ALIEN VAULT

BLACK HAT 2016

Threat Intelligence Déjà Vu

Section 1

Executive Summary

Effectively utilizing threat intelligence is as much about having the right processes in place as it is about choosing the most appropriate technologies. How to best incorporate threat intelligence is an area that many enterprises have been trying to wrap their heads around for some time. Whilst we are seeing a growing level of maturity at many organizations, the question still remains as critical and relevant.

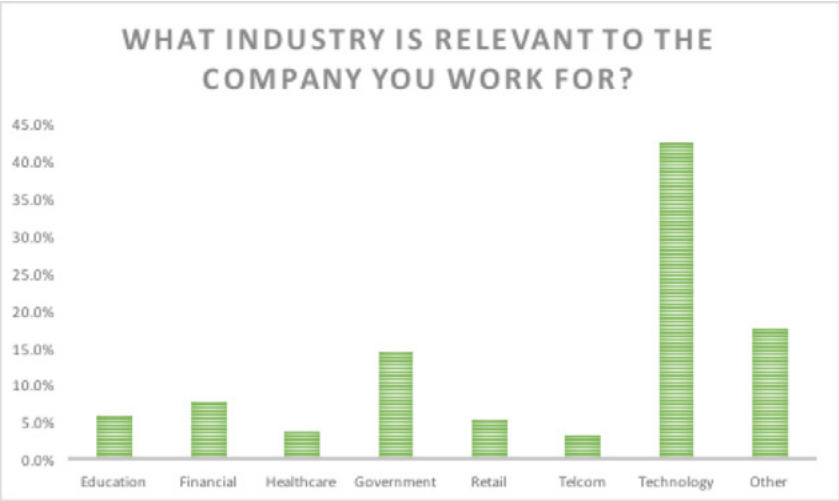
1.1 Key Findings

- Security teams are growing, as the number of security incidents over the past year have also reportedly increased.
- An overwhelming majority of respondents (76%) believe that the security industry has a moral obligation to share threat intelligence.
- There has been a gradual increase in the number of respondents sharing threat data publicly as well as amongst trusted peers. The largest jump has been in the adoption of crowdsourced platforms, which increased by almost five times since 2015.
- An overwhelming majority of respondents (69%) stated that incorporating threat intelligence had made it easier for security teams to respond to incidents.

1.2 Methodology and Scope

This report is based on the professional experience of the author (a former security consultant and industry analyst), in conjunction with a survey conducted at Black Hat 2016 in Las Vegas. The survey results consist of 222 responses from security professionals in attendance.

The majority of attendees, nearly 45%, work in the technology sector. A significant number of participants selected 'government' or 'other,' while the remaining respondents were distributed across a range of industry verticals.



In terms of the size of company that respondents worked for, it was an almost even split. Half of the respondents work for larger enterprises with over 2000 employees, while the remaining 50% work for companies that are smaller in size. Of the latter, mid-size enterprises (500-2000 employees) was the largest segment at 21 percent. Overall, this distribution gave us a balanced set of answers from a representative sample of employees from small, medium, and large enterprises.

This report was written by Javvad Malik, security advocate, AlienVault. Any questions about the methodology or findings should be addressed to him at jmalik@alienvault.com.

Section 2

The Questions

Survey participants were asked the following questions:

1. In the last two years, my security / IT team has:

a. Decreased in size

b. Stayed the same

c. Increased in size

2. Would you say your security team has seen:

a. A decrease in security incidents in the past year

b. About the same number of security incidents in the past year

c. An increase in security incidents in the past year

3. What sources of threat intelligence do you rely on? (Select all that apply)

a. Our own detection processes

b. Trusted peers

c. Paid subscription service

d. Government / government agencies

e. Crowdsourced / Open Source

f. Blogs / online forums

g. We do not use threat intelligence

4. What do you do with threat intelligence? (Select all that apply)

a. Protect my organization's network from threats

b. Obtain insights my organization is not capable of finding on its own

c. Use it to network with my peers

d. Manually ingest indicators of compromise

e. Use it for incident response purposes

f. Collect it for informational purposes only

5. As a security professional, there is a moral responsibility for the industry to share threat intelligence:

a. Disagree

b. Neutral

c. Agree

6. When you discover a threat, with whom do you share it? (select all that apply)

a. Trusted peers / closed community

b. Public

c. Government / government agencies

d. No one

e. Internally

f. With crowdsourced / open source platforms

7. Threat intelligence has:

a. Made it easier for my security team to respond to security incidents

b. Not had a significant impact on response time for my security team

c. Made it more difficult for my security team to respond to security incidents

8. Do you trust threat intelligence from (select all that apply):

a. Security vendors

b. Public threat feeds

c. Government threat feeds

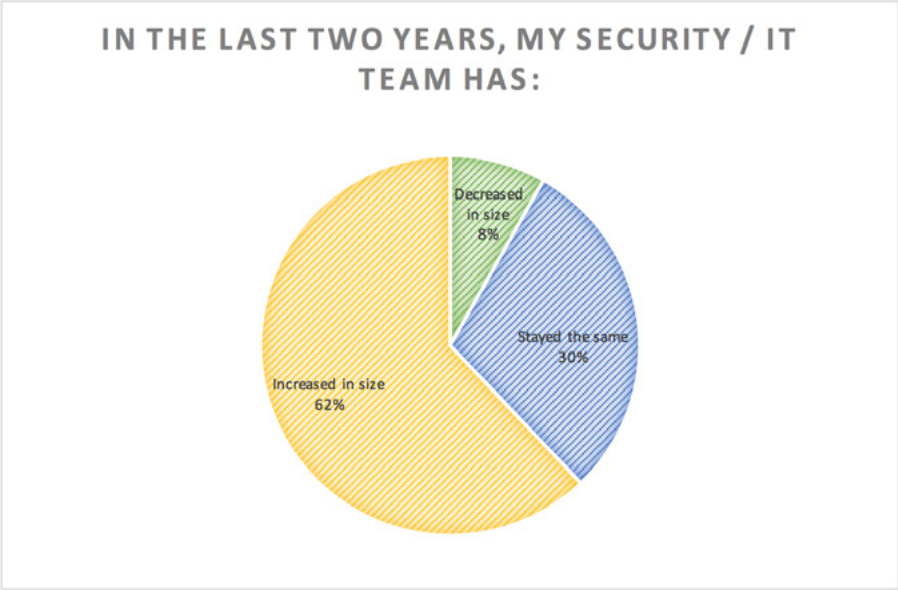
d. Crowd-sourced threat intelligence platforms

e. Peers

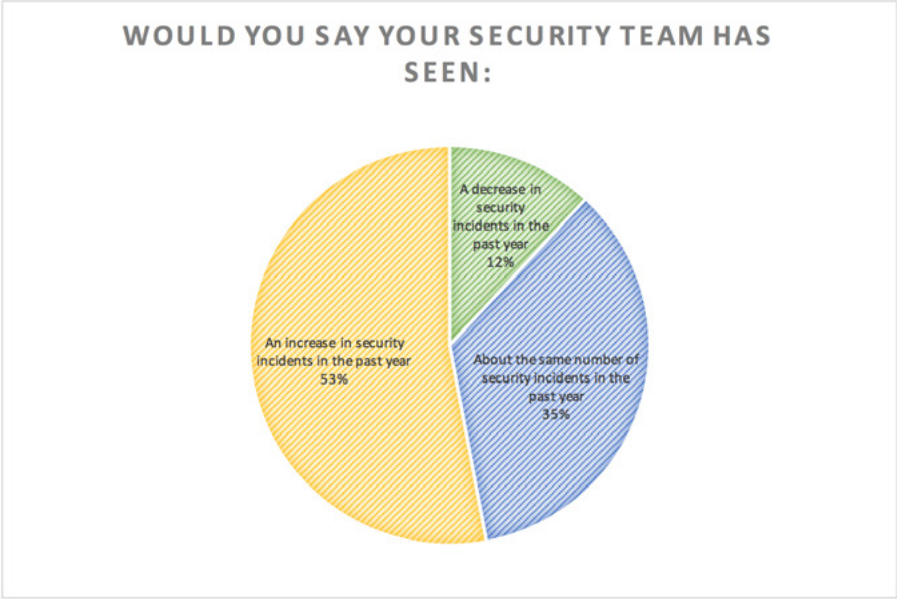
f. My own internal sources

2.1 Growth, Shrinkage, or Stability?

The majority of respondents (62%) stated that over the last two years, their security teams had increased in size. Overall, this is not surprising, as many studies have pointed out both the shortage of security skills as well as the fact that more companies are increasing their investment in security.



The next question gives us some insight into one of the drivers behind the growth of security teams. When we asked participants about the number of incidents their team had seen in the past year, 53% stated they'd observed an increase in security incidents.



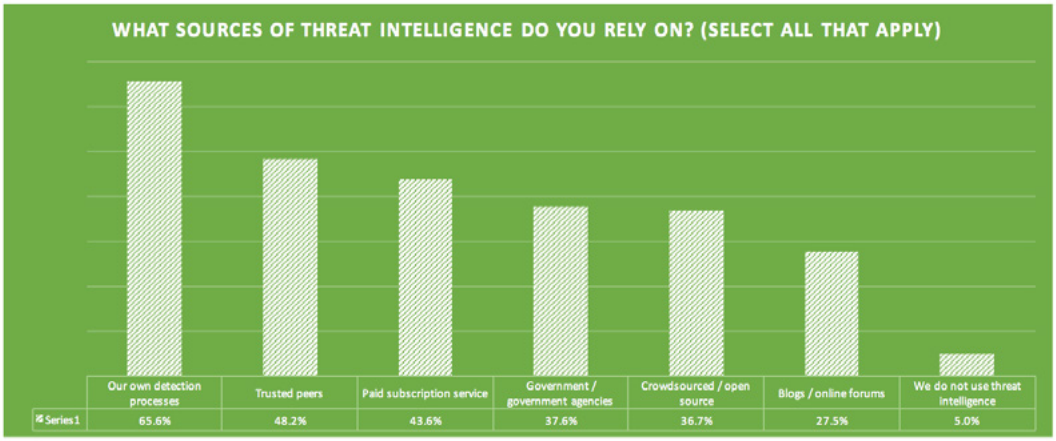
While the increase in observed incidents could simply be correlated with having larger security teams to monitor systems, there are more likely a combination of factors contributing toward this. The strongest likelihood is that enterprises are now actively paying more attention to IT security. With high-profile security incidents commonly reported in the mainstream media, many boardrooms are now taking more of an interest in ensuring that their company doesn't make the headlines for the wrong reasons.

It is also very possible that the actual number of incidents hasn't necessarily increased, but rather that an improvement in detection capabilities and a stronger appetite to identify malicious behavior has led to more incidents being discovered – and that previously enterprises simply suffered from a case of "inattentional blindness" that prevented them from noticing security incidents.

2.2 Sources of Threat Intelligence

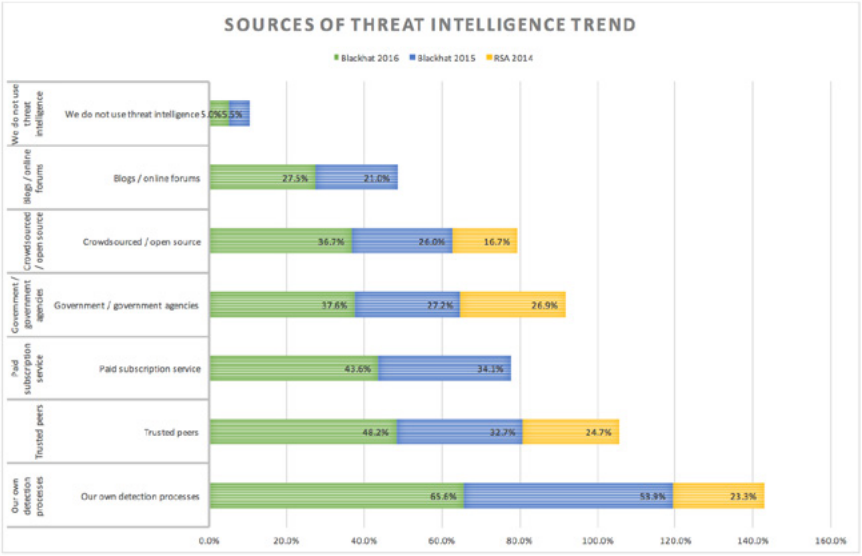
When it comes to threat intelligence, the intelligence is only as good as its sources. The majority of participants responded that they relied on their own internal detection processes. This is an encouraging result as it indicates that enterprises are looking at the most relevant datasets first (their own), and that they have the necessary in-house skills to do so.

With the exception of the 5% of respondents who stated that they do not use threat intelligence, there was a pretty even spread as to what sources were consumed.

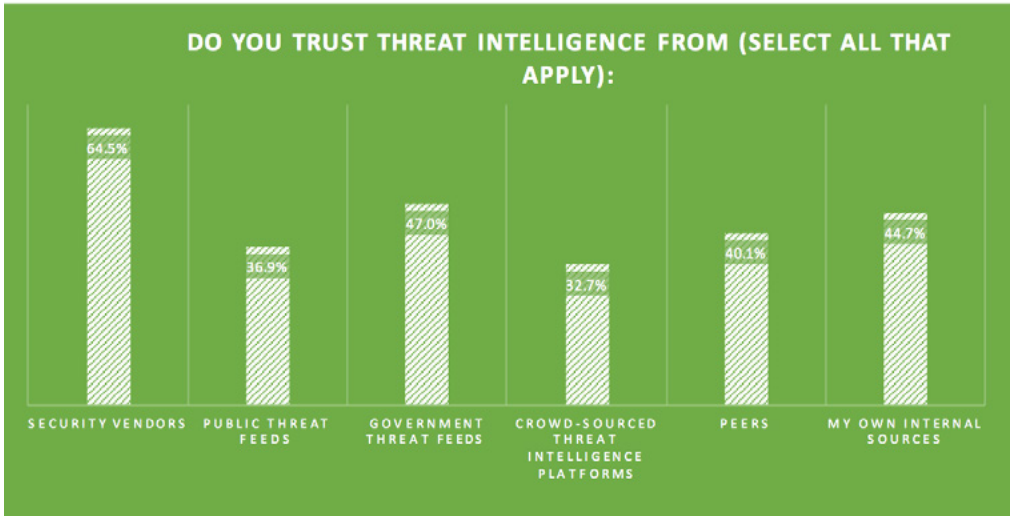


One of the reasons for this range is that threat intelligence can be additive in nature. A company can rely primarily on its own internal detection processes, but can choose to also complement this with, say, a government feed, or by pulling data from a crowdsourced platform, with little overlap in the data obtained. By referencing more threat intelligence sources, a company can gain a comprehensive view of the overall threat landscape.

This theory is supported by a trend we've witnessed over the last few years by asking the same question as this at Black Hat 2015 and RSA 2014. The results show that year-over-year, the range of threat intelligence sources that companies rely on has consistently increased.

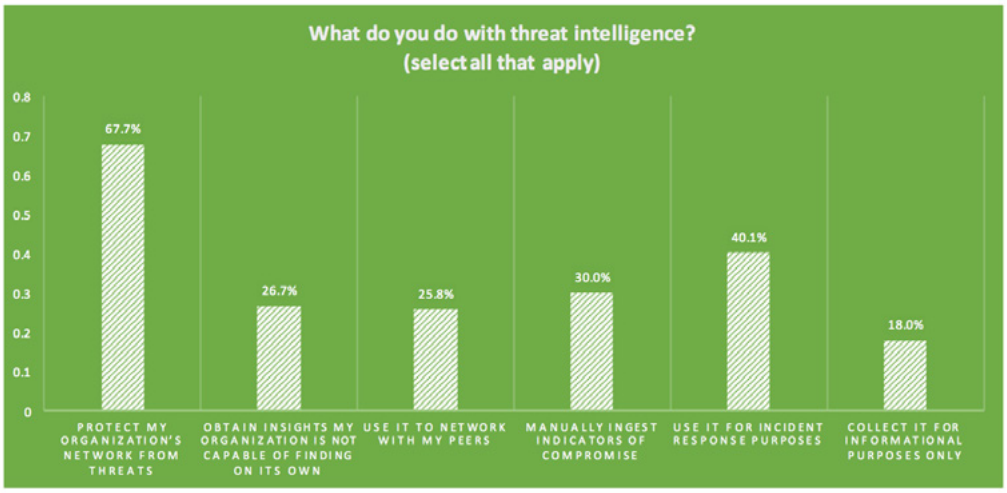


Additionally, we asked what sources of threat intelligence enterprises trust the most. Security vendors scored highest in trust, surprisingly ranking even higher than an enterprise's own internal sources. Government feeds scored higher than peers.



2.3 Using Threat Intelligence

Obtaining threat intelligence from reliable sources is one thing; however, knowing how to put it to use is quite another matter.

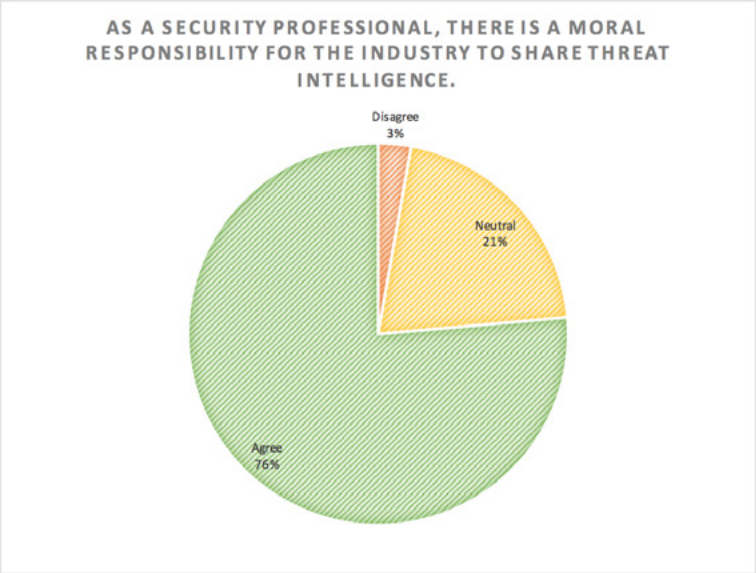


The majority of participants claim to use threat intelligence to protect their organizations from threats. However, many attendees identified challenges related to methods for utilizing this data, with approaches ranging from manual reviews, to automated workflows. This is somewhat reflected in the 30% who responded that they manually ingest indicators of compromise.

Other uses were mainly reactive or passive, using threat intelligence primarily for informational purposes, or for responding only after an incident has occurred.

2.4 Threat Sharing: A Moral Obligation

An overwhelming majority of respondents, 76% to be exact, believe that, as security professionals, the industry has a moral obligation to share threat intelligence with others. Only 3% disagreed with the statement, while 21% opted to remain neutral.



Threat intelligence is recognized as a key aspect of security for enterprises, as well as for vendors. It is used to improve protection capabilities, enhance threat detection, and also play a role in incident response.

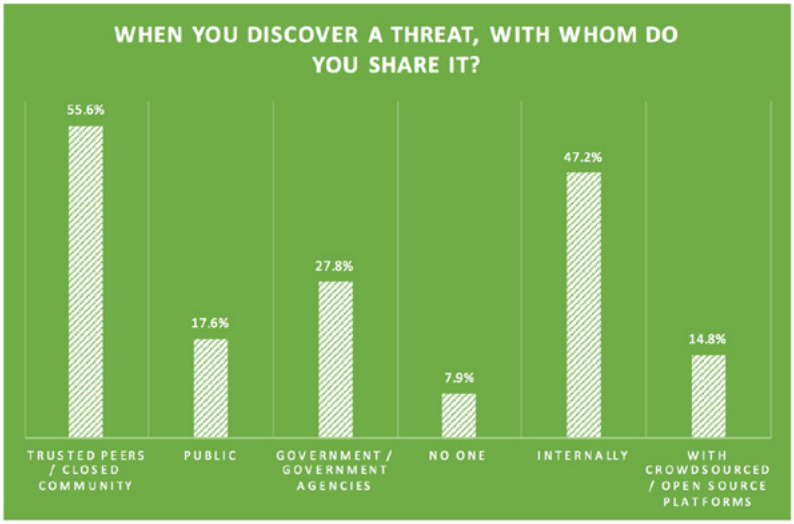
An oft-quoted statement in the security industry is taken from a statement the IRA made after then Prime Minister Margaret Thatcher narrowly escaped the Brighton hotel bombing in 1984:

“Remember we only have to be lucky once. You will have to be lucky always.”

While historically this analogy could have extended to the security industry, threat intelligence now flips the dynamic around. When a malicious actor utilizes a new method or technique against an enterprise, effective threat intelligence sharing can mean that the same technique cannot be successfully utilized against others.

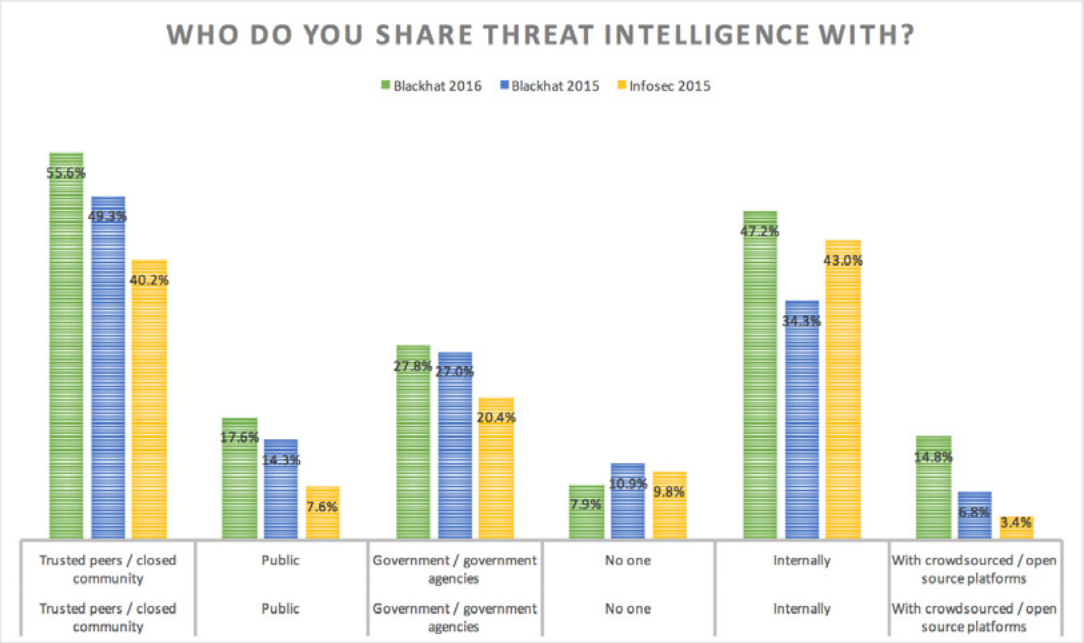
Although there is no requirement or mandate for companies to share threat intelligence, many professionals believe that if they were to observe an active exploit, it would be their duty to share it with others, so everyone could benefit from the combined capabilities. Not only would this be an effective way to decrease the ROI for attackers, but it also helps in addressing the skills shortage within the industry, as it allows even small teams to leverage the collective knowledge of a global workforce.

But how does this moral obligation pan out in reality? Only 8% of respondents stated that they did not share threat intelligence with anyone. 56% stated that they shared threat data with trusted peers or a closed community, and only 18% shared threat data publicly.



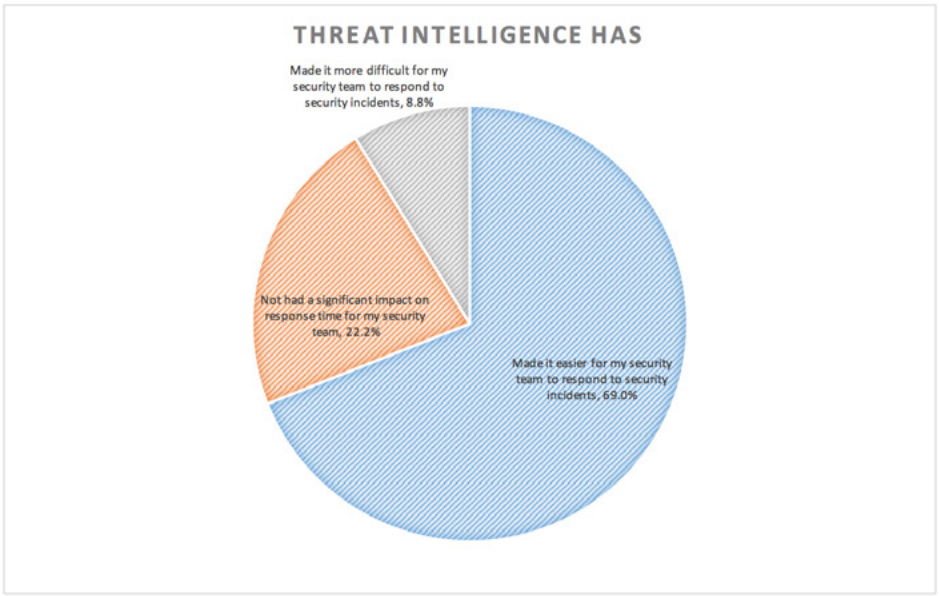
Looking back over the last year, this response extends a trend we saw when we asked these questions of participants at Black Hat 2015 and Infosec 2015: a gradual increase in the number of respondents sharing threat data publicly as well as amongst trusted peers.

The largest jump has been in the adoption of crowdsourced platforms, which increased by almost five times since last year. We expect to see this trend continue to develop as confidence in threat sharing platforms increases, and as the trusted peer groups of security professionals expands.



2.5 Benefits of Threat Intelligence

While many claims can be made about the benefits of threat intelligence, only enterprises can validate the true effectiveness.



69% of participants stated that incorporating threat intelligence had made it easier for security teams to respond to incidents.

22% did not witness a significant impact, whilst surprisingly 9% stated that threat intelligence made it more difficult for their security teams to respond to incidents. We assume that a portion of these responses may include those participants that didn't use threat intelligence, or only consumed it for informational purposes. It may also be possible that a lack of integrated systems, or available APIs, resulted in enterprises not being able to fully realize the benefits.

As threat intelligence capabilities and offerings become more sophisticated, and as internal capabilities to use it effectively improve, we will likely see threat intelligence play an increasing role in helping enterprises respond to security incidents.

SECTION 3

Conclusions

Security is ever-evolving and threat intelligence is still a maturing discipline for enterprises. As investments in threat detection capabilities increase, the result is typically greater visibility into active threats.

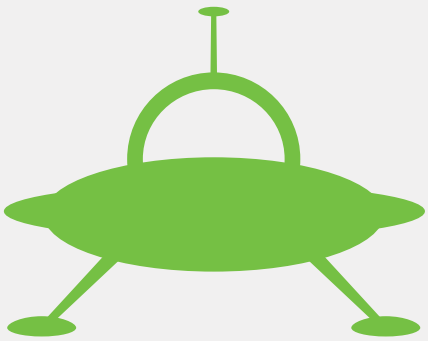
We've seen a gradual increase in the deployment and usage of threat intelligence. In particular, as the number of avenues to share threat data has increased, organizations have been able to share in accordance with the methods best-suited to them.

While the perceived and actual benefits of threat intelligence are reported as positive, there is still some apprehension around sharing and consuming public sources of data – with many respondents opting to primarily share only amongst trusted peers. However, even with that being said, the trend over the past few years has been toward more sharing, and this is a trend that we expect will continue.

Looking forward, we expect not only that threat sharing will increase, but that methods for applying threat intelligence will evolve as well.

Currently, many enterprises use threat intelligence for informational or reactive purposes, the forward-looking trend points toward more proactive uses for threat intelligence.

We also see that, as security teams' capabilities and maturity improves, more organizations are sharing threat intelligence. The rise of threat sharing allows the security industry to collaboratively defend against malicious attacks with greater agility and efficiency, enabling the benefits of threat intelligence to be experienced by not only the largest of enterprises, but even the smallest of IT teams.



About AlienVault

AlienVault has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management, with the power of AlienVault's Open Threat Exchange, the world's largest crowdsourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures.