THE URGENT NEED FOR SECURITY INSTRUMENTATION

Richard Stiennon
Chief Research Analyst, IT-Harvest

DEPLOY SECURITY INSTRUMENTATION. YESTERDAY.

Security Instrumentation is both familiar and refreshingly different. It even deserves to be called a new category in the cybersecurity industry, and it is urgently needed. Perhaps the reason it caught my attention is that it recalls my experience in automotive manufacturing.

In the physical realm of automobiles and auto components, every process is modeled and every component undergoes testing from prototype all the way to final production. There are a series of NHTSA standard tests intended to ensure the performance and safety of every part of a car, from seatbelts to steering wheels.

In cybersecurity we have been missing that. Yes, we scan, patch, and conduct penetration tests but that doesn't really validate the effectiveness of our security tools, optimize our defenses, or improve our defenders. Attackers are constantly probing, developing new attack vectors, and exploiting weaknesses while our poorly optimized security tools do little more than eat up time, money, and resources while not adequately reducing risk.

The history of cybersecurity has evolved, always with a new set of products to address a new threat: antivirus for malware, firewalls for gateways, IDS/IPS to add a layer of signature and anomaly detection, SIEMs and log management to collect all those logs to try and correlate them into actionable events.

In more sophisticated environments we are even layering in threat hunting, incident response, security orchestration, and, lately, deception sensors everywhere to try to catch nefarious activity coming into, across or out of our environments.

Why is the answer always to add more tools?

A lot of time and money is spent deploying "next-gen" solutions, but we never go back and test the efficacy of the tools we already have in place. We cannot just "set and forget" security technologies; our infrastructures are extremely complex and simple misconfigurations can dramatically undercut our efforts. Security Instrumentation is the answer to the blind spots that will inevitably develop in our multi-layer defenses. Security Instrumentation is a game-changer for security staff and security leadership as well as CFOs, CEOs, boards, and anyone else that has a stake in the business, brand, and budget.

INSIDE SECURITY INSTRUMENTATION

The concept of Security Instrumentation actually seems pretty obvious: deploy sensors — generally as virtual machines, in a cloud, or on small dedicated hardware devices — across your network zones such as partner, desktop and server networks, DMZs, and Internet. These sensors live in your production environment and measure the efficacy of your security tools across network, endpoint, email, and cloud.

The sensors run a large and growing library of test behaviors against other sensors, operating safely and ensuring that your assets aren't targeted while measuring if the security tools that you purchased to protect those assets are working. There are never false positives because sensors communicate with each other. Either the test was successful, or it wasn't. There's no guesswork, and asset confidentiality, integrity, and availability aren't impacted.

But validating the security efficacy of your preventative controls isn't where Security Instrumentation stops. There are also integrations with security management solutions such as firewall managers, endpoint security managers, log managers, SIEMs and so on. These integrations provide precise and actionable details regarding incident detection and response.

For example, you may find that not only was a test not blocked, but perhaps it wasn't even detected. Or, it could be that a test was detected on a firewall manager but the events never made it to the SIEM. And all too often, events that do make it to the SIEM don't result in a notable or correlated event because of faulty configurations as well as problems around alerting, parsing, time stamping, routing etc., meaning that the likelihood of a human seeing and responding to the event is very low.

Security Instrumentation automatically identifies these issues and provides actionable, prescriptive information on how to mitigate them.

Best of all, once you apply the fix such as a signature, firewall rule change, endpoint security adjustment, or SIEM correlation rule, you can re-validate to ensure the changes worked and then continuously validate to ensure there isn't drift from a known good state. This automated, continuous validation results in end-to-end security measurement and improvement across your entire security stack.

To put in the most basic terms, Security Instrumentation is security quality control — tangible proof that you are getting your money's worth from security purchases (or not). It provides a feedback loop that leads to better resource allocation, process improvement, and configuration assurance. These improvements are equally effective at measuring and sharpening your people and processes as well.

With Security Instrumentation, you never have to worry about inadvertently taking down a production system with a dangerous test or something as simple as a credentialed scan. So-called attack and penetration testing is rarely authorized against production systems (because no one wants to risk disrupting business) so you are often stuck testing some environment that is only a facsimile of the real thing. With Security Instrumentation, you get all the benefits of ensuring your security is effective without any of the risks.

The need for Security Instrumentation is urgent because so many security environments are obviously flawed.

THE TIME FOR SECURITY INSTRUMENTATION IS NOW

The traditional approach of standards, compliance, and policies have not worked. How many retail organizations that have experienced breaches have been PCI compliant? Just about all of them. How many of the targets of cyber espionage had ISO, COBIT, or ITIL compliance programs? Most of them.

Security Instrumentation is something that can be deployed today with no impact or risk to the existing environment. It can immediately deliver value by:

Answering questions the CISO has such as:

- Is this particular technology that is coming up for renewal providing a benefit?
- How can I better invest my limited budget while increasing my resilience to cyberattack?
- What level of assurance do I have that we are not exposed to a particular attack methodology?

On top of that, the CISO is armed to respond to questions he or she receives from higher up in the organization. Today, that could include, "Someone just released exploit code against NSA-developed exploits like those seen with NotPetya and WannaCry. Are we protected against these?"

Another question often heard is, “What happened to that next generation widget that you got budget for last year? Is it working?”

A deployment of Security Instrumentation will answer all of these questions and finally put an IT security team on the same footing as manufacturing, finance, logistics and HR. All of those teams undergo regular audits and tests of processes. Until now, a CIO or CFO has had to rely on trusting their security team — and if worst comes to worst — replacing them after a breach. Security Instrumentation has the promise to break that cycle. It may identify a gap in your technology and justify that next layer, whether it be threat intelligence or Data Leak Prevention. But, in the meantime, it will assure you that the investments you have made are doing their job.

You should be prepared for the fact that a lot of your security processes are broken or not actually doing what they are supposed to do. But Security Instrumentation gives you the platform you need to start down the road of continuous improvement. The urgency is to get the bad news out of the way and start addressing the problems. Strive for incremental improvements. Now, you have the ability to measure and communicate those improvements. But some of the most exciting advantages of Security Instrumentation aren’t even those squarely related to classical perspectives on the role of security.

Because of continuous and empiric evidence regarding your true state of security effectiveness, your organization can make more exacting plans, embrace new initiatives, generate more precise budgets, and ultimately make your business more competitive. This makes you more competitive, all while Security Instrumentation is ensuring effective risk mitigation, brand, and revenue protection. The convergence of business and security — that’s why I think Security Instrumentation is so exciting.

WORK SMARTER

Security Instrumentation is the first methodology I have seen that can put a stop to the thrashing around I see at even some of the largest organizations. Security Instrumentation is a major leap ahead, not just an incremental improvement.

There are several large financial institutions that spend hundreds of millions of dollars a year on security and support thousands of highly paid security people. Every new development in the arms race between defenders and attackers means more people and more budget.

Everyone acknowledges that good security requires hard work. But hard work applied without testing and measurement is often wasted effort and wasted dollars. With Security Instrumentation, it’s not about working harder; It’s about working smarter. Thanks to Security Instrumentation, for the first time, organizations have the advantage in the ongoing cyber arms race.