

Mastering Security Analytics

Fast data analysis can stymie attacks and strengthen enterprise security. Does your team have the data smarts? [>>](#)

By Ericka Chickowski

Powered by **InformationWeek**
DARKReading

Mastering Security Analytics

Fast data analysis can stymie attacks and strengthen enterprise security. Does your team have the data smarts?

By **Ericka Chickowski**  @ErickaChick

Today's enterprise security tools have developed an ability to detect a plethora of anomalies and "events" that indicate an attack is underway. For most companies, the problem is interpreting all of that security data to identify sophisticated threats and eliminate them before a serious data loss occurs.

"We're sort of living in this alert-driven culture, but no one has the resources to respond to every alert," says Dmitri Alperovitch, co-founder and CTO of CrowdStrike, a security intelligence and analytics firm. "There are a lot of false positives, so not every alert is going to be prioritized."

Innovations within security software, appliances, and services have automated many

detection and blocking tasks, resulting in improved protection from next-generation firewalls and intrusion-prevention systems. But no matter how advanced a tool is, it will never block 100% of attacks.

That's why, even with so much sophisticated technology available today, brainpower remains the most effective tool in fighting advanced attacks. Smart analysts can connect the dots among different security alerts and logs, letting analysts hunt down and shut down the sneakiest of exploits. But as security data proliferates, these analysts are being snowed under.

Even the most highly skilled analysts can only sift through so much data per day before they become ineffective. What's more, there are only so many analysts out there —

and they don't come cheap.

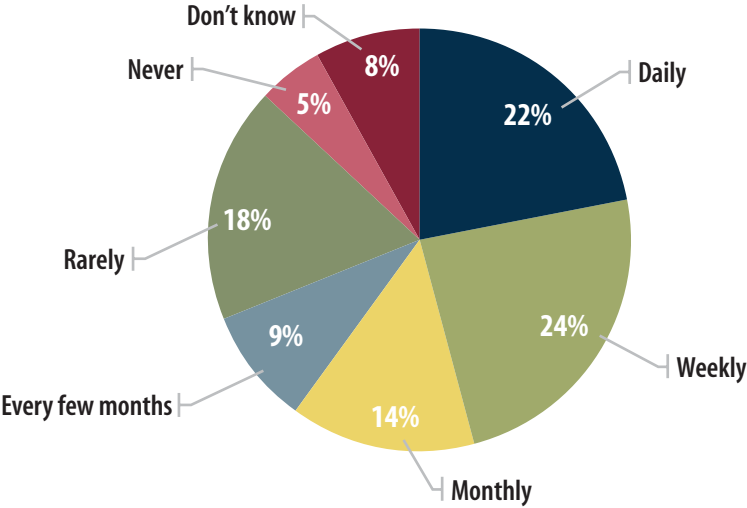
For most companies, then, it's not just a matter of hiring more analysts. "It's all about how do you maximize the efficiency of your human analysts — how you present them with the information that's most relevant to them and most actionable," Alperovitch says.

To do that, IT organizations must rethink the factors that drive their security intelligence and analysis. They need to find ways to digest data more efficiently and automate some of the easier correlations among data sets so that analysts have more time to focus on the complex ones.

There are a number of ways to improve data analysis, and much of it revolves around providing data in better context, automating data flows and mathematical analyses, and

Ad Hoc Data Queries

How often do you run ad hoc queries against your data?



Data: Dark Reading Threat Intelligence Survey of 337 business technology and security professionals using threat intelligence, June 2014 R8040914/9

improving the way data is presented to humans when it's decision-making time.

The Trouble With SIEM

Anyone who has been in IT security for a little while might stop at this point and ask, "Wait, isn't data analysis what security information and event management (SIEM) systems are for?"

When SIEM technology kicked off over a decade ago, the promise was that these platforms would become the catch-all system for storing and correlating secu-

rity data across the enterprise to help analysts stop attacks in their tracks. But that was a time when the corporate attack surface was fairly limited, and the volume of attacks was still manageable. Many of these SIEM systems had a pedigree in log management, and their underlying architecture was built in a time long before the nonrelational database revolutionized big data analysis. As a result, SIEM has a number of weaknesses that keep it from being an analytical superstar.

First, many SIEM platforms still can't pull

Damballa Resource Center



← Frost & Sullivan: Bot Detection Technology is Essential

DOWNLOAD NOW



← ESG Lab Spotlight: Damballa Failsafe with HP TippingPoint

DOWNLOAD NOW



← Damballa State of Infections Report – Q2 2014

DOWNLOAD NOW



← SANS Institute: Finding Advanced Threats Before Breach

DOWNLOAD NOW



DAMBALLA

in all of the necessary feeds to track attacks across the typical attack life cycle, or kill chain, which often spans endpoints, network resources, databases, and so on. Even when they can ingest data from, say, endpoint security systems, they are often unable to normalize it (meaning get the data sets into roughly the same format)

“The challenge is you have endpoint systems that don’t talk to log data and don’t talk to network data.”

— Craig Carpenter, AccessData

and pair it with related network security data that could help analysts correlate separate events into a single attack.

“The challenge is you have endpoint systems that don’t talk to log data and don’t talk to network data,” says Craig Carpenter of AccessData, a forensics and incident response vendor. “It may all be sitting in the SIEM, but it’s not being correlated. It’s not being translated into a singular language that the analyst can actually look at.”

In most cases, Carpenter adds, you’ll have two different teams looking at the data:

the network team and the endpoint team.

“And the two alerts don’t match to each other, so they look like completely different events to the analysts,” he says.

As the number of security data feeds increases with more specialized services and products — be they phishing and malware detection or external threat intelligence data — it only gets harder to map out a single attack across all of the different infrastructure touch points. It’s a case of too many alerts with little to no context.

“There’s no prioritization,” explains Alperovitch. “So it’s easy to say with hindsight that they should have connected the dots because there was one alert, but if there’s 5 million dots for you to connect, then it’s really, really hard for any organization to make sense of it all.”

For example, prior to its breach, the retailer Target did get an alert from its security tool, but it was lost in the noise of many other alerts coming in at a rate of hundreds a day.

Context Is Key

In order to hunt down today’s attacker, security teams must show how an attack

[SECURITY ANALYTICS]

Deeper security

Get the best protection for your network traffic — including SSL.

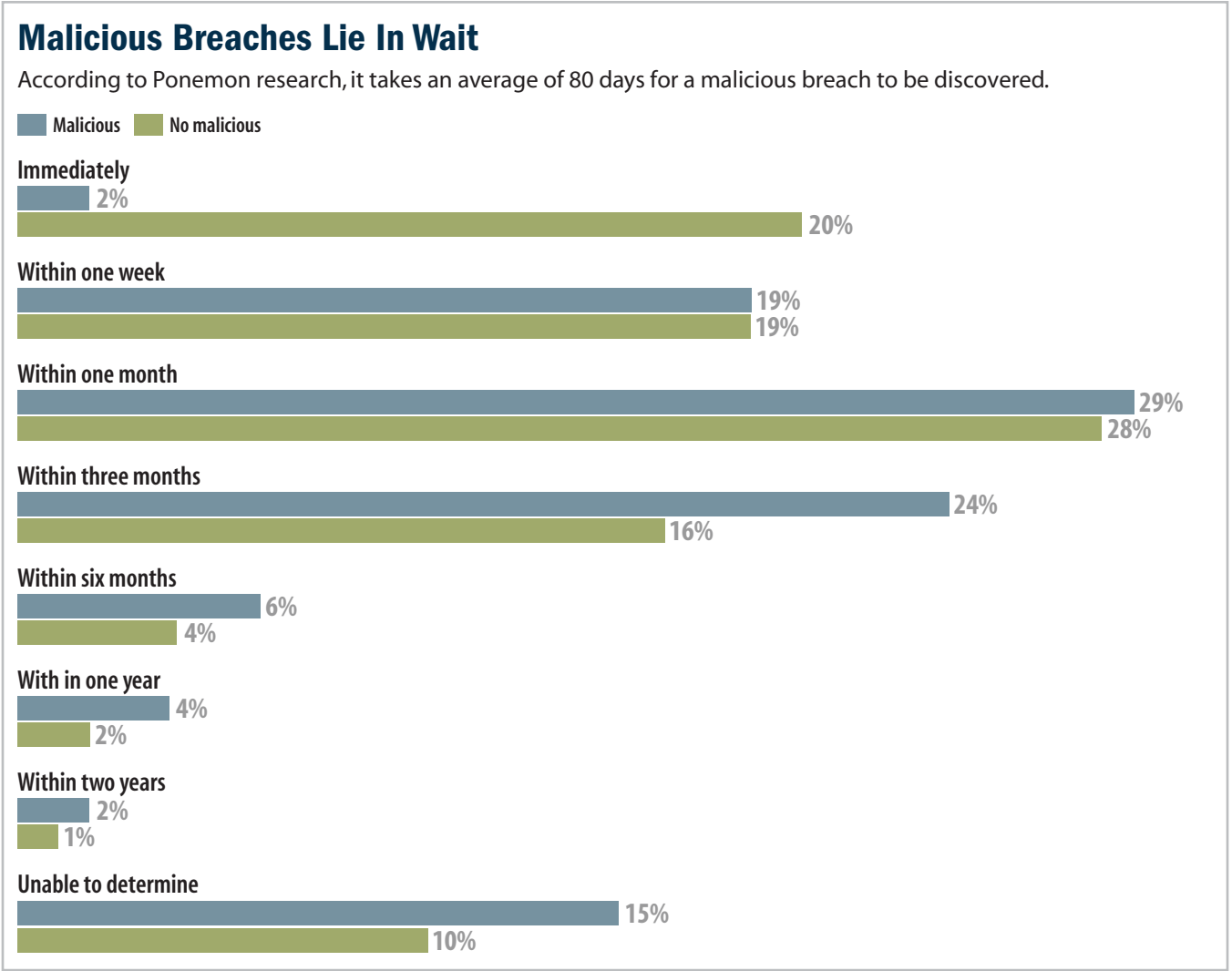
[Learn More](#)



progresses across all parts of their infrastructure. This is why context is so important for analysts. Most infiltrations into corporate networks are multistage, leaving forensic bread crumbs first on infected endpoints, then on network assets as the attacker starts scanning internally for additional ways to break identity and access management controls. Then signs might be left on high-value systems, such as databases, and then again on other areas of the network as the attacker exfiltrates the data.

IT teams must focus on setting up systems that let analysts know when activity on certain systems coincides with other activity on other systems. The better they are at that, the quicker analysts can spot patterns and indicators of compromise (IOCs). And the quicker they spot IOCs, the more likely they are to stop attacks from turning into breaches.

Security events need to not only be viewed in context with one another, but also in context with how IT architecture is set up and the relative importance of affected assets. Threat intelligence, which provides insight on how attackers behave across the web, may offer additional context. All of these aspects will help prioritize



Data: Ponemon

S7330913/2

risks, so that time-strapped analysts can know which threats to mitigate first when they're pressed for time.

This is where security analytics and security

intelligence vendors such as CrowdStrike, AccessData, RSA NetWitness, Splunk, Zetta-set, and Red Lambda have come to the table to provide the data crunching capability to

“work through the noise and separate out what’s really important,” says Alperovitch.

Adding automated analytical capabilities makes it easier to connect two seemingly unrelated events to “close the loop” and develop IOCs out of disparate security data, Carpenter says. While many analytics programs tempt IT with their machine-learning capabilities and math-

“We’re living in an alert-driven culture, but no one has the resources to respond to every alert.”

— Dmitri Alperovitch, CrowdStrike

ematical pattern matching, sometimes it’s the less sexy, simple features that can supercharge an analyst’s productivity.

“Some of the stuff that’s going to have the biggest bang for the buck is mundane, such as automating tasks that are simple but time-consuming for analysts,” Carpenter says.

For instance, a system that makes it easy to investigate alerts from five different systems on one console will save the analyst 10 to 30 minutes a day, Carpenter says. Multiply that times 50 to 100 ana-

lysts and “you’re talking about some major time and cost savings” — both direct costs and those related to mitigating risk.

The Power Of Analyst Brainpower

But buying a security analytics platform won’t automatically make forensics and incident response analysts more productive. There are many best practices that go into improving the human-powered analysis engine. In fact, organizations that have instituted some of these practices have built their own analysis, correlation, and visualization tools in-house to sift through data.

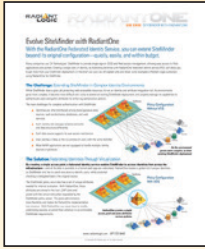
One of the first places to start, according to Andrew Hay, senior security research lead for OpenDNS, a provider of cloud-delivered security, is to flip the typical data collection paradigm on its head.

For many years, security teams have collected as much data as possible, just in case they needed it to answer security questions they hadn’t considered yet. But this type of mass collection led to a plethora of data they didn’t need, which only added to the noise. Instead, analysts should ask questions about what will help them spot IOCs more quickly, and then

Radiant Logic Resource Center



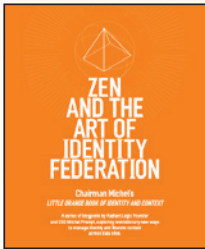
← **The Key to Seamless SSO**
DOWNLOAD NOW



← **Evolve SiteMinder With a Federated Identity Service**
DOWNLOAD NOW



← **Turn Identity into a Business Enabler, Not a Bottleneck**
DOWNLOAD NOW



← **Zen and the Art Of Identity Federation**
DOWNLOAD NOW

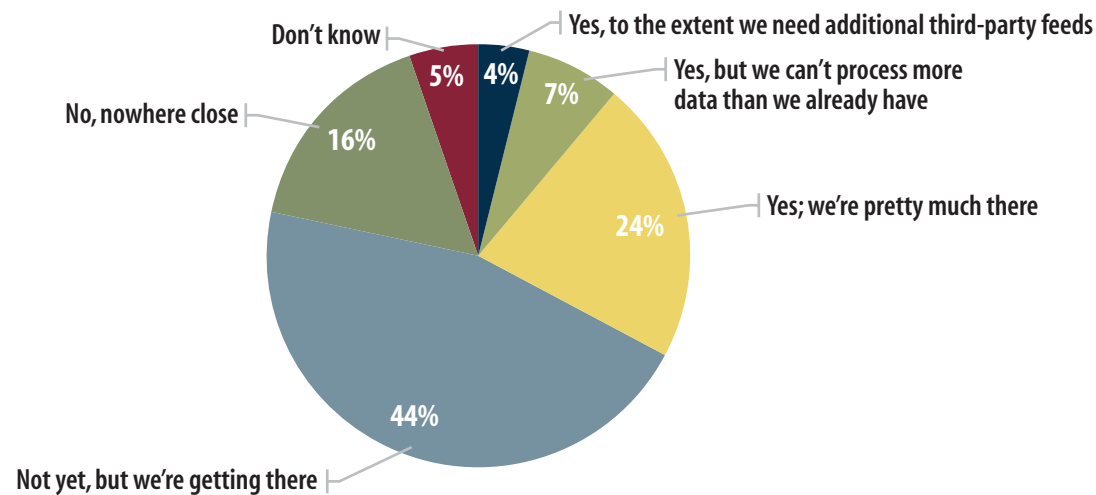


← **HDAP: The First Directory Built on Big Data Standards**
DOWNLOAD NOW



Inside Data

Have you fully realized the benefits of analyzing internally generated data?



Data: Dark Reading Threat Intelligence Survey of 337 business technology and security professionals using threat intelligence, June 2014 R8040914/6

model data collection around that.

"I'll admit I was a big proponent of collecting everything five or 10 years ago, but you can't possibly collect everything — at least not in a usable fashion," Hay says.

He points to mature organizations like Zions Bancorporation as enterprises that were "burned in the past by the collect-everything-and-figure-it-out-later approach [and now] are starting to ask the right questions." Several years ago, Zions built its own Hadoop-powered big data

repository and employed a data scientist to help the company query security data more effectively.

In addition to becoming more selective about what kind of data they collect, organizations should also consider how it's collected and stored.

"Start collecting data in a form that's very standard, even if it's only standard in your organization," says Jason Polancich, founder and chief architect for SurfWatch Labs. Data should be normalized so it can be more easily compared and linked



Employee and Event Log Monitoring Solutions

Free Downloads




[Implementing An Employee Monitoring Program](#)



[Monitoring Employee Productivity in a Roaming Workplace](#)



[Insider Threat Survey Report](#)

[More resources](#) 



Take a Spector 360 Test Drive and you could WIN a GoPro

[Get Started](#) 

— not just with security data, but with other systems such as logistics, financial performance, and business operations. These systems can provide context for how to prioritize assets that could impact which systems get the most attention from analysts.

Some of this contextual data and data

“Start collecting data in a form that’s very standard, even if it’s only standard in your organization.”

—Jason Polancich, SurfWatch Labs

comparison doesn’t need to be as precise as engineers usually try to make it. “Cyber-defense organizations can learn from Vegas,” Polancich says. “The oddsmakers do a really good job of putting together key data sets at a high level and making their decisions very quickly off of those key data points — and they’re right more often than not.”

This need to refine the information and improve the odds is why many organizations are diversifying their analyst team to include data scientists. But even organizations that can’t attract such a spe-

cialist could benefit from training their analyst teams on data science principles. Sharpening those skills could help teams build better in-house systems for querying data. And the added background could help them shop for systems that utilize complicated machine-learning and algorithmic principles.

Information Presentation

Whether using third-party security analytics platforms, in-house analytics, or a combination of both, organizations should also think about how they present information to analysts once the correlation work is done.

Data visualization can dramatically improve analyst productivity. An analyst can stare at a spreadsheet all day and not get the same kind of quick insight that a visual such as graphs or charts can provide.

Companies with large security organizations are buying data visualization platforms such as Tableau or Palantir in order to help analysts recognize data patterns faster and more efficiently. This need has also spurred OpenDNS to develop a free tool called OpenGraphiti, which is made

Box Resource Center



← An Alternative to Today's Distributed Content Security Chaos

DOWNLOAD NOW



← Securing Business Information in the Cloud

DOWNLOAD NOW



← A Fortune 100's Path to Secure Cloud Enablement

WATCH VIDEO



← Securing Business Information in the Cloud

DOWNLOAD NOW



← Splunk Boosts Day-to-Day Operational Intelligence, Secures its IP with Box

DOWNLOAD NOW



specifically for data scientists and security teams seeking to improve the effectiveness of their analysts.

There are various ways to visualize data, says Alperovitch, but even the most effective visualizations depend on the kind of team that's using them.

"For the intelligence team, it's critical to use link analysis types of systems like Palantir and Maltego to analyze relationships between threats," he says. "For SOC [security operations center] analysts, it's more important to get visualizations on their network and dig into alerts and see in a very easy-to-understand graphical fashion what's actually going on."

Even then, an analytics system may not be enough. Organizations should also employ threat intelligence analysis and what Alperovitch calls "hunt teams" to seek out active but hidden attacks on the network. This proactive approach has analyst teams constantly looking through data, trying to figure out whether malicious actors have already penetrated defenses, much like a security guard going around a building with a flashlight to make sure there's no

one really in the building, as opposed to sitting at a desk waiting for an alarm to go off.

If the attackers are really good at their illegal craft, "you aren't going to get an alert," Alperovitch warns.

Ericka Chickowski specializes in coverage of information technology and business innovation. Write to us at editors@darkreading.com

Copyright 2014 UBM LLC. All rights reserved.

[SECURITY ANALYTICS]

websense® RESOURCE CENTER



EXCLUSIVE INTEL FOR SECURITY STRATEGISTS - 2014 THREAT REPORT



USING ANOMALIES IN CRASH REPORTS TO DETECT UNKNOWN THREATS



FAST RESPONSES TO SECURITY INCIDENTS WITH THREAT MONITORING



ROADBLOCKS, REFRESH & RAISING THE HUMAN SECURITY IQ. -PONEMON REPORT



THE SEVEN STAGES OF ADVANCED THREATS

Download Now