eWEEK

http://www.eweek.com/security/jask-applies-ai-to-security-incident-analysis-management
JASK Applies AI to Security Incident Analysis, Management
24/05/18

By: Wayne Rash | May 24, 2018
NEWS ANALYSIS: A new autonomous security operations center platform from JASK promises to make the workload of security analysts more effective and less overwhelming than what's been done in the past.

SAN JOSE, CA—Imagine a security analysis platform that can comb through the thousands of alerts you're getting from your intrusion detection system, your firewalls and your log files and look for connections between seemingly minor events to develop a picture of what may become a major security incident.

Then imagine that it uses that information to present an evaluation of the potential security incident in a way that lets you see that the threat may be along with correlated data.

This is exactly what JASK (and acronym comprised of "Just Ask") is intended to do. JASK can accept input from a variety of security appliances, software packages, log files and combine it with a vast database of previous security incidents as well as warnings from security services and then look for patterns.

It learns from patterns previously seen from other JASK users to analyze and evaluate those incidents. Then it presents them with its appraisal of the threat level and the degree of confidence. A security analyst can click on the display of an evaluated series of incidents to get a detailed explanation of the factors that prompted the system to display an alert.

"We have a huge corpus of knowledge," explained Greg Fitzgerald, CMO of JASK. He added that because each organization is different, JASK will still have a learning curve as it begins being used in a new organization, but "It gets smart fast," he said.

While I was discussing a demonstration of JASK at the NetEvents conference at the Hayes Mansion here, I saw what the company calls an "Insight" presented as an insider threat. The

Insight was a circle with several small segments, each with a level of severity indicated by color. Those segments are called “Signals” and they represent a particular action taking place on the network that taken together can indicate a security threat.

Click on each one of those segments and it spells out exactly what happened. In one case it might be a series of failed logins. In another it might be a series of horizontal network connections that don’t normally exist. Or it might be a large data transfer.

The segments, or Signals, in themselves might be minor, but it’s the correlation that makes them important enough to become an Insight. In the case I was looking at, the Insight revealed an IP address, which revealed the identity of a specific employee’s workstation. In this case it even had the employee’s photo.

The confluence of information was enough to warrant a discussion with the employee, but the fact that the person’s photo was included also meant that it was possible to tell if the employee assigned to that workstation was actually the one using it. This could have been a disgruntled employee getting ready to leave the company, but it also could have been someone else at that employee’s workstation, quietly stealing data while the employee was away.

What’s important about the JASK software is that it can discover events that would probably never be noticed by a human analyst that’s confronted by thousands of incidents on a daily basis. In the demonstration incident I saw each of the individual Signals that made up the Insight was too minor to come to the attention of an analyst. It was only when they were examined together that their importance became apparent

This sort of pattern is very common for major security breaches. A series of small incidents, perhaps a phishing email sent to an administrative employee that harvests credentials, followed by an email to the CFO or the CEO designed to elicit a cash transfer might get the attention of a security analyst if the events had been noticed.

But tie that to a hacking incident that reveals the employee phone book and then to a series of other phishing emails that weren’t acted on, along with emails from an outside server spoofed so that they seemed to be from an inside server are all indications that an attack is about to begin.

A warning like that, received in a timely manner, would be crucial to preventing a breach. It may also point up potential security weaknesses that can be fixed before serious data loss happens.

What makes JASK unusual, along with the machine learning and AI that allow it to make those correlations, is the fact that it doesn’t need to supplant your existing security structure. It makes use of the output of whatever security systems the customer is already using. It can also extract data from your existing log files and from your raw network traffic. All you need to do is provide access.

JASK is a cloud-based application that lives on Amazon Web Services. It can use data from other cloud services or from on-premises sources. The pricing model for JASK is fairly simple, starting at $100 per user per year with volume discounts for larger organizations. Fitzgerald said that the largest customer is a Fortune 100 company with over 300,000 users, but that it can scale down to single user companies.

This is a significant step in solving the problem that plagues corporate IT security operations. They have just too much security data and no efficient way to sort through it. Many, if not most, major breaches were obvious when they were analyzed after the fact. But when they happened the signs were too small to be noticed. Now JASK has found a way to make sure they’re not missed.