Five Threat Intelligence Traps TO AVOID »»»

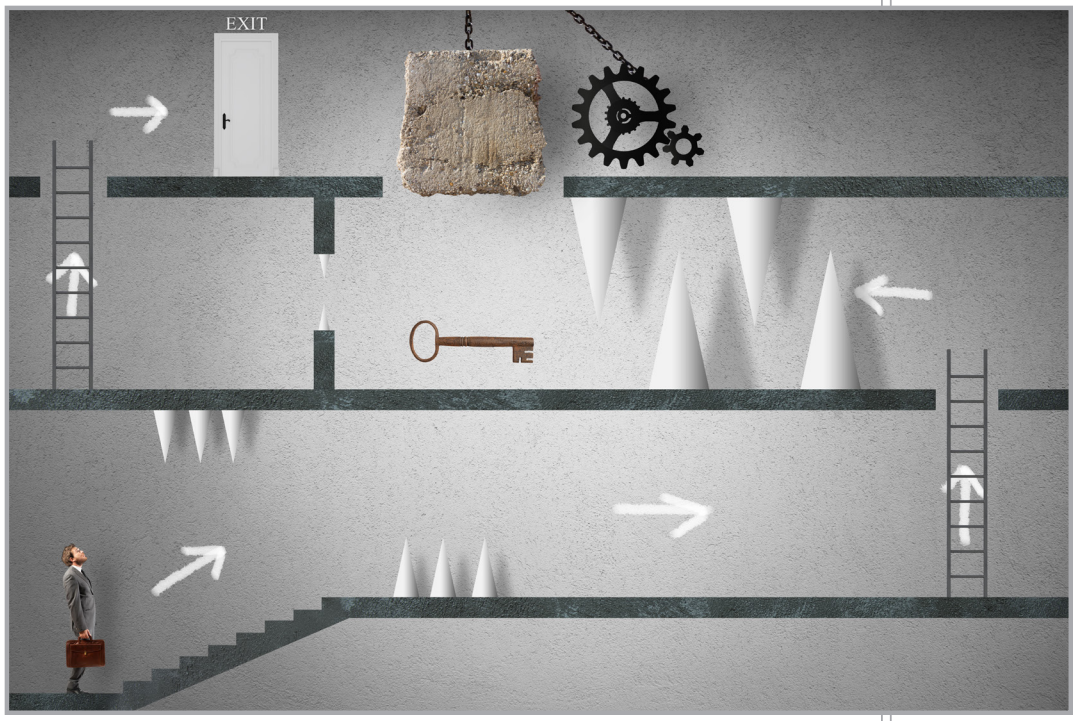
UBM Tech

Recent events, which include gigantic data breaches affecting retailers, health care organizations and government agencies, have shown just how challenging today's cyberthreat landscape has become. Organizations have to defend themselves against an increasingly diverse set of threats while managing an ever-expanding universe of devices, users and data all fluidly entering and leaving the network. The benefits of including threat intelligence in the defensive arsenal are well established, but in most organizations, it is frequently misunderstood and underutilized.

"Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats," Forrester Research said in a recent paper.

As a concept, threat intelligence makes a lot of sense, as it merges threat information collected from various data sources to identify adversaries, as well as their campaigns, attack patterns and potential threat indicators. Threat intelligence doesn't just combine logs and network artifacts into one feed; it derives information regarding attack techniques and indicators after analyzing a variety of data sources, which can include forward-looking data such as underground sources. With threat intelligence, organizations can develop effective responses against existing and emerging threats.

Organizations should learn from the common pitfalls encountered by peers to ensure they get the most out of their investment when incorporating threat intelligence into their security programs. Mistakes include not aligning threat intelligence efforts with strategic business goals, relying on poor or incomplete data sources, not involving senior executives, missing context in intelligence sources, and focusing too much on blocking commodity attacks. This paper discusses five key traps to avoid.



TRAP 1 Lacking a Defined Intelligence Program and Processes

Organizations that have made significant security investments over the years are now drowning in data and need to prioritize important alerts above others. Security intelligence enables organizations to identify key threats and allocate resources to align with those threats. However, as is the case whenever planning is an afterthought, if intelligence initiatives are launched independently, the overall program will lack the coherence and unified objectives needed to ensure best results. That's why organizations should create a defined intelligence program and update it as their programs expand and mature, and as needs change.

Forrester noted that if threat intelligence efforts are not aligned with business goals and success factors, organizations will experience suboptimal results from their investments. They should understand which business processes are important and focus on how to protect related assets. That means identifying what information is relevant to users protecting those assets and delivering it accordingly.

Organizations should not develop or acquire threat intelligence for the

sake of threat intelligence alone; it serves a higher purpose, Forrester said in its report.

Threat intelligence informs business decisions regarding the risks and implications associated with threats. It can do so only if the intelligence provides relevant information that key users need to protect business processes. Understanding the data requirements has the added benefit of identifying other stakeholders who can use the information. Adversary intelligence can be used by threat intelligence teams to identify emerging threats and put effective controls in place, as well as by incident response teams to identify important incidents and understand what they are seeing when investigating a potential breach. Network operations teams can proactively hunt for indicators of compromise and reduce the amount of time attackers can hide in their networks. Aligning intelligence requirements with business goals focuses attention on what is critical and needs immediate attention.

Quality matters more than quantity when choosing intelligence sources.

Appropriate planning can also maximize program impact by ensuring that resources are aligned. For example, organizations need adequately trained staff when acquiring a new intelligence source in order to interpret the threat data or ensure that process or technical restrictions don't preclude use of associated indicators in the company's security infrastructure.

With today's high turnover rates, organizations should consider what happens when a security director or a senior manager leaves the company. Without a clearly documented outline of how threat intelligence fits into the overall security program, the incoming manager or director may not understand how the technology and data are being used. Even in times of high staff turnover, it's possible to maintain continuity with documented processes.

How to Develop Intelligence Requirements

- Establish and nurture business relationships with the following: business operations, compliance, finance, internal audit, legal, and risk management. Also work with the audit committee and governance board.
- Understand the success factors and risks to your business.
- Utilize the formal risk assessments process within your organization.
- Embed business security analysts in the organizational units. If you cannot afford to have dedicated staff, then designate staff within the business organizations to have this additional function.
- Listen to investor calls; review SEC forms, including annual reports and Form 10-Ks.
- Leverage Open Source Intelligence (OSINT) collection on your own organization (i.e., Google alerts on press releases and major announcements).
- By the time you learn of business initiatives via SEC forms and OSINT, it's likely too late, but understanding these initiatives builds credibility when performing outreach to understand the risks to your business.

Source: Forrester Research, Inc.

TRAP 2 Relying on Inappropriate Intelligence

Not all data sources are equal, and bad intelligence can cause more harm than good. Threat intelligence is supposed to help security directors and senior executives make good decisions, and that depends heavily on the data inputs of the threat intelligence process. It's a simple equation: Bad intelligence equals bad decisions.

Organizations must be careful about the sources they pick for threat intelligence programs, since quality matters more than quantity. Many organizations, especially those with immature threat intelligence programs, rely on low-cost providers or seek free sources, such as scraping the information available on the Internet or waiting to receive vulnerability and patch reports from vendors. While this is not necessarily a bad thing when in the early stages of designing the program, or for use as test data, relying on cheap and free sources of intelligence will significantly compromise the quality of decision-making and introduce unnecessary risk to the organization.

Sources should be selected not just for content, but also for relevance, timeliness, accuracy and coverage. Look for global-scale intelligence leveraging broad attack surface visibility, as well as regional and industry-specific insights to improve visibility. Consider the source's resources and its ability to recognize new indicators and changes

in tactics. If the source has delays in picking up the new information or identifying relationships among obscure disparate raw data, it could seriously hinder the program's effectiveness and decision-making abilities. The right intelligence will actually enable organizations to go on the offensive. When they understand what threats are hitting their industry or supply chain, they can apply protective measures before being attacked and can also proactively hunt for indications of targeted activity.

Bad intelligence can cause more harm than good.

The organization already has access to many valuable insights about ongoing activities from its own network. Its logs may show periodic traffic going to an IP address in Asia, but correlating with outside intelligence provides context, such as the fact the IP address belongs to a command-and-control server associated in the past with a known cyberespionage operation. That is intelligence the defenders can actually use.

Intelligence sources should be selected to take care of the heavy lifting — collecting and distilling threat data from multiple sources, and associating it with historical information to uncover new threats or existing ones that have evolved — leaving organizations free to correlate the data with their environment.

TRAP 3 Failing to Identify Executive Suite as a Key Consumer

Cybersecurity has become a board-level conversation, and senior security executives must be knowledgeable and prepared to consider their security posture in relation to the greater threat landscape at any time. It's not simply an "Are we getting attacked?" conversation. Because an organization's security posture and overall security program affect other facets of business, such as the organization's brand reputation if breached, loss of intellectual property, and even cyber insurance policies and premiums, the ability to protect against and respond to threats will continue to grow in importance to the bottom line.

Intelligence has frequently been consumed by threat analysts, security operations, and incident response teams, and it is usually kept within the middle and lower levels of the organization. Today, an organization requires a more formal and mature threat-intelligence program for better visibility and understanding of sophisticated adversaries and the tactics and campaigns being activated. This level of insight is expected to be communicated upstream to senior executives so they can be aware of the risks confronting the organization.

Adversary intelligence provides the executive team with insight into who is attacking the organization's industry, the goals and techniques of a threat actor or group, and what active or emerging campaigns may affect the organization. This essentially puts a face on the attacker and helps make threats more tangible, rather than abstract. For example, being able to describe a specific campaign affecting the industry and the tools and tactics that threat actors are using will make it easier to assess potential risk, implement countermeasures, and tie security spending to specific initiatives and risk-reduction measures.

It's one thing to say that the organization is vulnerable and something needs to be patched, or to read in the headlines of an attack on a peer. It's completely different to describe the nature of an existing campaign and the course it is taking. By providing such information on a regular basis and not waiting for senior executives to ask about something they've heard in the news, the chief information security officer (CISO) and the security director demonstrate mastery of the environment, which in turn, increases trust in the security organization.

TRAP 4 Believing Raw Threat Data Equates to Threat Intelligence

Organizations with less mature security programs don't always understand the role contextual information plays in determining what is relevant and what is not. Much information is available, and rich context helps organizations apply intelligence effectively.

Some sources just dump raw threat data. That isn't threat intelligence, as there is no curation or interpretation added to provide context. Raw, unqualified data will not provide the right level of relevancy. It's one thing to have an IP address flagged as malicious, but the security organization needs to know what malicious activity is occurring, how long it has been going on, and what impact that activity might have on the organization. Instead of saying an IP address is bad, it's more helpful to say the IP address is spreading a specific variant of malware. The layer of additional intelligence makes it possible for security professionals to go to the affected endpoint and know what to look for, as well as to prioritize the severity of the threat. Saying an international campaign is targeting financial services is not very helpful, but if the data source has details, such as the name of the attached file used, the subject line of the phishing

email being sent, email addresses being used, or even the hash of the malware being sent, then that information is actionable. The security team can look for those elements to determine whether the organization has already been hit, or proactively set up rules to block the attack.

Details matter. Data on victimization and technical indicators is key to acting on intelligence and operating proactively. Having the full picture of the threat lets security professionals filter out information that is not relevant to the organization and use intelligence effectively.

TRAP 5 Narrowly Focusing on Commodity Attacks

Historically, organizations had focused on creating an impenetrable perimeter to keep out threats. Recently, organizations have started trying to make those past investments more effective by injecting technical intelligence into them. They are making updates to existing preventative measures, such as utilizing reputation data to identify and block attacks via existing security information and event management (SEIM) or Intrustion Protection System (IPS) technology.

As the volume and sophistication of attacks has increased, this approach is still required but is no longer sufficient in itself. Focusing solely on blocking commodity attacks to the exclusion of developing strategies to deal with new, targeted, emerging threats leaves organizations open to nasty surprises. This is a two-pronged effort and both need to happen. A cybercrime campaign may target specific organizations, and all the information on hand about commodity attacks won't help detect or deter the advanced attack. What's needed is forward looking intelligence, which can, for example, be gleaned from tracking threat activity on underground forums, such as information related to new malware or vulnerabilities being sold, and tools being offered. This type of threat intelligence helps pinpoint potential methodology for attacks that haven't yet happened, enabling an organization to proactively get in front of an attack.

Threat intelligence allows organizations to focus on new and emerging threats targeting their unique environment and update their security strategy to implement protective measures, prioritize resources and respond effectively.

Don't Get Trapped

Knowledge is power, and security professionals must rely on threat intelligence gathered from various sources to tell them who the attackers are, what the attacks look like and how to stop them. Threat intelligence fuels an organization's security program and helps organizations understand who the adversaries are, proactively communicate active and emerging threats to senior executives, identify measures that can be taken to protect key business assets, pinpoint indicators of targeted attacks, and provide context to help security teams operate effectively.

Modern attackers are well funded, patient and highly organized as they target vulnerabilities in technologies, processes and people. Their attack methods are sophisticated and highly adaptable based on the defense mechanisms they encounter. If they are blocked at one point, they pivot and try again from a different angle. When one attack technique stops working, they pick up a new tool or technique and start over again. They will not stop until they identify the right vulnerable penetration point, and defenders are at a disadvantage since they have to try to block every single one.

With the growing realization among organizations that it is no longer — if it ever was — feasible to attempt to detect and prevent all attacks and breaches, organizations and their security professionals need to focus on threat intelligence that can adequately inform business-risk decisions, inform security operations and response teams, and strengthen their overall security program.

You will be trapped if you:

1. Lack a defined intelligence program and processes
2. Rely on inappropriate intelligence
3. Fail to identify executive suite as a key consumer
4. Believe raw threat data equates to threat intelligence
5. Narrowly focus on commodity attacks