Case Study

Sentry Metrics Provides the Answer to Threat Level Assessment & Better Security Visibility

PRIMARY OBJECTIVE & STRATEGIC GOALS

AMD/ATI was searching for a method to stop the scrambling of IT staff in response to attempts to break into their systems.

They also required higher visibility into their operational infrastructure and a comprehensive trends analysis engine based on selected KPI's (key performance indicators).

PRINCIPAL CONTACTS

Alim Baydzhanov, Head of Security
Peter Hourihan, VP, CIO

DATE PUBLISHED

January 2007

SITUATION SUMMARY

ATI's Head of Security, Alim Baydzhanov, and his staff were already monitoring a large number of alerts and logs in their DMZ, but they were becoming "alert-fatigued".

Responding to each event and assessing the threat level in a timely, meaningful fashion was taking away valuable IT resources from the Enterprise.

Meantime, VP and CIO, Peter Hourihan, needed a higher level of understanding of the IT department's security state.

He needed better visibility into selected security events, as well as an easy way to track activity and flag potentially damaging trends.

Sentry Metrics provided the answer to both concerns.

PROBLEM / OBJECTIVE

Like most high profile companies AMD/ATI found itself the target of attacks of all kinds—from hackers, viruses, nasty zombie bots, and even disgruntled employees.

The number of incidents was increasing, and each one required a manual, time-consuming response. More often than not the incidents proved to be trivial or false, but they all needed to be attended to, taking costly IT personnel away from more productive work.

Additional staff may have helped, but this approach was not practical or feasible. A monitoring system may have improved visibility, but Alim was already "fed up with systems and their endless alerts".

In short, AMD/ATI suffered from *Alert Fatigue*. And it was getting worse.

> *"If you paid attention to every alert you'd miss something more important.*
> *The volume is too high. And there are lots of fake threats.*
> *You need to decide if you need to do the serious monitoring".*
> -Alim Baydzhanov

There are numerous commercial monitoring solutions available on the market but they all lack human intelligence. They "don't talk reason". A system can't understand the Enterprise and its particular needs.

What was needed was an intelligent second line of defence, somebody behind the monitoring system. An educated support team, available 24/7, to augment ATI/AMD's existing security and network group.

Leveraging Sentry Metrics' industry-leading Dashboard theSentry allowed Alim to bring in more knowledge without hiring more staff. In effect, he introduced a backup for his technical team with knowledge on demand, 24/7, and certified security experts (CISSP, CISA, CISM, Cisco, ISS, Check Point, etc.) who also have intimate knowledge of his environment.

Talk about adding value!

One of the biggest challenges in most organizations is a lack of visibility into the computing environment, and ATI/AMD was no exception.

Their VP and CIO, Peter Hourihan, was concerned about not just *what* was happening, but whether there were *trends* developing that required some type of response. He identified a specific range of metrics that required ongoing, consistent, reliable tracking and displaying in a coherent fashion so that trend analysis decisions could be made quickly and accurately.

He passed the monitoring of these key metrics to *Sentry Metrics* security professionals who were able to spot trends by leveraging their knowledge of the AMD/ATI environment. They continuously monitored the data stream and correlated the required Key Performance Indicators via their *Report Manager*.

Sentry Metrics shows him his true IT and Security operations.

The extensive data collection employed by *SentryMetrics* also allows AMD/ATI to leverage that information in both their immediate and long term Security and Compliance (e.g., SarbOx) decision making processes.

Historical information is stored so that compliance can be demonstrated to auditors, and explicit reports can be generated on demand.

The end result is that Peter now has a highly visual representation of the business and a transparency of function not previously available.

Not only did *Sentry Metrics' Report Manager* generate the requested data and present it clearly and accurately for Peter, but the certified professionals at *Sentry Metrics* had already screened out and assessed the trivial and false security alerts and threats, allowing Alim to concentrate on real-time security issues.

For both Peter and Alim, *Sentry Metrics* is seen not as a product, but as an efficient use of resources. Professional help and the personal touch they bring is always a phone call away, any time—a single source for knowledge, reports and analysis.

> *"Quantitative solutions don't work.*
> *You can't keep growing the department.*
> *The 'leg work' can be done better externally while we keep our strategy internally.*
> *That's the added value."*
> *-Alim Baydzhanov*

ABOUT AMD/ATI

AMD (formerly ATI) is a Canadian success story, developing and manufacturing high performance graphics technology since 1985.

On October 25, 2006, AMD and ATI joined forces, combining AMD's technology leadership in microprocessors with ATI's strengths in graphics, chipsets and consumer electronics.

On October 25, 2006, AMD and ATI joined forces, combining AMD's technology leadership in microprocessors with ATI's strengths in graphics, chipsets and consumer electronics.

Headquartered in Sunnyvale, California the new company has a combined workforce of approximately 16,000 employees worldwide.

ABOUT SENTRY METRICS INC.

Sentry Metrics was created to address the growing need for comprehensive Monitored Security Services for enterprise network environments.

Our philosophy is simple: build a talented team of certified security professionals, select the best tools the industry has to offer, and combine these resources into a centralized holistic environment to provide non-stop security services to our clients.

The culmination of these efforts is *The Sentry*, our centralized security repository that allows authorized clients to see a report card of their security posture, and to interact with our experts to understand the significance of events and appropriate responses. *The Sentry* allows our clients to raise the level of security with the knowledge that we are watching your networks 24 x 7.

Our secure data centre provides the central integrated environment for monitoring, correlating events, and providing metrics and recommendations for improvement. We cover seven domains of the spectrum of I.T. Security Services, as well as comprehensive Consulting Services for those requirements that fall outside of our services umbrella.

We invite you to browse our web site and to see how *The Sentry* can help you build your business with confidence!

www.sentrymetrics.com
info@sentrymetrics.com

CORPORATE HEADQUARTERS
1852 Queen Street East, Suite 200
Toronto ON, Canada
M4L 1H1
T: 416.488.2323
F: 416.482.8063