WHITE PAPER

The Promise of Threat Intelligence: What Your Enterprise Needs to Know NOW

Minimizing Risks by the Collection of Actionable Information

Regroup Mass Notification

Contents

Introduction

With today's constantly evolving cyber landscape, combined with companies embracing a remote workforce, threat intelligence has become a crucial tool for businesses seeking operational resilience. Simply stated, threat intelligence is the collection and analysis of data points that illustrate trends that could negatively impact a business or organization. These trends may include disruptions in supply chains, civil unrest, increased cyberattack activity, reputational threats and a host of other potential hazards.

This evidenced-based knowledge includes context, mechanisms, indicators and actionable direction about existing or emerging dangers to people and assets.

Traditionally, threat intelligence has been an expensive effort — necessitating dedicated teams focused on data acquisition and analysis. These days, however, organizations wishing to strengthen their security have more options and more tools at their disposal.

This paper explores what threat intelligence is — and isn't, why it's crucial for a variety of industries and what expectations team leaders should set for their security goals.

EVIDENCED-BASED KNOWLEDGE

about existing or emerging dangers to people and assets.

- ● CONTEXT
- ● MECHANISMS
- ● INDICATORS
- ● ACTIONABLE DIRECTION

Why Threat Intelligence is Important to Your Business

Early in 2020, the global pandemic of COVID-19 forever changed the way governments, businesses and public facilities operated. With lockdowns and stay-at-home orders put into place across the globe, businesses were forced to incorporate remote and hybrid working conditions for their teams. And, with more individuals working from home — without much supervision — the opportunities for cyberattacks and phishing became more prevalent.

In May 2020, the death of George Floyd sparked weeks of protests across the United States and in some European cities. Many of these protests turned violent with cities like Portland, Oregon falling victim to widespread vandalism, fires and other matters of social unrest.

In May 2021, hackers used a single compromised password to breach Colonial Pipeline, owners of the largest fuel pipeline in the United States. This created shortages in several states and ultimately cost Colonial Pipeline over $4 million in ransom.

Though these three events are vastly different, they all pose substantial threats to business operations and continuity. Disruptions in supply chains, cyberattacks and civil unrest can dramatically impact the health of any enterprise and expose organizations to larger, financially devastating risks. Even societal movements can undermine business with risks to reputation and, ultimately, profitability.

Eliminating security blind spots through threat intelligence means empowering enterprises with the ability to focus on risk mitigation and collaborative actions to keep people and assets safer.

RECENT EVENTS THAT AFFECTED MILLIONS

and pose threatened business operations and continuity

Early
2020

The COVID-19 Pandemic

May
2020

The Death of George Floyd

May
2021

The Hacking of Colonial Pipeline

The Right Approach to Threat Intelligence Gathering

Though COVID-19 remains a significant business risk, other disruptions continue to threaten resilience in the enterprise environment. Persistent risks like supply chain disruptions, cybercrime, IT failures and outages, severe weather, natural disasters and political instabilities all have the ability to devastate an otherwise thriving business.

Monitoring a single threat is an insufficient approach to bolstering an organization's defenses. The right approach has to take into account global and local threats, assets, vulnerabilities and aggregate data sources.

When organizations take these tasks in-house, their available tools must have the ability to collect intelligence from a variety of channels and sources. What's more, real-time monitoring of corporate assets, relative to location, is an indispensable mechanism for keeping people and property safe.

This can be a daunting task without the appropriate structure in place. Because of that, threat intelligence suites can provide the right solution.

This type of data collecting and reporting software can provide critical global and hyperlocal intelligence from a wide range of channels. Ideally, a threat intelligence suite like Regroup's, aggregates data from news (local, national and international), RSS, social media, emergency agencies and weather reporting agencies. The gathered intelligence can then be used to determine the organization's exposure to specific types of threats, or to devise an enterprise-wide response when security has been compromised.

The most effective approach is to cast a wide net of relevant data collection from a number of vetted sources.

THREAT INTELLIGENCE DATA AGGREGATION

NEWS

Local, national and international

+

RSS

+

SOCIAL MEDIA

+

EMERGENCY AGENCIES

+

WEATHER AGENCIES

Making Threat Intelligence Actionable

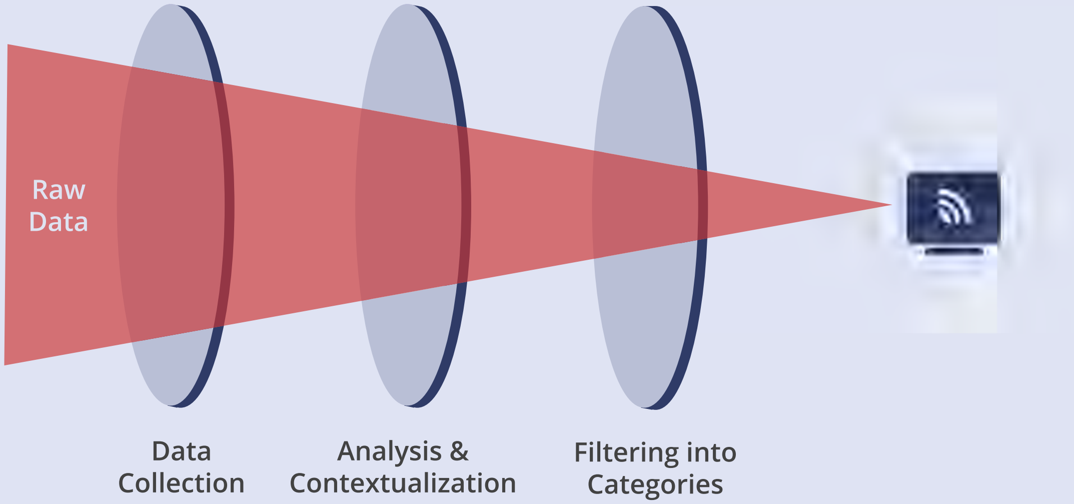
Using threat intelligence to bolster situational awareness and enterprise security begins with understanding the data. For this purpose, a threat intelligence suite must provide useful filtering for regions, severity, industry and type of threat. Visualization can also be useful for administrators to gain insights on threats to corporate assets and specific locations.

With this knowledge in hand, team leaders can be better prepared to train and guide employees on cybersecurity, the appropriate use of company technology resources and response to threats. Leaders can also prepare alternative resources should things like supply chains be at risk of interruption.

IT departments can also use intelligence to identify emerging trends in cybercrime and take the needed steps to protect network assets across the organization. Since cyberattacks and other menaces (like phishing) are continually changing, trend intelligence for these attacks is an invaluable tool for proactive security measures.

Additionally, when severe weather or other natural disasters threaten, information can be used to alert team members of potential dangers, evacuation instructions and physical procedures to protect corporate assets from damage.

ACTIONABLE THREAT INTELLIGENCE TO YOUR DESKTOP



The Importance of Your Action Plan

Organization-wide security is improved by a corporate security plan and a solid communication plan. Your corporate security plan should include measures to prevent external threats and define the appropriate steps taken in the event of a breach. In developing your plan, consider these steps:

IDENTIFY VULNERABILITIES

This can include outdated hardware and software, exposure to cyberattacks, facilities issues or lack of employee training.

INCLUDE EMPLOYEES IN POLICY DEVELOPMENT

Involving employees at all levels can help you better identify workplace risks and other factors.

GET GUIDANCE FROM EXPERTS

Whether local law enforcement, or a security consulting firm, reach out to professionals to guide you in the process.

TRAIN EMPLOYEES

Staff training is one of the most important measures you can take to protect your network and assets in the event of a threat.

PUT IT IN WRITING

Your plan should be clear, concise and updates to it communicated throughout the entire organization.

Integrating a threat response protocol into your communications plan is also an important step in securing your organization. With the right type of communication, you can head off disasters off and provide the appropriate team members with action items to minimize damage. This is particularly effective when you incorporate mass notification into your overarching plan.

When considering a mass notification platform, it’s important to identify the following must-have features:

1. Can the platform be used during power outages or cellular tower overloads?

2. Will it alert specific groups and teams easily and quickly?

3. Does the solution have two-way communication capabilities for managing response?

4. Can it alert via email, text/SMS, desktop alerts, intranets and other channels?

5. Is it easy to use and adoptable?

6. Does the platform provide automated alerts for severe weather and natural disasters?

Threat intelligence is only as good as the security policy and enterprise-wide communication you establish. Therefore, keeping your organization resilient and people and assets safe requires a commitment from all involved.

About Regroup Mass Notification

Since 2006, Regroup Mass Notification has kept institutions safe, informed and productive with its cloud-based mass notification platform. Regroup has helped institutions in higher education, healthcare, enterprise, government and manufacturing solve their communications challenges with a system that is easy to use, robust and reliable.

Regroup also provides a comprehensive Threat Intelligence Suite that helps organizations mitigate risks and identify trends in cyber, civil and other threats.

Learn More **www.regroup.com** Call Us **855-REGROUP**