Telin
by Telkom Indonesia

Whitepaper

Improving Web Security Intelligence

The importance of contextual data is growing, for protecting data as well as analyzing threats. How can companies improve and aggregate the security information they collect?

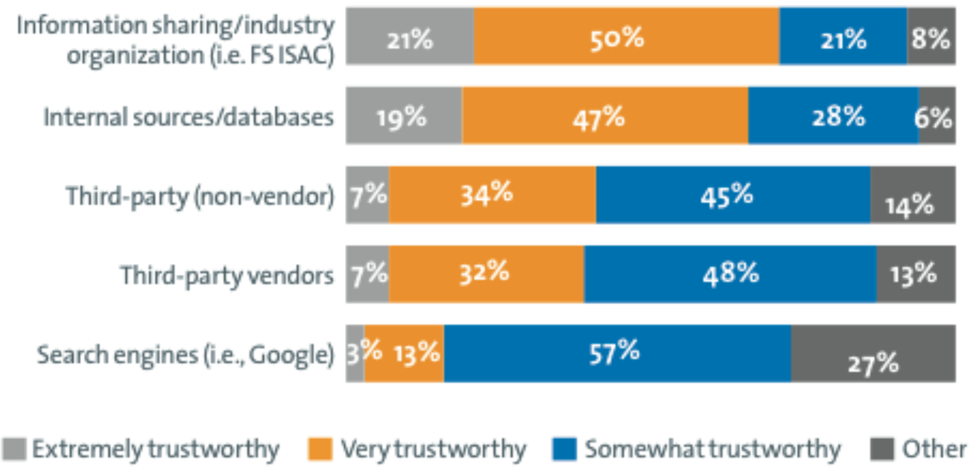
The importance of contextual data is growing, for protecting data as well as analyzing threats. How can companies improve and aggregate the security information they collect?

In a battle, perspective is everything. A soldier peering at an enemy platoon with a pair of binoculars has a narrower perspective than a helicopter pilot who can see enemy forces, the terrain and even oncoming weather. In the battle against hackers, Web security intelligence is becoming as important as military intelligence—and a wider perspective is increasingly crucial as well.

Compiling Web security intelligence, however, can be complex. It requires organizations to track a variety of issues, including malware signatures, Web application firewall rules, and graphical views of network traffic and threat descriptions. But like that soldier on the ground, most companies see only one perspective: attacks against themselves. They need context: Are specific attacks going on against other companies in my industry? Are generalized attacks occurring elsewhere on the Internet?

Increasingly, organizations understand the importance of the wider perspective. To get contextual data about Web security events, they rely on multiple sources of data, including third- party security vendors, industry organizations and even search engines. But according to a new IDG Research Services survey these methods are falling short. Organizations don't have a high level of trust in the sources of information they're using. They're looking for effective and efficient ways to aggregate the data, analyze it and use it to protect themselves.

The Most Trustworthy Web Security Intelligence Data Sources



SOURCE: IDG Research Services, October 2013

What’s Missing from Web Security Intelligence Strategies

Unfortunately, as security issues evolve, organizations’ intelligence efforts aren’t keeping up. Hackers are much better at sharing information than organizations are. Once hackers unmask a particular vulnerability, they willingly offer it for sale or simply share it via social media.

Organizations aren’t as agile. According to the survey results, the ongoing challenge of maintaining rules, signatures and patches remains daunting to most organizations. Just over half of the surveyed organizations update malware signatures and rules more than once a month. Fewer than half update patches and security rules more than once a month, and some update less than once every six months.

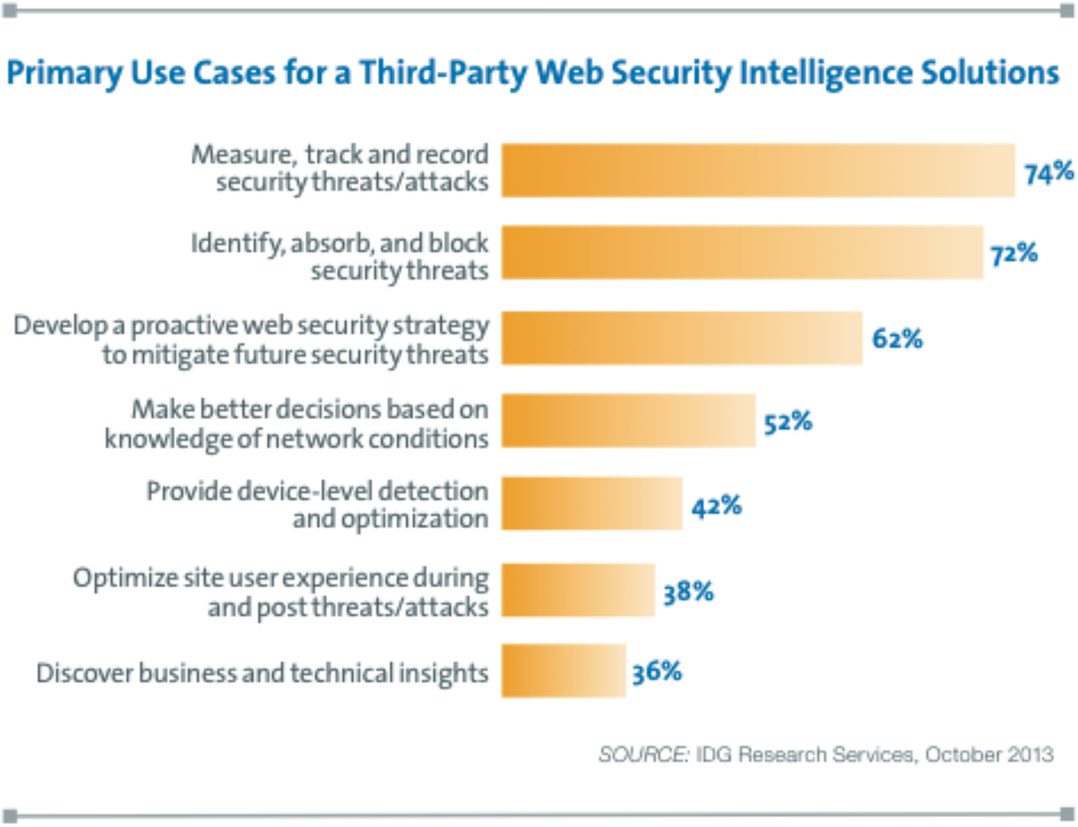
More troubling still: The threat landscape is changing quickly, and organizations are having difficulty keeping up. They believe that descriptions of threat actor tactics, a reputational scoring system and behavioral profiles are all important, but less than half of organizations have them.

Only by aggregating information across numerous attacks at many sites can organizations start to see trends emerge. For example, what ports are most often attacked? Which applications? From which countries do attacks originate most frequently? When are attacks most likely to occur? (Answer to the last question: Hackers have figured out that lunchtime is a great time to attack financial institutions.)

Of course, organizations today can subscribe to security updates from security vendors, industry organizations and the Web. But as the survey results show, the responding organizations don’t find these particularly helpful. (They’re using search engines 53 percent of the time, but 57 percent of the respondents said they’re only somewhat trustworthy.) For one thing, most organizations are loath to report they’ve had an attack. It’s a paradoxical situation: The information that organizations need most is the information that’s least likely to be shared. Even if they report it, it may take time for the information to be disseminated, so it often lacks immediacy.

How Web Security Intelligence Solutions Help

That’s why Web security intelligence solutions are so important. By looking at information from a variety of sources, organizations gain a contextual awareness that can help them protect themselves. For instance, if a retailer sees that another retailer has been attacked—even if the report keeps the vulnerable party anonymous — the first retailer can heighten its security posture. It’s the same concept as the helicopter pilot’s having a wider perspective than the lone soldier.



Organizations are using third-party intelligence solutions in a variety of ways, including the following:

- Measuring, tracking and recording security threats
- Identifying, absorbing and blocking security threats
- Developing a proactive Web security strategy to mitigate future threats
- Making better decisions based on knowledge of network conditions

For example, Telin's CDN uncovered the existence of a tool called Account checker. Working under the premise that users tend to use the same password at different online retailers, it's used by hackers to collect personally identifiable information—including passwords - which, in turn, is sold to other hackers. Then they attack other retailers, searching for the same customers in order to test the password theory. Alerted by Telin's CDN that such an effort was under way, retailers were able to monitor accounts for unusual usage and implement controls to block the attack.

How Telin CDN Helps

Turning to a third-party provider such as Telin goes a long way toward gaining the context that organization needs. Its platform touches every point on the Internet, enabling it to track IP addresses and maintain databases of suspicious ones. It even has the ability to peer into tools such as Account checker to see if customers are cited in it.

Another resource issue concerns the voluminous amounts of information relating to security issues. It must be stored, categorized and queried, and few organizations have query tools that can quickly assess such data for potential threats. Telin CDN has these capabilities.

In addition, when Telin CDN learns about attacks, it can disseminate the information quickly while masking the victim's identity. The reports it disseminates are both timely and reliable. Telin CDN is also developing tools to better identify suspicious IP addresses as well as to help organizations with online reputation management.

A subsidiary of PT Telekomunikasi Indonesia (Telkom), Tbk, Indonesia's state-owned telecommunication and network service provider, PT Telekomunikasi Indonesia International (Telin) is the World's hub for Telecommunication, Information, Media, Edutainment and Services (TIMES) focuses on international telecommunication business and serves as Telkom's business arms in managing and developing its business lines abroad.

Today's customers want a reliable and trusted partner who has both technical capabilities and deep understanding of their business requirements as well as the business objectives. Whether it is an overseas company who wants to tap into Indonesia's mobile and telecommunication potential market or vice-versa, a local business who needs to broaden its network internationally or share its contents globally, Telin is the perfect telecommunication partner to help reach your business goals.

For more information about Telin's products, services and solutions:

Telkom Indonesia International (Telin)
Menara Jamsostek North Tower, 24th floor
Jl. Jendral Gatot Subroto Street, Kav 36,
Jakarta 12710 Indonesia
Phone: +62 21 2995 2300
Fax: +62 21 5296 2358

Email: info@telin.co.id
Website: www.telin.co.id