Bitdefender
BUILT FOR RESILIENCE

Exploit Defense

Threat Intelligence

The Changing World of Cybercrime

There was a time when the typical picture most people would envision when thinking about a cybercriminal, is a lone actor in a hoodie, working out of a dimly lit room, possibly a basement. This person would look to hack into a computer to steal information or cause mischief. We've come a long way from that concept of cybercrime. Cybercrime is estimated to cost the world $10.5 trillion dollars annually by 2025[1]. Much of that cybercrime is now state-sponsored. Cybercriminals are actively recruited on the dark web, and are offered six-figure salaries. The basement is now a boardroom, the lone computer is now an entire nation's infrastructure. To face such an overwhelming challenge requires having the right set of information in the right hands.

Cyber Threat Intelligence is at the forefront of the battle to keep businesses, nations, and institutions protected against cybercrime. Cyber threat intelligence experts are tasked with gathering data from various sources, analysing the data, and delivering key insights to security teams that will help them defend against cybercriminals. This threat intelligence helps drive operations, and forms the basis for well-informed decision making. As technology advances, so do the types of threats that entities need to contend with. To face these threats, cybersecurity and information gathering solutions have also advanced, but it's up to the cyber intelligence teams to discern how to best use this technology to stay one step ahead of the bad actors. **Threat Intelligence is a key component of a business's cybersecurity and comes with unique set of challenges:**

- Gathering re**liable data sources –** threat intelligence experts must cast as wide a net as possible and parse through the data to extract reliable information.
- **Security expertise –** having threat intelligence experts with the right knowledge and experience is critical.
- **Tight collaboration with security teams –** the threat intelligence team must be able to work closely with security teams to ensure timely action on potential threats.
- **Powerful cybersecurity and intelligence gathering tools are essential–** in order to battle the most sophisticated of attacks, security teams and cyber intelligence specialist must arm themselves with the best tools possible.

1 Numbers provided by Cybercrime Magazine https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

At-a-Glance

In a world of ever evolving cyber threats, Threat Intelligence helps drive the operations of cybersecurity teams. The Bitdefender Threat Intelligence team gathers information from various sources and creates tailored security plans based on each customer's individual threat model. With the Bitdefender Managed Detection and Response, customers of all sizes will have at their disposal a cybersecurity team with over 100 years of expertise managing award-winning tools, and using relevant, actionable data from a dedicated threat intelligence team.

Key Capabilities

- Custom Threat Model – each customer is different and Bitdefender's custom threat model will ensure that every customer will have a cybersecurity plan that's tailored just for them.Active threat hunts – the Bitdefender security team will perform threat hunts to help identify suspicious behavior, and activity that can put the business at risk of cyberattacks.
- Tipper Report – the Bitdefender Tipper report will provide relevant, actionable information to customers on threat actors, techniques, and emerging threat trends that can target the business .

Not all Threat Intelligence is Equal

Many cybersecurity companies claim to have strong threat intelligence capabilities. When examined with greater scrutiny, it's common to find that their claims are exaggerated. The threat intelligence often simply consists of telemetry data retrieved from their own cybersecurity solutions, and their focus is limited to cybersecurity trends. Bitdefender Threat Intelligence provides actionable threat data gathered from sources that include, web crawling systems, email traps, honeypots, monitored botnets, data shared with industry partners and law enforcement agencies, and a virtual machine farm that executes over 200,000 malware samples per day. All this impressive technology is only a part of the story. The strength of Bitdefender's Threat Intelligence are the minds that are using this technology in conjunction with their own vast expertise to deliver relevant, actionable information to the Bitdefender Managed Detection and Response (MDR) Security Team and our customers.

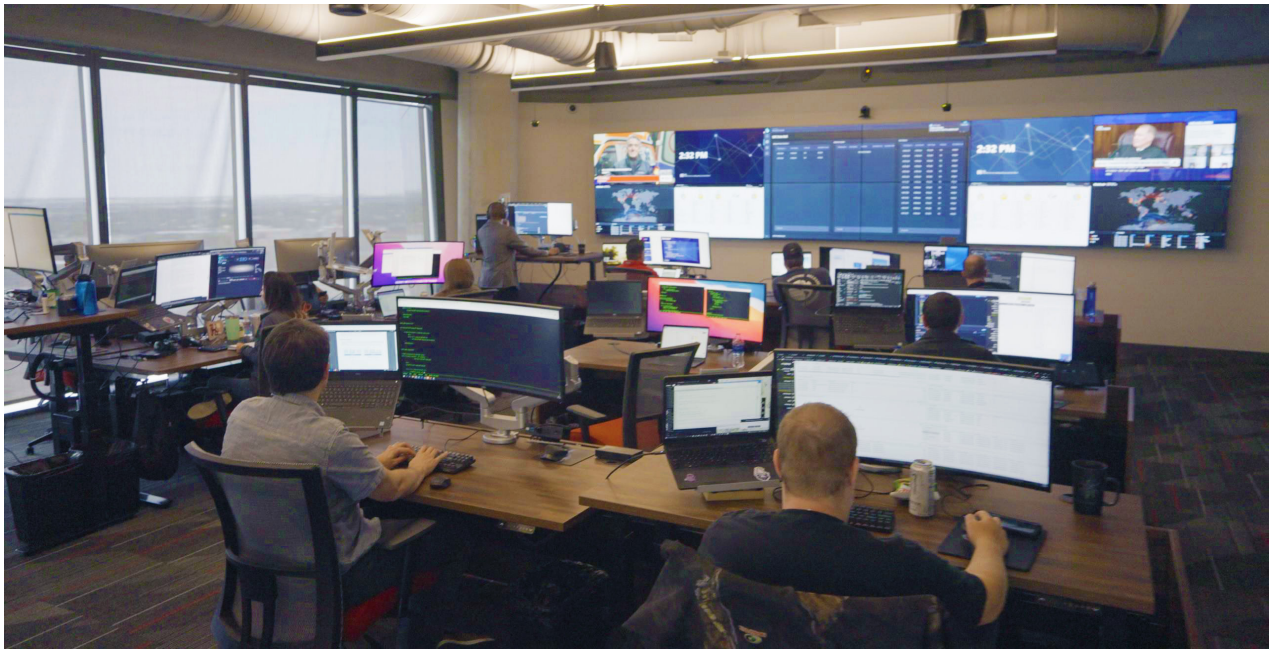

Figure 1.1: Hosted out of the famous Frost Tower in San Antonio, Texas, Bitdefender's main Security Operations Center has a staff with over 100 years of cybersecurity expertise with diverse backgrounds including former US military intelligence personnel.

Bitdefender MDR Threat Intelligence

The Bitdefender Managed Detection and Response team consists of a staff with over 100 years of cybersecurity expertise. The threat intelligence personnel's experience isn't limited to cyberthreats, as many of the staff have years of experience as United States military intelligence personnel. The threat intelligence team assesses information gathered from a wide variety of sources including: various cyber-intelligence gathering tools, scouring the dark and deep web, gathering data from various law enforcement organizations around the world, gathering threat information from the Bitdefender labs team, and reviewing information from various reliable news authorities.

The threat intelligence team casts a wide net and parses through the information to extract reliable, relevant information. This intelligence helps the security team address and prepare for the wide variety of threats that are actively targeting or could be targeting the Bitdefender customers. They identify trends that help them make educated deductions and stay one step ahead of cybercriminals. Their analysis is not limited to cybersecurity however, they examine business and geopolitical news that can also be a contributing factor to cybersecurity vulnerabilities.

Useful Data Gathering

Information is the most powerful tool we have against cyberthreats, but if that information isn't useful, it can hinder an entity's ability to protect itself against cyberthreats. Useless or misleading data can increase the time needed to remediate any threat. Without good information, security teams can be led down the wrong path in an investigation, which can in turn further compromise the security of the business. It's important that security teams have access to actionable intelligence, and this is where a great threat intelligence team comes in.

The Bitdefender MDR threat intelligence cell is tasked with collecting information from a variety of sources and then dissecting the bits that are useful and actionable. To organize the data, the team uses security and information event management (SIEM) tools, a security orchestration, automation, and response (SOAR) platform, and the GravityZone platform to identify meaningful data. The Threat Intelligence analysts will provide context to the data and help to eliminate false positives, ambiguity, and duplication of efforts. Their findings are discussed with the Bitdefender MDR Security Analysts and actions plans are custom tailored to each individual customer based on the customer's environment, the businesses' field of activity, and details of the identified potential threat.

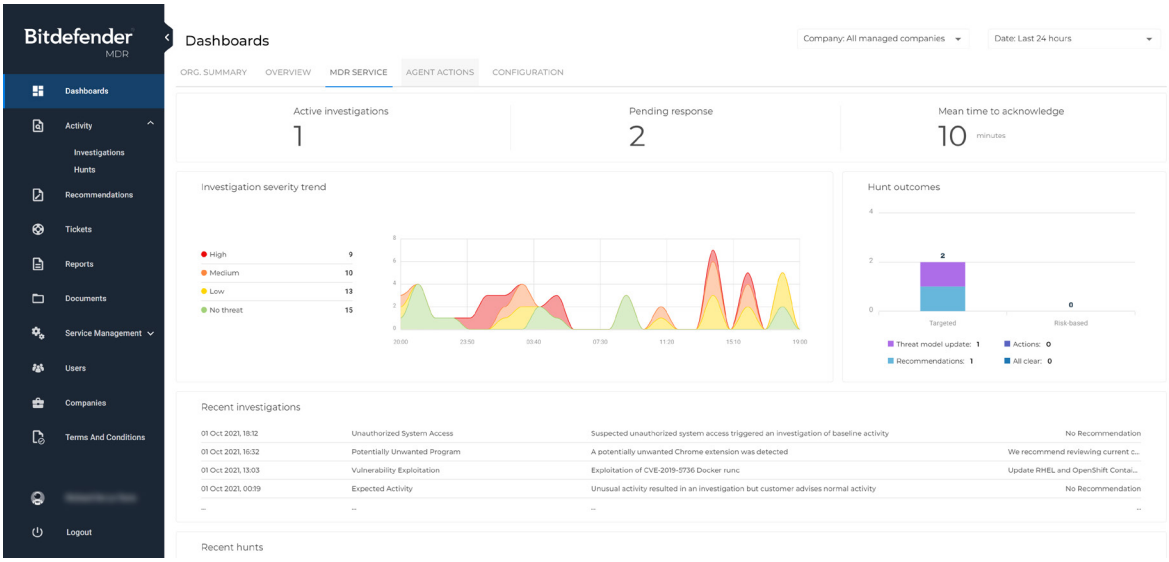

Figure 2.1: Using the GravityZone MDR Customer Portal, customers will be able to track the MDR team's cybersecurity activity including active investigations and threat hunts status, along with access to reports covering incident details, monthly findings, and "tipper" reports that detail specific threat intelligence findings.

The Threat Model

In order to understand the business risks and align them with the strategic cybersecurity goals of the business, the Bitdefender MDR threat intelligence cell creates a threat model. In the initial onboarding process with the Bitdefender MDR team, the customer is provided a questionnaire that allows the team to learn more about the customer's infrastructure, security concerns, user environment, domains, and cybersecurity risks. With this information, the Bitdefender Threat Intelligence team generates an overview of who, what, where, and why cybercriminals would potentially target the business. Data points are gathered and compared to various threat intelligence models, and further research and analysis is performed to create a custom threat model for the customer.

With this threat model in place, the Bitdefender Threat Intelligence Cell and Security analysts can then accurately monitor for the following indicators of compromise: credentials leaks, Unauthorized publication of code or customer information monitoring, typosquatting – also known as URL hijacking, and dark web monitoring for mentions of the business and users. This threat model is also used for threat hunts and custom Tipper reports.

Threat Hunting

One of the most useful techniques used to stay ahead of the cybercriminal is the threat hunt. Using information gathered from the customer, as well as an understanding of current and emerging threats, the Bitdefender MDR team conducts regular threat hunts. Using the Bitdefender GravityZone platform, endpoint and user risks are identified, suspicious activity is monitored with the Bitdefender XDR technology – at the endpoint, network, identity, and cloud level – and indicators of compromise are identified and addressed. Regular triages are performed with the Bitdefender Security Analysts and the customer to discuss how they can best prepare to protect themselves from potential cyberattacks. Using the GravityZone MDR Customer Portal, customers can also configure pre-approved actions and whom to contact in case an emergency action needs to be performed – for example: isolating a host/server with malicious activity, disabling a user account, and more.

Tipper Report

Another powerful tool provided by the Bitdefender Threat Intelligence Cell is the Tipper report. The Tipper reports can be accessed from the reporting section of the GravityZone MDR Customer Portal. The report details threat intelligence gathered on cybercriminal activity. This can include details on a specific cybercriminal group and who they are targeting and how. It can also provide details on a specific threat that may affect the business such as a new ransomware variant targeting a specific security vulnerability in the customer's environment, and new emerging threat trends.

The Tipper report will include key points to review, a summary and details, the MDR team's actions taken to protect the customer from the threat or vulnerability, additional recommendations, and identified indicators of compromise and tactics, techniques and procedures associated with the threat and in correlation to the customer's threat model.

Bitdefender Managed Detection and Response

Bitdefender MDR combines endpoint, network, cloud, identity, and productivity application telemetry into actionable security analytics, augmented by the threat-hunting expertise of a fully staffed security operations center (SOC) with security analysts from global intelligence agencies. Using the award-winning Bitdefender GravityZone tools, in conjunction with over 100 years of cybersecurity expertise, Bitdefender MDR will deliver 24x7 security monitoring, a custom threat model, root cause and impact analysis, dark web monitoring, targeted threat hunts, brand, ip, domain, and asset protection, and tailored response playbooks to customers of all sizes.

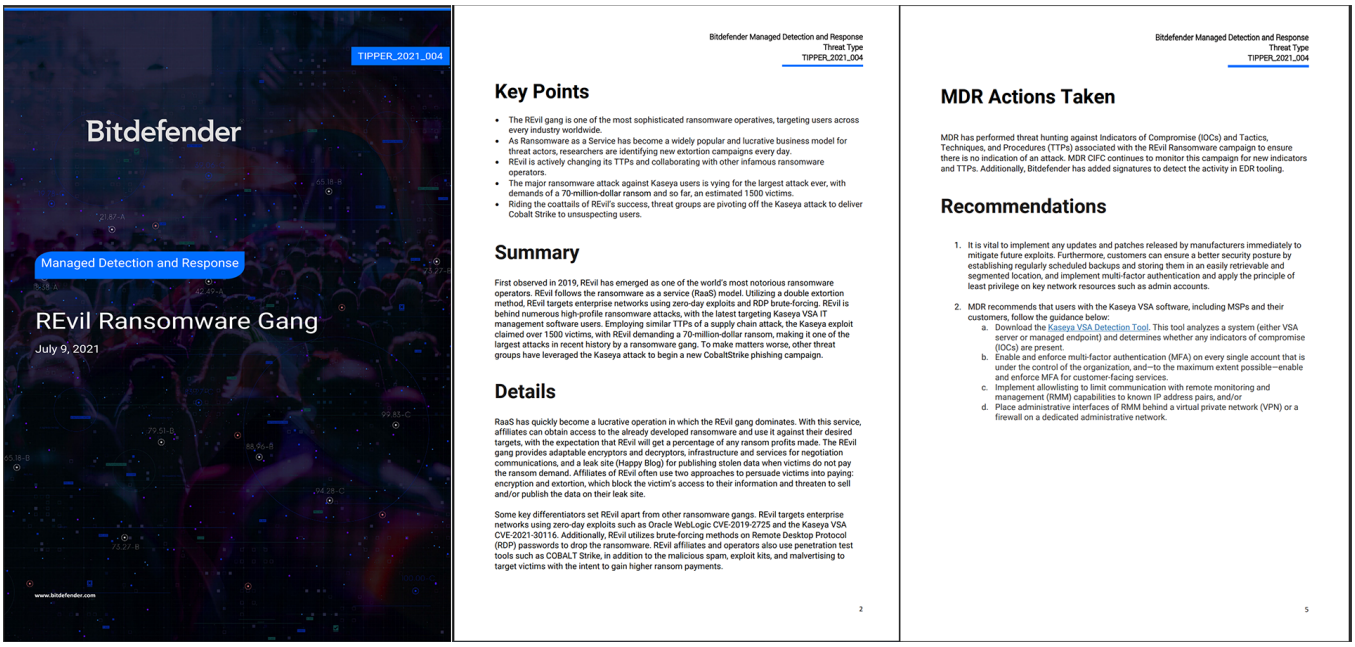

Figure 3.1: The GravityZone MDR Tipper Report will provide detailed information based on threat intelligence gathered on cybercriminal activities, key system vulnerabilities discovered, emerging trends and more – all tailored to the specific MDR customer.

Bitdefender
BUILT FOR RESILIENCE

3945 Freedom Circle
Ste 500, Santa Clara
California, 95054, USA

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

For more information, visit https://www.bitdefender.com.

Bitdefender-BSS-MDR_ThreatIntelligence-SolutionBrief-NO_LOCALIZATION-DEX6474-en_EN
CD-May/25/2022 • MD-May/26/2022