive technology tells me right away, something that I would have to be very lucky to learn from a regular vulnerability scanner that might not be run for days or weeks after the vulnerable new system has been installed. In addition, passive technology isn't intrusive to my network or servers the way active systems can be.

Q. Are the active vulnerability scanners more accurate?

I believe it is probably more detailed on the less important problems, but I have yet to find a situation where the Sourcefire RNA® (Real-Time Network Awareness) passive technology didn't tell me about the important vulnerabilities.

Q. So if I understand you correctly, you now have a passive discovery system continuously monitoring your network assets, called RNA, that tells you which vulnerable systems are on the net.

A. Yes, RNA does that and more. What is great about it is that it marries that information with the IDS attack data so it can tell me whether an attack is actually likely to be successful.

Q. How do you respond to alerts?

A. I look at each of the high priority events. For example, when a high priority alert comes in, I take down information about the operating system and application. I have a close relationship with the operations team, so I go to the team and ask them for patch level and other data about the target machine. I have procedures in place that get triggered depending on their response.

Then I go to the IDS and see what happened. I do this for high impact events only. We probably get one or two a day. Based on the architecture and application, I know where we are most vulnerable and I go there first.

Q. What kinds of things has it helped you find?

A. I have found a lot of things relating to internal users such as peer-to-peer traffic and worms. Another example is that we discover unauthorized dual booted machines (set up to support both Windows and Linux on the same computer) because we see mail going out over port 25 from the Linux partition.

"[Sourcefire RNA] is much better than the vulnerability scanners. Most of the active vulnerability scanners are used once a month or once a quarter. The passive technology is continuous."

"And RNA, the passive technology just works right out of the box. It doesn't take any time at all."

"The ability to correlate events from Sourcefire's RNA and Intrusion Sensors into one ImpactFlag event has helped AutoTrader.com identify the most important problems"

Q. What do you do when you find something like that?

A. We ask people very nicely to stop. Over time word gets around about the things we have found and users start to believe that the security department can see anything. They get spooked into playing nicely.

Q. How good has the technical support been from the Sourcefire people?

A. Any time I need help I get it. I believe they have the best support staff and more willingness and ability to resolve problems than any other security vendor. No one is perfect. We might not always get the answer we like, but we do get the right answer.

Q. Have you ever asked for additional capabilities?

A. Originally the correlation of an RNA and IDS event created one composite event that had an Impact flag. It wasn't real time. We pushed and they fixed it so it comes pretty close to real time. The tools they give you are exceptionally powerful.

Q. Can you think of features you would like to see in RNA that are not there now?

A. Resolving employee IP addresses to machine names would be a nice touch. One of the first things a security engineer has to do when an employee event requires further analysis is convert the IP to a machine name.

Q. If someone was going to implement the Sourcefire 3D System, which includes RNA and Snort-based Intrusion Sensors and the Defense Center, how many people should they allocate to support the facility?

A. It depends on many factors. Previous experience with open-source Snort and, of course, a SANS IDS class couldn't hurt. The creation of the policies for the Intrusion Sensors will take the most time to fine tune. Having an engineer with prior knowledge of your network can greatly minimize time. Push the policy and the system runs on its own, relatively speaking. And RNA, the passive technology just works right out of the box. It doesn't take any time at all.

I spend much more time with the operations staff identifying and correcting security problems. Once the system provides me with the impact flag events, I use this data to decide what warrants further analysis. So all day long, my eyeballs are on the SEM watching for new discoveries. I can also set it up so that it alerts me when, for example, it sees outgoing email (port 25) traffic going across the wire.

Q. What type of problems have you been fixing lately that the system has found?

A. Unauthorized Operating Systems are very easy to detect. In addition, any worm with an installation of a SMTP engine is now very easy to detect real time. It's a great tool for ensuring servers are adhering to your network usage policy. (e.g., servers in the management network that don't allow any connections to the outside world are easily caught if configured incorrectly.)

Q. Do you have any advice for people who are thinking about following this approach?

A. Do your homework. Conduct your own analysis, document your findings and match that against your requirements. Once I did all this, the product sold itself. Sourcefire met all my expectations, plus resolved several new requirements within a few product updates.

"The tools they [Sourcefire] give you are exceptionally powerful."

Q. For you, what has been the bottom line?

A. The ability to correlate events from Sourcefire's RNA and Intrusion Sensors into one ImpactFlag event has helped AutoTrader.com identify the most important problems. The problem of dealing with false positives isn't gone but it has been greatly reduced and reduced enough to give engineers the ability to act. It lets us clean our systems and keep them clean.

BOTTOM LINE ON SOURCEFIRE RNA

1. Converts IDS information into actual threat information.
2. Prioritizes actions so security engineers know what to fix first.
3. Provides proof that problems are actually being attempted so system administrators know it is important to get them fixed.
4. Helps improve security by giving a centralized place to view vulnerability status of applications, per server.
5. Watches and interprets all network traffic, and provides up-to-the-minute information on what is and isn't running on network.
6. Sourcefire's RNA has helped identify the most important problems and keep the systems clean.

ABOUT SANS WHAT WORKS

SANS What Works saves user organizations months of time that would be wasted in trying to uncover the truth about which Internet security tools actually work in their environments. What Works is a user-to-user program in which managers from organizations that have implemented each of the effective internet security technologies tell a complete story of why they deployed it, how it works, how they know it actually improves security, what problems they faced, and what lessons they learned. Without What Works, buyers are at the mercy of sales people who, too often, do not have sufficient security expertise to understand how their products fit into a defense in depth and what the tools can and cannot do. Only users know the answers to those questions. Smart buyers have always demanded an opportunity to talk to users directly. SANS What Works brings those users to you in written interviews and in live and recorded webcasts where you can get your questions answered.