

THREAT INTELLIGENCE REALITIES



Threat intelligence sharing has received a lot of attention over the past 12 months due to industry messages and proposed government legislation for public/private threat intelligence sharing. Enterprises are embracing threat intelligence programs, but these efforts remain immature and fraught with operational problems. Furthermore, most large organizations are focused on threat intelligence consumption rather than threat intelligence sharing. Vast improvements in threat intelligence standards, timeliness, contextualization, and operations are necessary before the cybersecurity community can truly benefit from the threat intelligence sharing vision being promoted by industry organizations and government agencies.

Top Objectives of Organizations' Threat **Intelligence Programs**

Enterprise organizations have several objectives for their threat intelligence programs, but the general goal is to improve security efficacy and operational efficiency.



38%

Improve automated incident prevention



the cybersecurity activities of smaller units

Establish a central threat intelligence service to help guide



25%

Improve incident response

Improve incident detection

Length of Time Threat Intelligence Programs Have Been in Place

intelligence programs, these efforts are fairly immature.

Although many organizations have established threat



of enterprises have had their threat intelligence programs in place for less than 2 years.



Analyzing External Threat Intelligence Given the relative immaturity of threat intelligence programs, it is no surprise that organizations have encountered numerous challenges. CISOs will need to invest ample resources to improve threat

Challenges Experienced with Collecting and

operationalize their threat intelligence programs. REPORTED CHALLENGES EXPERIENCED:

intelligence skills and automate threat intelligence collection, processing, and analysis in order to truly

32% of organizations have inadvertently blocked legitimate traffic as a result of a problem with threat intelligence collection/analysis.



32% say threat intelligence is collected and analyzed by different individuals and

tools, so it is difficult to get a holistic picture of internal and external threats.



26% say threat intelligence does not come in a standard data format, requiring

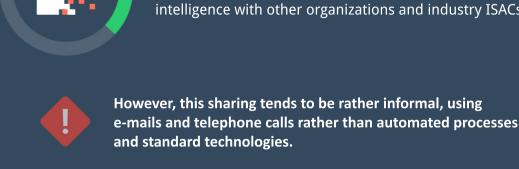
staff to develop tools or use manual processes to normalize the data.

26% say threat intelligence sharing is immature and requires too much manual labor and customization to get maximum value out of the process.



37% of organizations regularly share internally derived threat intelligence with other organizations and industry ISACs.

Sharing of Internally Derived Threat Intelligence with



Other Organizations/Industry ISACs

and standard technologies.

The Bigger Truth

Organizations have aggressive plans to improve their threat intelligence programs. Many plan to increase threat intelligence program spending, and collect and analyze more internal and external data. Enterprises are also committed to threat intelligence standards and are willing to share

internally derived data in public and private threat intelligence sharing communities. CISOs plan to increase their threat intelligence consumption and sharing, but they still have a lot of work ahead.





© 2015 by The Enterprise Strategy Group, Inc. All Rights Reserved.

contact@esg-global.com



Enterprise Strategy Group is an integrated IT research, analysis, and strategy firm that is world

renowned for providing actionable insight and intelligence to the global IT community.