NETWITNESS

WHITE PAPER

# Threat Intelligence: The Key to Higher Security Operation Performance

## Threats Today are Relentless and Come in all Shape and Sizes

The internet has become the catalyst to an ever-growing global economy. At its foundation, it was designed for connectivity, but not security. This in turn means that organizations that have moved to a digital business model are open to the risk of data being stolen. Throughout the years, approaches such as intrusion detection systems, anti-virus programs, and traditional incident response methodologies have attempted to fill the security gap. However, these approaches by themselves have had limited success as new and ever more sophisticated threats have been found ways around those defense systems.

Findings from the 2021 Data Breach Investigations Report[1] show that in 2020, data continued to be lost or stolen, a pattern that is unlikely to change anytime soon. These threat actors may be internal (for loss) or external (for theft).

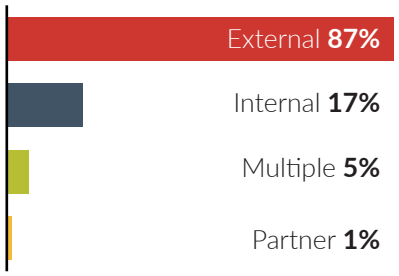
Cyberthreat actors are leveraging more tools, techniques, and procedures (TTP) that are only becoming more sophisticated and are outpacing stand-alone security solutions. allowing them to get past disparate and uncoordinated defenses.

### FREQUENCY

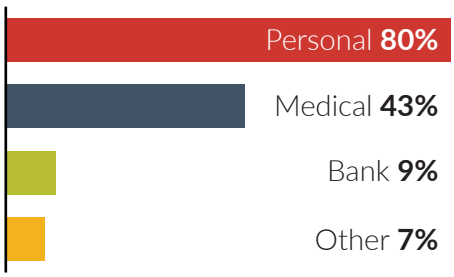
**1,295 incidents**

84 with confirmed data disclosure

### THREAT ACTORS




### DATA COMPROMISED




### THREAT ACTOR MOTIVES

**Financial**

**100%**

Cyberthreat actors are leveraging more tools, techniques, and procedures (TTP) that are only becoming more sophisticated and are outpacing stand-alone security solutions. allowing them to get past disparate and uncoordinated defenses. Advanced Persistent Threats (APTs), which are comprised of organized criminal or state-sponsored groups, have the tools, training, and resources to disrupt or breach most conventional network defense systems. These incursions are not conducted as isolated attempts. They are often multi-year campaigns targeting valuable, sensitive data.

Clearly, you need to react to threats. But if you are only reacting, you are playing a never-ending game of catch-up and clean-up. Having a threat-intelligence-led security program gives your company or agency a fighting chance to defeat these ever-changing threats. You need a holistic view of the threat landscape and a proactive posture to protect your institution from the multitude of threats you face every day.

To combat these sophisticated threats, you need to constantly harvest and process knowledge about the threat actors, not just the specific incidents. Knowing the "Who, What, Where, When, and How" of your adversaries' actions is the only way to decrease their chances of success. But the volume of intelligence is so massive that tracking and understanding adversarial actions can be overwhelming. Therefore, incorporating threat intelligence management is becoming more critical to a threat detection and response strategy.

To combat these sophisticated threats, you need to constantly harvest and process knowledge about the threat actors, not just the specific incidents.

Effective threat intelligence management is an ongoing effort. The threat landscape is already large, and it's only growing, becoming more complex and getting more efficient as time passes. To keep pace, organizations must constantly examine their defensive positions and adjust operations and strategies to defend against the evolving technologies and adversaries that endanger assets. In the same way that an individual pays for a gym membership and uses it regularly to keep fit, your organization must make a continual investment and commitment to protecting your assets.

## Threat Intelligence Management Can Help

Any delay is a moment of risk. Your assets are being examined. Your vulnerabilities are being identified. Who are these adversaries? What do they want, how will they attack, and when will they do it? Have they attacked any of your partners or competitors, and, if so, what happened in those attacks? This is the breadth and depth of knowledge that you need to secure your assets today. This is where Threat Intelligence Management can help in multiple ways.

### Drive Security Process with Intelligence

First and foremost, threat intelligence management, also called a threat intelligence platform (TIP), should allow government agencies and large enterprises to aggregate all available threat data – both internal and external, structured and unstructured – analyze it rapidly, automate action, and then produce tactical, operational, and strategic threat intelligence all in one place.

### Unite all Resources Behind a Common Defense

With well-defined data architecture, your threat intelligence management will unite intelligence analysts with incident response, security operations, and risk management in your common mission to defend the enterprise from modern threats. Then, through either public or private communities that you choose, secure crowdsourcing surfaces more than you could on your own. And, it should work with your other systems to automate action based on workflows you set.

### Provide Enterprise-Level Intelligence for Better Operations

Security organizations spend enormous amounts of resources identifying, investigating, and remediating incidents that lead to real business-impacting threats. Threat Intelligence is key to ensuring that the organizations are focused on the right incidents, identifying the right evidence, and taking targeted action to remediate or avoid negative consequences.

## Modern, Holistic, and Focused Approach to Threat Intelligence

All organizations need to gather intelligence about the threats that endanger their systems. Intelligence provides private organizations and government agencies with the means to fend off threats in progress and, in many cases, prevent adversaries from infiltrating the network at all. The use of threat intelligence leads to a more holistic and a focused approach to security.

### Holistic Approach

Modern organizations know that to properly secure their environments, they need to go beyond identifying and patching network vulnerabilities to mitigate risk. They need a holistic approach that looks at every aspect of its threat management in relation to every other aspect. Cybercriminals are uncovering and taking advantage of new attack vectors. Without complete visibility of the attack landscape, organizations will be subject to infiltration and possible exfiltration of critical data.

### Focused Approach

A focused approach concentrates resources on concrete threats to its network. A focused approach does not replace the redundant layers of information assurance; rather, it strategically orchestrates the layers so that they can provide the most efficient defense.

Threat intelligence enables an organization to detect, recognize, and prevent attacks. Threat intelligence platform functionality strengthens security monitoring by delivering feeds of threat-related indicators and providing a single platform to analyze and act on those indicators. The result is a holistic view of the threats, adversaries, and tradecraft. By analyzing threats in relation to these indicators, you can proactively deploy network-or host-based detection indicators and signatures for threat-related activity, thus halting threats before the infiltration has become critical.

Intelligence provides private organizations and government agencies with the means to fend off threats in progress and, in many cases, prevent adversaries from infiltrating the network at all.

When an attack is discovered, incident-response investigations must be conducted more quickly because the threat intelligence has already exposed the adversary's TTPs. Since the knowledge of the adversary has been revealed, an organization can best align its overall security programs to real threats. Specific adversaries' motives, goals, objectives, and capabilities can be identified and tracked. When an adversary is known, his next move is predictable.

The use of threat intelligence enables you to prioritize your defenses around highly targeted assets, focusing on remediating vulnerabilities that adversaries are known to be capable of exploiting. Threat intelligence reveals which vulnerabilities are most likely to be targeted, while also revealing ways that the adversary activity can be mitigated. By examining where threats are coming from (sources) and the processes or business goals they are intended to act upon (functions), your organization can develop strong, actionable threat intelligence.

## Understanding Threat Intelligence

Threat Intelligence is defined in simple terms as the knowledge of a threat's capabilities, infrastructure, motives, goals, and resources. By applying this information, operational security defenses can be vastly improved.

Threats can exist internally and externally. Threat Intelligence Management attempts to capture intelligence on both enabling organizations to create a more relevant and accurate threat profile while rating and ranking the value of threat intelligence sources.

Leveraging threat intelligence from your own network, such as log files, alerts, and incident response reports, you can recognize and stop threats.

### Internal Resources

Your own network is the greatest source of intelligence as it pertains specifically to your organization. Leveraging threat intelligence from your own network, such as log files, alerts, and incident response reports, you can recognize and stop threats. An ideal place to start is to utilize a Security Information Event Management (SIEM). Several raw sources of internal network event data (such as event logs, DNS logs, firewall logs, etc.) are already present in your SIEM. Maintaining historic knowledge of past incident-response engagements is helpful in leveraging more mature threat awareness based on internal sources. This includes retaining accessible data on the systems affected during an incident, the vulnerabilities exploited, the related indicators and malware, and, if known, the attribution and motivation of adversaries. Retaining malware used, relevant packet capture, and NetFlow can also be invaluable sources of intelligence.

### External Resources

External sources can be quite varied, with many degrees of details and trustworthiness. "Open source" intelligence, such as security researcher or vendor blogs or publicly available reputation and block lists, can provide indicators for detection and context. Private or commercial sources of threat intelligence can include threat intelligence feeds, structured data reports (such as STIX), unstructured reports (such as PDF and Word documents), emails from sharing

groups, etc. Some of this data, particularly that from vendors, may be refined with context for a particular industry or government. However, it is ultimately up to your security team or someone with specific knowledge of your organization's threat landscape to determine its relevance.

## Valuing Threat Intelligence

For threat intelligence to be useful to an organization, sources must focus on real threats specific to your organization, as opposed to a generic intelligence feed. All threat intelligence must be evaluated based on relevance, variety, timelines, and accuracy.

### Relevance

The relevance of threat intelligence is measured by positive "hits" or alerts in the environment when deployed. Relevance is enhanced by the volume or "completeness" of the threat data. Some threats or classes of threats are larger in scope than others and require more volume to be closer to "complete," so numbers by themselves cannot be the sole metric. To determine the relevance of data on active threats, you first need to understand the types of threats targeting your assets. This requires the mapping of business processes to specific geographic, political, and industry-focused threat classes. Once the classes are identified, then you must learn more about potential adversaries by focusing on threat intelligence sources that provide data on these types of threats. In practice, this is an iterative process. The more intelligence an organization has available to determine threat-based risk, the better it can understand which intelligence is most relevant.

### Variety

Incident detection and prevention should not rely on one medium, technique, or capability. Threat intelligence used to enhance incident detection and prevention should not do so either. Operational intelligence is essential to use a combination of host- and network-based indicators and signatures. Likewise, a combination of indicators or other detection techniques that find both adversary infrastructure and capabilities usage are critical. Threat intelligence that enables you to detect or prevent activity at multiple phases of an intrusion, such as in kill chain tactics, is more valuable.

### Timeliness

Timeliness refers to the frequency of updates relative to new threat activity, changes, or evolutions in capability or infrastructure. Some types of threat intelligence are more subject to change than others. This attribute is called expiration frequency, and it depends on adversary resources, skill, tactics, techniques, and procedures. When threat intelligence provides a way to detect adversary activity that persists through evolutions in capabilities and infrastructure, then that intelligence is less prone to expiration, is more reliable, and saves effort in making frequent updates.

To determine the relevance of data on active threats, you first need to understand the types of threats targeting your assets.

### Accuracy

Accuracy is based on the number of false positive alerts or actions obtained from the threat intelligence. The lower the number, the more accurate the intelligence. Confidence ratings or certainty scoring may help in assessing the potential for false positives. Accuracy is also contextual. Hitting on actual "evil" is important for operational threat intelligence. Knowing what to do next is important for strategic threat intelligence. Context is the "glue" between operational and strategic threat intelligence, and it determines the next steps to take once there is an alert. When context correctly links the operational and strategic aspects of a threat, the activity can be accurately attributed, and the motives and capabilities of the adversary can be assessed. Inaccurate context results in incident-response efforts that are misdirected, and strategic defenses that are misaligned with real threats.

## Applying Threat Intelligence to Your Security Strategy

In recent years, security operations have seen the value that threat intelligence has added to threat detection and response activities. The use cases described below are a handful of ways threat intelligence empowers security teams to be more successful.

### Alerting and Blocking

As a fundamental use case, threat intelligence can use tactical feeds of threat-intelligence-derived indicators to block malicious activity at the point of attempted entry into the environment. Detecting indictors of compromise (IOCs) can be done by leveraging the alerts from a SIEM leveraging logs, as signatures from and IDS/IPS, or host-based signatures on endpoint protection products.

### Contextual Alerting and Signature Management

Context provided by threat intelligence is critical in determining the severity and validity of alerts. Host- and network-based detection signatures are more effective using the context from threat intelligence. This provides confidence in the alerts, helps security analysts prioritize alerts and decide on the best next steps based on the adversary's known TTPs.

### Incident Response

Threat intelligence is directly correlated to incident response processes by providing needed context around incidents of compromise. This helps security analysts determine the next best step when investigating intrusions. This context also drives prioritization and can link multiple incident investigations together based on common evidence abstracted leveraging threat intelligence.

### Intelligence Consolidation

Assessing intelligence from multiple sources and source types creates a complete threat and risk picture for an organization. Consolidating and making sense all this threat intelligence at scale is an underlying and critical function of any

Assessing intelligence from multiple sources and source types creates a complete threat and risk picture for an organization.

threat-intelligence analysis effort. It allows for the creation of comprehensive threat assessments and provides specific threat relevance by overlaying external intelligence sources onto internal ones.

### Security Planning

Using threat intelligence that is relevant to your risk posture, security planning drives architecture decisions and refines security processes to better defend against known threats.

### Extend Threat Intelligence Across the Security Community

Sharing data allows organizations to get a more accurate understanding of the information they're collecting by leveraging the expertise of their peers to validate their findings about incidents or threats. As public and private organizations begin to collaborate, analysis is conducted more broadly through an established circle of trust. By validating threat intelligence across the community organizations of like size and industry, teams can then compare what they are seeing within their environment to determine if an incident is a true threat or an anomaly.

## NetWitness Orchestrator Leverages Threat Intelligence Management

NetWitness Orchestrator was born from a threat intelligence platform and maintains that deep threat intelligence management DNA. This empowers security analysts to focus on the threats that matter most. It automates detection and prevention with multisource, validated threat intelligence to make sure you are getting alerts for -- and responding to -- the right things. Eliminating false positives and using validated intelligence help you take more accurate actions. The threat intelligence management capabilities of NetWitness Orchestrator bring consistency and efficiency to threat investigation, hunting and response. Working directly from threat intelligence sourced from open and subscription-based feeds, public information, internal intelligence, and crowd sourced intelligence allows you to work faster, and to prevent more attacks before they happen. The more you can automate up front, the more proactive you can be. Eliminating false positives and using validated intelligence help you take more accurate actions which in turn improves speed and precision.

## About NetWitness

NetWitness, an RSA® Business, provides comprehensive and highly scalable threat detection and response capabilities for organizations around the world. The NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. This empowers security analysts to be more efficient and stay ahead of business-impacting threats. For more information, go to netwitness.com.

NETWITNESS
An RSA Business