IBM Software Community

Overview
Recent Updates
Members
- **Blog**

Bookmarks
Feeds
Files

Categories

Connect and collaborate
Turn information into insights
Optimize business integration and optimization
Enable product and service innovation
Impact of business infrastructure and services
Manage risk, security, and compliance

Tags

Find a Tag

2012 analytics application baforum big-data bpm business business_analytics business-analytics business-rules capabilities capability cloud cloud-computing

IBM Software Blog

This blog promotes thoughtful discussions and perspectives on how software is changing the way we live and do business.

The short URL for this blog is http://ibm.com/blogs/software

My grandmother – security intelligence pioneer

Wes Simonds | Feb 14 2012 | Tags: software log ibm service-management management labs simonds michael siem security information intelligence applebaum event capabilities wes q1 rsa

0 Comments | 10,274 Visits

Quite a few of today's organizations could learn a little something about security from my grandmother -- a thoughtful, yet paranoid creature who maintained a watchful vigilance over her home. I recall once she was going to Europe for two weeks. So, anticipating hordes of burglars, she developed an advanced domestic security architecture:

1. Neighbors facing the front and back of the house were asked to keep watch for any sign of intrusion, such as open windows
2. The doors and windows were locked, and to the doors, new deadbolts were added
3. Her mail and newspapers were stopped
4. All her more expensive possessions, such as jewelry, were hidden
5. There were many such hiding places distributed throughout the house
6. The list of hiding places was, itself, hidden -- in the dictionary, under the verb 'hide'

I believe quite a few IT security concepts can be extrapolated from this ad hoc architecture. Let's go down that list and rephrase things a bit...

1. Data must be continually collected from many sources and analyzed for relevance, using proven heuristics
2. Point solutions like firewalls, though useful, are far from adequate by themselves
3. Proactive measures should be taken to address potential security gaps
4. Assets should be protected in proportion to their business value
5. Strategies spanning multiple domains should be pursued to maximize holistic security
6. Centralized oversight of those strategies will simplify and accelerate management

Not too shabby, I think, for a woman in her late seventies with no training.

And in the area of security intelligence, one finds many of the same concepts explored. In fact, security intelligence – powered by next-generation Security Information and Event Management (SIEM) and log management – emphasizes all the points above. Taken together, these assertions about data, analytics and centralized analysis can lead to a greatly enhanced security posture.

This may remind you of business intelligence, which uses advanced analytics to aggregate business data and sift through it looking for hidden patterns or insights. Security intelligence does much the same with security data. And just

Feeds

Feed for Blog Entries
Feed for Blog Comments
Feed for Comments for this Entry

Blog Authors


Marcela Adan


Whei-Jen Chen


BRENDAN MCGUIRE

1 - 3 of 69 authors

Translate this page

IBM Software Elsewhere

IBM Software on the Web
IBM Software Conversations
IBM Software community
IBM Software on Twitter
IBM Software on YouTube
IBM Software on Livestream
IBM Software on LinkedIn
IBM Software Newsletter
E-mail IBM Software

Archive

September 2015
July 2015
April 2015
March 2015
February 2015
January 2015
December 2014
November 2014
October 2014

cognos cognos10 data decision-making decision-management ibm ibm-security ibm100 ibminterco nnect ibmsecurity ibmsoftware ibmwatson informatio n-insights interconne ct iod11 management mobile mobility predictive -analytics product-in novation rational rules security security-i ntelligence service-ma nagement simonds smarter smarter-analytics social social-business social-media software spss statistics websphere wes

Cloud | List

Tagged #ibmsoftware

Similar Entries

IBM Analytics Proven...
Blog: IBM Analytics...
Susan Magilton
Updated Wednesday 9:37 PM
0 0

Internet das Coisas:...
Blog: Falando de TI
Roberto Amaro
Updated Wednesday 8:04 AM
0 0

New z13 Mainframe is...
Blog: Linux is on f...
Mihai Ioan
Updated Sep 7
0 0

Turbo-Charge Your Li...
Blog: Linux is on f...
Mihai Ioan
Updated Sep 7

as with business intelligence, security intelligence works better when solutions are smarter: capable of drawing more data, from more sources, analyzing it more quickly, drawing more accurate conclusions and thus turning a spotlight on what really matters (while avoiding, what doesn't).

That, in a nutshell, is why in 2011 IBM acquired Q1 Labs, a leading provider of SIEM and security intelligence solutions that reduce security and compliance risks and better detect suspicious events that may be taking place in the IT environment.

Last-generation solutions can't cope with next-generation threats
Recently I had a chance to talk to Michael Applebaum, Director of Product Marketing for Q1 Labs, about security intelligence and how it relates SIEM.

'Security Intelligence is actually a superset of SIEM,' said Applebaum. 'It involves collecting and analyzing many types of security and compliance-relevant data for real-time decision making. And to do that, it goes far beyond first-generation SIEM tools -- not just performing log data analysis, but also correlating related data like network flows and asset profiles, to provide deeper visibility into what's really happening.'

The problem with earlier SIEM solutions, it appears, is threefold: They aren't smart enough to make sense of all the data, they aren't adequately integrated with other security solutions and they aren't flexible enough to cope with organizations' changing needs.

So IT teams tend to get bombarded with false positives that, though seemingly suspicious, don't actually involve a security incident. This is roughly like the difference between 'breaches' (which are security-relevant) and 'breeches' (which are short pants).

'Too often, solutions dump so much data on the security professional that the solutions become useless,' said Applebaum. 'Managing more data than ever before requires sharper tools to find what matters. SIEM and security intelligence, then, are about culling through the masses of data to find the signal in the noise.'

Indeed. And bumping up that signal-to-noise ratio, via smart analysis, is particularly critical at a time when hackers and malware are both getting more sophisticated and capable -- often, in ways that simply defeat last-generation security solutions.

Want an example? Consider the Conficker worm -- an incredibly resilient form of malware with multiple variations that can attack organizations using multiple, completely different attack vectors. This is not the sort of thing organizations are going to be able to recognize and eradicate using traditional, signature-based tactics, which is probably why Conficker is still around, and still creating problems, despite the fact that it was originally detected in 2008.

Organizations are, from a security standpoint, simply living in a different world than they were even five years ago, and they need solutions that are just as smart as the threats they face -- or, ideally, smarter. And that's exactly where security intelligence can play a valuable role.

What IBM's new security intelligence solutions bring to the game is scalable, fast correlation of exceptionally large data volumes, originating from a wide range of IT systems and devices, to deliver a complete view of the total security posture at any point in time. So, going beyond log analysis, that also means key capabilities like configuration monitoring, network anomaly detection and advanced persistent threat detection.

In this way, threats like Conficker become significantly more detectable and resolvable, even though they appear in multiple variations and take advantage of different security weaknesses. Instead of trying to recognize them using a specific exploit-based signature, or any other limited identifier, organizations can instead recognize that type of behavior as suspicious and worthy of investigation.

Perhaps, for instance, a sequence of failed log-in attempts to a high-value database is followed by a successful log-in attempt and a data selection, which is then followed by an email transmission of a large amount of data to an IP address in an eastern European country where this organization has never done business.

September 2014
August 2014
July 2014
June 2014
April 2014
March 2014
February 2014
January 2014
December 2013
November 2013
October 2013
September 2013
August 2013
July 2013
June 2013
May 2013
April 2013
March 2013
February 2013
January 2013
December 2012
November 2012
October 2012
September 2012
August 2012
July 2012
June 2012
May 2012
April 2012
March 2012
February 2012
January 2012
December 2011
November 2011
October 2011
September 2011
August 2011
July 2011
June 2011
May 2011
April 2011
March 2011
February 2011
January 2011
December 2010
November 2010
October 2010
September 2010
August 2010
July 2010

0 0

CAPI is Core to POWE...

Blog: Linux is on f...

Mihai Ioan

Updated Sep 7

0 0

This type of comprehensive analysis and insight detects questionable behavior almost in the way a trained and experienced human security expert would. It's significantly smarter and more flexible than the siloed kind of analysis most organizations are limited to today.

Get a 360-degree, real-time view of your complete security posture
However, making all of that happen does, in turn, mean security intelligence solutions have to bridge security, network and infrastructure silos, to put the whole picture -- prioritized by business value / risk and rendered via intuitive dashboards -- at the fingertips of security pros and executives.

Fortunately, that's just what IBM's new offerings can do. And it's a compelling strength, especially for organizations who may not have realized such a thing is even possible.

'The real 'a-ha' moment is when clients see how easily they can view and drill down into security-relevant activity across the enterprise -- logs, network flows, vulnerabilities, identities, asset profiles, threat intelligence -- all with a single user interface,' said Applebaum. 'Clients are so used to dealing with silos of data they are blown away by a security dashboard that provides seamless visibility.'

Still more value stems from the extensive range of report templates and correlation rules (like the kind I described above, involving a database compromise) that come with the solutions right out of the box. Through them, clients who deploy IBM's security intelligence solutions immediately inherit much of the deep expertise developed by Q1 Labs through years of real-world client experience.

That's not just better security, but better security achieved faster. And over time, as those templates and rules are expanded to include new insight from IBM's X-Force team, that argument will just get stronger and stronger.

Finally, all of these new security capabilities also pertain to a closely related issue: regulatory compliance. Through smarter, more comprehensive monitoring and reporting, organizations will find it easier not just to achieve compliance, but also to demonstrate it easily in the event of an audit.

'Clients often start by focusing on compliance initiatives because of the potential penalties for failure,' said Applebaum. 'And while compliance is just a part of a security program, it's an important step. Next-generation SIEM and log management provide central logging, reporting and monitoring, which provide peace of mind while reducing a great deal of manual effort.'

Additional Information

Discover how to build security intelligence into your processes

Check out Q1 Labs, an IBM company

Attend a webcast with Q1 Labs and Gartner about security in a post-perimeter world

Learn more about security intelligence at RSA Conference 2012

Connect with the IBM Security communities

Get the IBM X-Force 2011 Trend & Risk Report:

Read more at the official Q1 Labs blog

About the author
Guest blogger Wes Simonds worked in IT for seven years before becoming a technology writer on topics including virtualization, cloud computing and service management. He lives in sunny Austin, Texas and believes Mexican food should always be served with queso.

1

Add a Comment | More Actions

Comments (0)

There are no comments to display

Previous Entry | Main | Next Entry

Feed for Blog Entries | Feed for Blog Comments | Feed for Comments for this Entry