The Need for Threat Intelligence in Keeping Data Secure

COMCAST BUSINESS

Introduction

Organizations today face more security threats than ever. The scope, frequency and severity of attacks by cybercriminals are rising to unprecedented levels, leaving every company vulnerable to an attack that is most assuredly going to happen.

Threats to organizations are myriad and growing ever more prevalent. According to a report by Symantec, supply-chain attacks saw a 78% increase in 2018, while malware increasingly is being used beyond simple intelligence-gathering to actually destroy or disrupt corporate networks. Such attacks rose 25% in 2018.

Whether it's a spear-phishing campaign, distributed denial-of-service (DDoS) attack or botnets infiltrating the network to steal sensitive data, the threats are very real—and very dangerous.

Today's security landscape has evolved to meet the threats of cybercriminals, but point solutions are no longer enough to thwart attacks. And as more organizations shift to heterogeneous IT environments to save money and gain agility, they unwittingly create a larger attack surface for malicious actors to do harm.

Organizations, therefore, must work smarter to keep their data and their networks secure. That's where threat intelligence comes in, providing insight to spot potential security problems so they can be remediated quickly.

The State of Corporate Security

Organizations face an uphill battle when it comes to their corporate security. With every day comes another headline about a data breach, ransomware attack or other security malfeasance resulting in stolen credentials, compromised consumer privacy and, in some cases, financial loss. As the tide of security breaches continues to rise, confidence in corporate networks and strategies to keep sensitive data and personal information safe concurrently is falling: 79% of business leaders say they can't keep up with the amount of new technology vulnerabilities being introduced by new business models.

At the same time, digital transformation efforts are expanding an organization's attack surface, making it vulnerable not only within the corporate network but also in the cloud, through subscriptions and as-a-service offerings. Memory exploits in cloud services providers wrought by the likes of Spectre and Meltdown put data at risk due to the shared memory pool setup of cloud services, while misconfigured workload or storage instances introduce risk of not only data compromise but also non-compliance with government

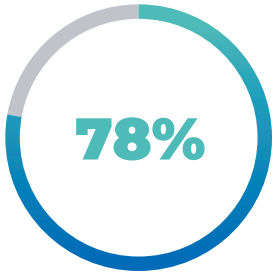
regulations—which could cost an organization millions in fines.

Add to the mix a growing dependence on the Internet of Things and the numerous connected devices—consumer, business and industrial—and it's easy to see why ensuring end-to-end security is becoming a daunting and impossible task for many organizations.

And it appears that the bad guys are winning: According to Cyberedge, the number of organizations that were breached in 2018 increased to 78%, and 32% reported being breached six or more times in the last 12 months—an increase of 27% over 2017.

Part of the issue has been—and continues to be—a lack of qualified security personnel. The skills shortage is impacting all areas of cybersecurity; as such, more organizations are relying more heavily on security technologies to lighten the load for security employees and fill the gaps where there is a lack of qualified workers. Bringing a level of intelligence around security threats, both current and anticipated, can help organizations improve their security posture and approach security from a more proactive standpoint.

Breaches Rose in 2018



78 percent of organizations were breached in 2018

32 percent of which were breached **six or more times** in the last six months

Source: CyberEdge Group "2019 Cyberthreat Defense Report", https://assets1.dxc.technology/security/downloads/2019_CDR_Exec_Brief_-_DXC.PDF

What is Threat Intelligence?

Threat intelligence is, quite simply, the use of data to uncover and understand potential threats to the network. The data provides context to enable organizations to make more informed decisions regarding their security posture and their response to threats.

Threat intelligence incorporates artificial intelligence and machine learning to collect and analyze data from inside and outside the corporate network to root out suspicious activity that might not be uncovered simply by examining network logs or other traditional data sets. For example, data could reveal that an internal server is connecting to a particular-yet-unfamiliar IP address every evening during off-hours. This could indicate the server has been infected with malware and is a threat to the security of the network.

Threat intelligence can be helpful to many different security roles in an

organization. Security operations teams can use threat intelligence to provide context to alerts so they can better understand which are the real threats. Incident response teams, meanwhile, can use threat intelligence to uncover threats in real-time for immediate action. And security leaders can use threat intelligence to understand how well their current security technologies are working—and where there are any gaps in their security strategy. Other roles also can benefit from threat intelligence, including fraud detection teams, risk analysis teams and vulnerability management teams.

The need for threat intelligence is palpable: In a recent study by Cyberedge, organizations rated "Too much data to analyze" as their top inhibitor to adequately defending themselves in a cyberattack. Organizations crave a level of context and intelligence that standard security tools don't deliver so they can cut through the noise and recognize what's happening on their networks and with their data. Indeed, in the same study, respondents listed advanced security analytics and threat intelligence services as their most sought-after technologies.

In a recent study by Cyberedge, organizations rated **"Too much data to analyze"** as their top inhibitor to **adequately defending themselves** in a cyberattack.

How Does Threat Intelligence Work?

Because threat intelligence relies on data to uncover potential threats, the amount of data and how it's collected are critical in an effective threat management program. Data can be culled from a number of sources including threat feeds from external providers such as NIST or security vendors, internal sources such as router logs and vulnerability scans, and other external sources such as social media and dark web forums.

Once collected, the disparate data is processed into usable formats, then analyzed by threat analysts, who then make the determination whether a threat is real and the necessary response.

Organizations increasingly need this level of insight, not only to ward off attackers but also to ensure the effectiveness of their security technology. Indeed, spending on cybersecurity technology is at an all-time high, with companies spending a cumulative $1 trillion from 2017 to 2021 to protect their data and networks. At the same time, more organizations are falling victim to cyberattacks—according to the FBI, the total amount of ransom

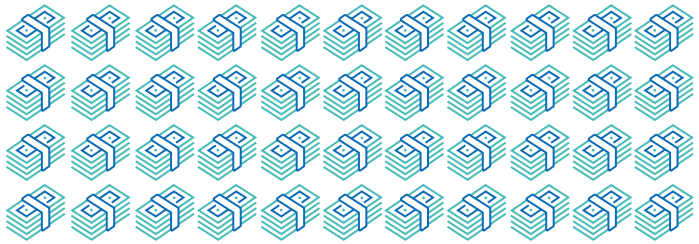
payments for data worldwide is approaching $1 billion annually.

Threat intelligence is one element in a comprehensive security strategy that also includes technologies such as security incident and event management (SIEM) systems, firewalls and identity and access management systems—all of which provides relevant data to root out potential threats.

Companies spent a cumulative $1 trillion from 2017 to 2021 to protect their data and networks

Source: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

The total amount of ransom payments for data worldwide is approaching $1 billion annually.



Source: FBI

Benefits of Threat Intelligence in Keeping Organizations Secure

Beyond the immediate and obvious benefit of shining a light on current and potential security threats, threat intelligence can help companies stay on top of new and emerging threats to their data and their networks. And, they can make more intelligent decisions regarding their response to threats, such as how best to mitigate the threat and ensure it doesn't come back.

In the same vein, the insights provided by threat intelligence can help incident response and other teams improve their response times by being able to make better and more informed decisions.

Smarter business decisions also are possible using threat intelligence.

Organizations not only can better understand how their current security technologies are performing, they also can see where there are holes in their strategy and make decisions regarding new technologies or employees to fill those holes.

For organizations with a dearth of skilled security employees, threat intelligence can help fill the gaps by providing access to information automatically without having to sift through mountains of data.

Better insight can improve an organization's efficiencies, leading to a more robust and effective security posture.

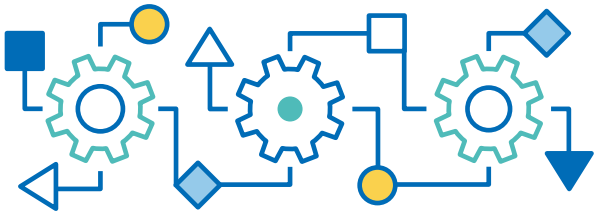
Threat intelligence can help fill the gaps by providing **access to information automatically** without having to sift through mountains of data.

Comcast Business' Role in Threat Intelligence

The ever-evolving security landscape is becoming more difficult for organizations of any size in any industry to manage. At the same time, cyberthreats are growing more sophisticated and more nefarious. Tools such as threat intelligence are helping level the playing field, giving organizations a fighting chance against cybercriminals.

Threat intelligence is just one of the many technologies that make up a comprehensive security portfolio, as organizations strive to ensure their sensitive data and networks are protected. Other technologies in a comprehensive portfolio include web application firewalls and a unified threat management system consisting of intrusion detection, content filtering, data loss prevention, anti-virus and anti-spam technologies. Together, these provide threat intelligence systems with the right data to detect unusual activity that could indicate threats to or attacks on the network.

Comcast Business offers a suite of cybersecurity products to help your business defend against malicious attacks like malware and denial of service. Visit Comcast Business website to learn more about our DDoS Mitigation Service and Managed Security offerings.



Threat intelligence is just **one of the many technologies** that make up a comprehensive **security portfolio.**

TOP

The Need for Threat Intelligence in Keeping Data Secure

COMCAST BUSINESS