 Business Impact Brief

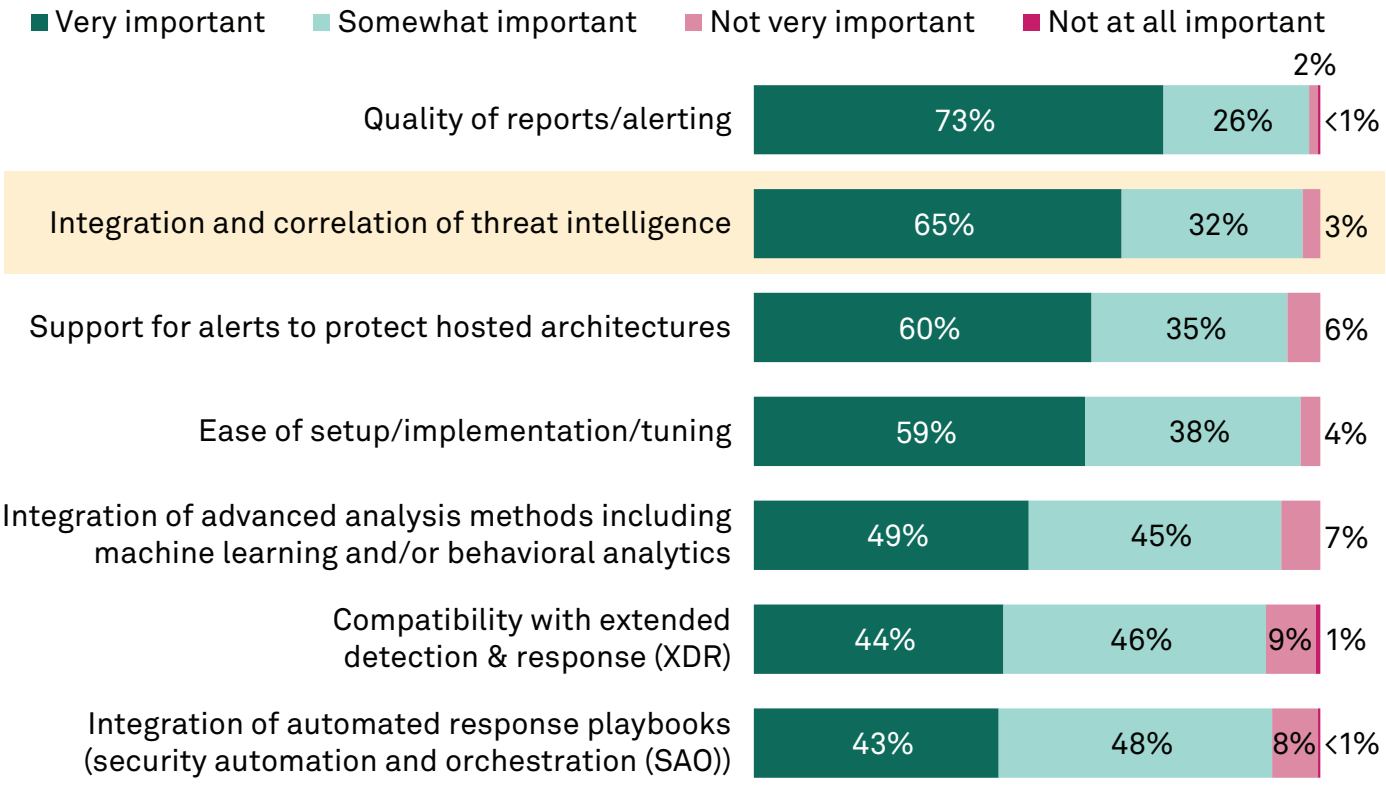
Security Teams Need Threat Intelligence Integration

The 451 Take

In the past several months, a seemingly unending sequence of high-profile, often high-impact cyberattacks has elevated the criticality of threat visibility for information security teams. This demand is reflected in the importance that enterprise security professionals place on the integration of threat intelligence into their security operations – and the technologies on which those operations depend.

In 451 Research's Voice of the Enterprise: Information Security, Vendor Evaluations 2021 study, nearly two-thirds (65%) of survey respondents cited the integration and correlation of threat intelligence in security operations as 'very important' in the selection of a SIEM (security information & event management) vendor.

Integration of Threat Intelligence Is Critical for Enterprises



Q: How would you rate the level of importance of each of the following attributes when selecting a SIEM (security information & event management) vendor?

Base: Respondents currently using SIEM, abbreviated fielding (n=258-261)

Source: 451 Research's Voice of the Enterprise: Information Security, Vendor Evaluations 2021

Business Impact

No credible security strategy can be built without threat intelligence. 451 Research findings such as the data above speak to a foundational principle of security: you cannot manage what you don't know. For security teams, threat intelligence is a fundamental source of this knowledge. It is the primary means of understanding what attackers are actually targeting, how they are targeting it, and how an organization can recognize how it's being targeted. That means threat intelligence is essential to knowing how best to apply limited resources in people, expertise and investments in countermeasures and technology.

A structured approach to managing threat intelligence is essential to making it actionable. As valuable as threat intelligence is, it can also be overwhelming. A great many sources cover a wide range of adversarial activity, from open source intelligence (OSINT) to curated feeds and finished reports. Even further compounding the load is the fact that sources often overlap. Multiple observers frequently report on the same activity, often using differing terminology for the same actors, attacks or other identifiers. Normalization and prioritization of all this data is essential to focus and identify the most significant findings. Threat intelligence management systems can bring the order needed to realize value from all this insight, correlating findings not only to high-value assets, but to specific activity targeting those assets. This enables security teams to realize their threat intelligence objectives: prioritizing response and making informed investments.

A structured approach to threat intelligence enables teams and communities of interest to learn from each other. Organizations with similar risks can benefit from knowing that which has targeted one, or many, of such a group, in order to prioritize their own efforts and learn from the successes of their peers and the challenges they face. Sharing intelligence within an organization should be as seamless as possible, while sharing with third parties requires confidence in the security and discretion applied. Both require a consistent approach to intelligence governance and the ability to share valuable content securely, protecting organizational interests while making findings as available as possible to those who can best benefit from them.

Organizations should discover and make the most of as many resources as they can. What exactly contributes to threat intelligence? Many more sources than some might think. It isn't just OSINT that may be freely available; internal sources may contribute as well. Examples worth exploring include internal incident reports, trouble tickets and service desk cases, suspicious email, and unexpected issues in IT performance or availability. All these can enhance the context of threat intelligence to call out threats that may otherwise go unrecognized and also better recognize future events. Together with the findings of peer organizations or others facing similar exposures, this more comprehensive view of the opportunity can further help organizations build maturity in intelligence-informed security operations, making security investments better informed, more effective and – crucially – more credible.

Looking Ahead

The high-profile attacks and unprecedented cyber activity of the past several months have significantly raised the value of threat intelligence. Geopolitical instability has more recently heightened its value even further. We expect these trends to result in greatly increased volumes of threat intelligence requiring systematic management.

Taming this volume of data and the complexity of its variety will require even further application of artificial intelligence and machine learning to help analysts already stretched thin by demand, as well as increase the speed and efficiency of realizing actionable findings, and their correlation to an increasingly complex tech environment. Increased application of automation will also be required to enhance the efficiency and effectiveness of response.

Because the threats to one organization may very well target others facing similar risks, we also expect escalating cyber activity to further increase demand for resources that can share threat intelligence across organizations with confidence and security. These include information sharing and analysis organizations (ISAOs) and centers (ISACs) requiring solutions built for purpose.