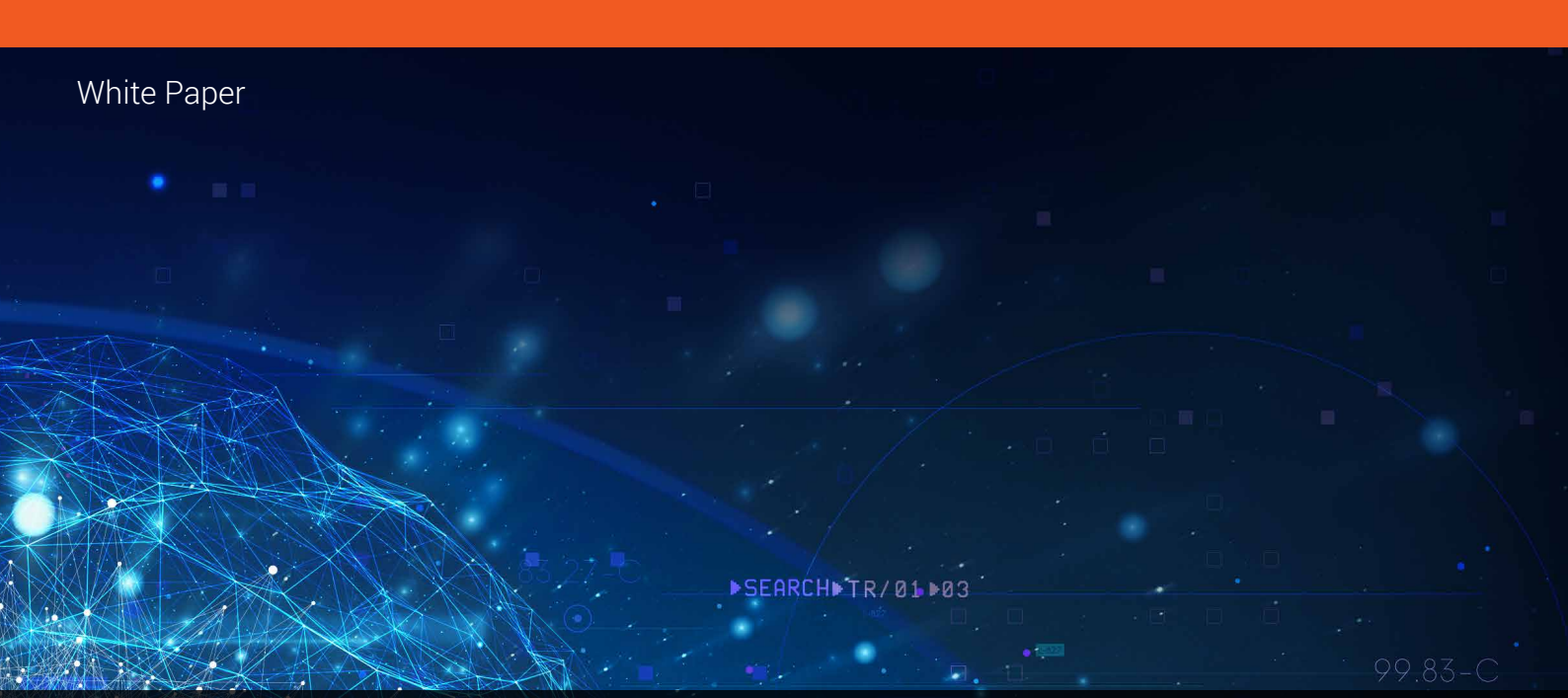
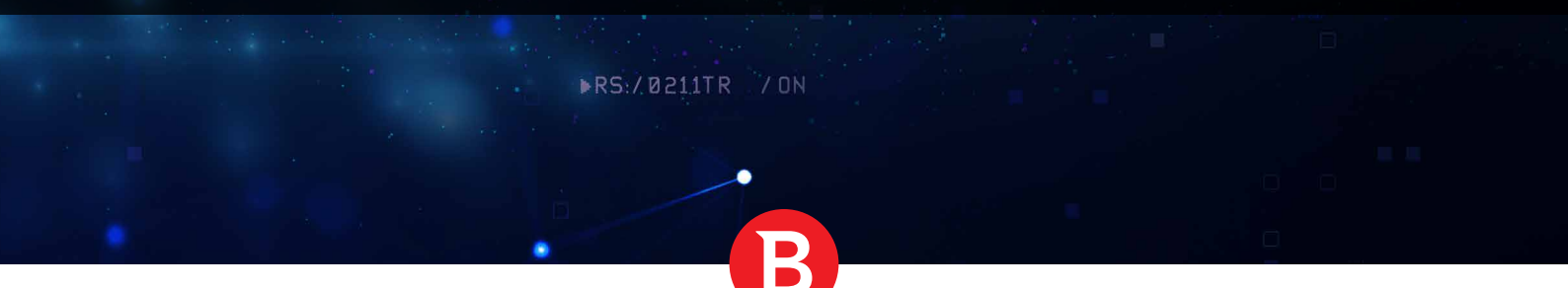
White Paper



Bitdefender®

Advanced Threat Intelligence

Boosting SOC Efficiency with Contextual and Real-Time Insights into the Global Threat Landscape



> "By 2022, 20% of large enterprises will use commercial threat intelligence (TI) services to inform their security strategies, which is an increase from fewer than 10% today."
>
> Gartner ***Market Guide for Security Threat Intelligence Products and Services***, Craig Lawson, Ryan Benson, Ruggero Contu, 19 February 2019

The cybercrime industry has evolved over the past couple of years, and is becoming increasingly sophisticated and lucrative. It generated over $1.5 trillion in illicit profit during 2017 and 2018, and is predicted to inflict over $6 trillion dollars in damages by 2021. Destructive malware attacks have become one of the most prevalent and expensive consequences of advanced cybercrime. While the number of reported data breaches fell slightly in 2018 from 2017, the number of exposed records is estimated at 5 billion.

An increasingly complex business environment and a more sophisticated and well-equipped adversary requires organizations **to better understand the attackers** and the attacks that threaten them most right now and, critically, which attackers and types of attacks will threaten the most next month, next year and beyond. Threat Intelligence (TI) is becoming a **critical weapon** in the Chief Information Security Officer's (CISO's) armory, as security programs strive to take a more proactive approach to keep up with events in their threat landscape. This dependence on predictive intelligence as well as reliable tactical and operational intelligence is driving growth in the threat intelligence market, which has been forecast to increase from **$4bn in 2018 to $13bn by 2025.**

If understood and used appropriately, Threat Intelligence has two critical use cases:

- Tactical and Operational support to cyber operations. Timely and actionable provision of information and Indicators of Compromise (IoCs) of current attacks that present risks today.

- Strategic support for cyber operations. Predictive intelligence and information about attackers and attacks that will present risk in the future.

Most Threat Intelligence services today focus on tactical intelligence, often promoted as 'actionable'. While undeniably critical, these services are reactionary in nature and provided by collecting and analyzing attacks that have already happened. Modern security programs recognize that they must take a longer-term approach to understanding the threat landscape, as capabilities require people, process and technology and take time to fund and build.

The Heterogeneous Threat Landscape

Some 1 billion malware samples will roam the internet by the end of 2019, but not all threats are created equal. Prevalent and highly virulent threats might not pose a high security risk because they could be easy to detect by traditional security solutions, but advanced and sophisticated threats that usually involve only a handful of samples going after select victims could fly below the radar, undetected by security software. The new frontier consists of novel and advanced techniques for attacking organizations and infrastructures or stealing and destroying data.

For instance, while incidents such as those that involved Marriot or Facebook were mostly about data theft, attackers used ransomware such as ONI, NotPetya and Hermes during the final stages of the attack to conceal their footprint.

Through phishing URLs, social engineering or malicious insiders, cybercriminals are now exploiting the weakest link in the security chain – the human component. After tricking employees into clicking or opening various URLs and documents, it's only a matter of time until threat actors download additional malicious components on the victim's machine, move laterally, and exfiltrate data.

Some cyberattacks, attributed to nation-states because of their sophistication or the targeted infrastructure, such as industrial systems or government institutions, are on the verge of being classified as acts of war. Cyberattacks on critical infrastructures belonging to NATO states are even considered to fall under Article 5, declaring a state of war within the Alliance and forcing an in-kind military or cyber response.

The evolution of malware during the past couple of years has strictly focused on financial implications. Ransomware, for example, is a billion-dollar business that has plagued consumers for years and has now moved on to targeting business and large infrastructures. Ransomware is constantly updated to include new obfuscation techniques that make it difficult for security software to spot, and pack encryption optimization features that allow for quick and irreversible file encryption, turning what was once a nuisance into a growing pain.

Distributed through exploit kits that abuse unpatched vulnerabilities in victim's computers simply by visiting a malicious URL, or via spear-phishing emails that contain attachments laced with macros and scripts that download the ransomware from attacker-controlled Command & Control (C2 servers), ransomware usually causes the most data disruptions for organizations. Traditionally, ransomware samples are not bundled in with the actual email attachment or automatically downloaded once a malicious URL is visited. A malicious component first assesses the victim's system for unpatched vulnerabilities or the presence of a security solution. Only afterwards does it connect to a C2 server to download the ransomware or additional components.

To grasp just how popular ransomware is among cybercriminals, it's worth remembering that some ransomware families have even adopted an as-a-service business model with affiliate programs. For instance, **GandCrab, which currently accounts for more than 50% of the ransomware market**, is distributed by affiliates that share revenue with the ransomware's developers, who operate as a software outsourcing organization. Ransomware payments are usually split 60%/40% or 70%/30% between the ransomware developer and the affiliate, meaning developers have the financial resources to keep investing in new capabilities and features, while the affiliate generates revenue simply by distributing the ransomware and waiting for victims to pay.

The second most financially profitable threats are cryptocurrency miners. The Bitcoin craze in late 2017 and early 2018, when the currency peaked at over $19,000 per unit, prompted criminals to steal the currency instead of mining for it. Also, because the computing power needed to mine new cryptocurrency increased exponentially with each new mined unit, threat actors have started going after the computing power of larger infrastructures.

The emergence of CoinHive, a legitimate script-based cryptocurrency miner that could mine Monero cryptocurrency directly in the browser without installing any clients on the victim's machine, was considered an option to traditional ads. Those who visited legitimate websites would share their CPU computing power to mine for Monero for the website owner, instead of having to view ads and commercial banners. However, threat actors quickly abused the script and started exploiting vulnerabilities in popular websites to place the Monero-mining script so users unknowingly mine cryptocurrency.

Again, as complexity for mining new units grew, attackers went after large infrastructures for computing power. Since cloud infrastructures have a huge farm of powerful CPUs, they were quickly targeted. Tesla reported that some of its cloud instances were compromised and used to mine cryptocurrency. Docker images were tainted and deployed by IT admins within infrastructures without knowing they were being used to mine Monero. And even critical infrastructure systems, such as a water utility plant, was used to mine Monero. It became so popular that by late 2017 over **3 million websites** hosted the script, generating over $250,000 per week.

While these three threats have shown a somewhat opportunistic and entrepreneurial approach towards leveraging malware to generate revenue, advanced persistent threats – known as APTs – have also joined the new norm. What sets these threats apart is that both their sophistication and pinpoint accuracy in targeting only select organizations and government institutions. For instance, if the first APT discovered was Stuxnet in 2010, the rate at which new APTs are discovered and analyzed has increased to almost two every month. What makes APTs interesting is that they usually exploit several unknown or zero-day vulnerabilities to infiltrate an organization. For example, Stuxnet was found to exploit up to four separate zero-day vulnerabilities to compromise the infrastructure.

The zero-day vulnerability market has been booming for the past couple of years, with security researchers and black hats rushing to find new ones in both software and hardware. However, not all zero-day vulnerabilities are reported to affected vendors. Some organizations even purchase zero-days for up to $1 million per vulnerability, then sell them to state-actors as part of an exclusive tool kit to be used to compromise systems. Since most of these vulnerabilities are usually triggered via URLs accessed either through mobile devices or traditional workstations, it stands to reason that security teams within organizations are worried not just about malware itself, but also about potentially unknown domains, IPs, and phishing emails.

Challenges that Security Operations Centers Face

A direct consequence for companies of the evolving threat landscape is that security professionals **now face a large number of challenges** in terms of the **complexity raised by tools** used to quickly identify and prevent these threats from infiltrating the infrastructure and having the threat intelligence required to improve and automate their work.

- Cybersecurity skill shortage
- Lack of evidence-based knowledge and context
- Compliance and regulatory issues
- Manual forensic and investigation processes
- Limited expertise with using threat intelligence data
- Understanding and assessing URL, domain, IP reputation and information

A well-documented and global **cybersecurity skill shortage** is a significant concern for 53 percent of IT professionals. Cybersecurity professionals are difficult to find, expensive to recruit and challenging to retain. In today's understaffed environments where these professionals are often overworked, it is critical that Security Operations Centers (SOCs) use technology that enables their analysts. Today's threat actors are well-trained, well-equipped experts in their fields and, if we are to successfully defend organizations against them, we need equally well-trained, well-equipped analysts. Technology should act as a force multiplier for our most critical assets, automating lower-skilled functionality and ensuring that cyber analysts spend their time operating as modern threat hunters, engaging in the type of proactive analysis that is effective below that threshold that tools operate in.

Compliance is also a major concern, as many organizations need to deal with regulatory issues involving security and data handling practices, and even need to set policies and procedures in place. This raises the overall complexity of keeping the company compliant, while placing additional strain on Security Operations Centers, Managed Security Service Providers, Managed Detection & Response companies, and security consultancies. While it's difficult enough for analysts to find and manage the right threat intelligence or automation tools, there's also the added stress of remaining compliant and proving they were compliant during a post-breach investigation.

Threat landscape data is usually scattered across the organization, from servers to endpoints and network telemetry, but it has little value to analysts if it's not centralized, analyzed, and even interpreted in a meaningful and actionable way. Relying on **manual processes** for this is not only time consuming, but also downplays the strategic role and expertise a security team should have in maintaining the overall security posture of the organization.

Of course, this feeds into **the issue of having the expertise to make use of threat intelligence data**. The cybersecurity skill shortage causes delays and inefficiencies, leaving organizations to face serious difficulties in having the right people to deliver security services and the ability to spot and investigate sophisticated threats.

Security professionals often struggle with understanding whether specific URLs or domains are dangerous. The majority of today's threats use URLs and domains as an infection vector when launching or escalating opportunistic or advanced attacks, in addition to more sophisticated phishing, online fraud, and scams.

Understanding the reputation of files, such as those from content delivery networks, is also an issue, as security analysts often seek answers to questions related to whether downloaded files are malicious or clean, or if there is more actionable information available regarding a potentially malicious file before submitting it for analysis. This can help prioritize potential analysis of a file based on how malicious it could be or whether it has been attributed to other advanced malware campaigns.

At a time where all malware, regardless of sophistication, either dials home to a C2 service or is delivered via an IP address that's unknown, it's vital to have ample **information about the reputation of IPs** before assessing whether they're a threat, part of a larger malware campaigns, or part of an advanced attack specifically targeting an organization. Knowing whether the IP address has been previously associated with cybercriminal activity, to which ISP provider it belongs, who registered it, and whether the same company has had other IP addresses associated with cybercriminal activities is the type of threat intelligence that analysts need to make informed decisions when assessing the status of unknown IPs.

Choosing a Reliable Threat Intelligence Vendor

One of the hardest and most valuable lessons learned by the global intelligence community over the last few years has been the value, importance, and reliability of sources. Consumers should be demanding concerning the collection capability of the intelligence provider, as that capability directly influences reliability. Many intelligence feeds are little more than repackaged open-source data collected from publicly available sources, the integrity of which has often been compromised. Unique, validated intelligence from a reliable source allows security teams to make decisions with confidence.

What to look for when assessing a Threat Intelligence solution:

- Easy integration with existing tooling (SIEM, TIP, SOAR)
- Targeted threat intelligence based on company profile
- Predictive and more strategic data
- Demonstrated results

Current threat intelligence vendors still assume too much capability on the part of the customer. Most security teams still struggle to understand their own data and environment. Without the infrastructure to enable customers to consume intelligence and correlate it, in context with their own enterprise, security analysts can't make it actionable. Valuable and actionable **threat intelligence needs to integrate with existing tooling** (SIEM, TIP, SOAR) and help customers extract the true value of the intelligence they provide.

Threat intelligence should also be targeted, and the targeting is driven by Intelligence Requirements. It's true that many customers don't yet understand their intelligence requirements, but the result is an overwhelming firehose approach from vendors, who throw everything they have at customers. Those customers often lack the expertise and capabilities to identify and use the intelligence that is relevant to them. This means that **threat intelligence needs to become more targeted, to specific groups of customers**.

It's up to threat intelligence vendors to do some of the work of defining intelligence requirements for their customers. This should start by initially producing intelligence reports and feeds that are industry specific, but larger organizations need intelligence that is specific to their business, to their intellectual property and to the specific adversaries that would target them.

If intelligence is to be more predictive, it needs to become more strategic. Understanding issues like the strategic intent of an adversary group and the capabilities they have at their disposal can give us clues as to what they will do and where they will go next. This type of information, when used correctly, will allow security teams to take a more proactive approach.

A threat intelligence solution that satisfies all of the above can help security leaders make more informed decisions based on credible risk, and avoid "chasing ghosts". This means that, instead of simply consuming intelligence from multiple sources, a potent **threat intelligence solution needs to demonstrate when it is right and how often it is right, and compare that to its competitors**.

The Value of Bitdefender Advanced Threat Intelligence

Bitdefender Advanced Threat Intelligence delivers contextual, real-time insights into the cyber-threat landscape. From unique, evasive malware, to advanced persistent threats, zero-days, and Command & Control servers that are hard to catch, to the reputation of files, URLs, domains and IPs, this living database of knowledge eliminates a long-standing blind spot for security analysts and enables them to thrive in an increasingly dangerous, complex world of criminal and state-sponsored attacks.

Key capabilities of Bitdefender Advanced Threat Intelligence:

- URL Reputation and Domain Reputation services offer insights into URLs and DNS domains known to spread malware, phishing or other cyber-threats;
- File Reputation services based on hash lookup (md5, SHA) of files known to be part of threats or attacks;
- IP Reputation services offer insights into IPs known to contain various threats, including botnet C&Cs or DoS attacks;
- Advanced Persistent Threats (APT) and Command and Control (C&C) Server Feeds.

The value of Bitdefender's Advanced Threat Intelligence stands out due to the superior efficacy of the telemetry and data processed and analyzed by one of the largest and most respected security R&D centers in the world.

With over **800 security experts**, Bitdefender Cyber-Threat Intelligence Labs have perfected and innovated technologies in over 17+ years of research. The Labs analyze and block approximately **600,000 IoCs**, up to **2 million pieces of malware**, and more than **50 million malicious URLs**, offering technology partners a reliable service based on global threat intelligence sensors.

This scale is a direct result of collecting intelligence from **Surface Web Intelligence, Technical Intelligence,** and even **Dark Web Intelligence**. Bitdefender has gathered dark web data for several years now, with **95,000 unique onion URLs monitored**, plus **6.5 million onions seen by our servers** (including duplicates), as well as **7 million onion visits**, demonstrating the company's technical prowess and continued effort in understanding cybercrime and how threats evolve on an international scale.

To grasp the volume of information that Bitdefender Advanced Threat Intelligence includes, here are some stats:

- 100 million URLs (with 1.1 million URLs cleaned up every month)
- 127 million domains
- 12,000 domains with malware found and added in the repository on a daily basis
- 46,800 URLs with malware or spam per day
- 2,800 new IP records with malware added per day
- 2.7 billion entries in our file reputation database
- 1.06 petabytes of searchable file data
- Information on 143 million unique IPs
- 16 million unique IPs per month
- 500,000 new IPs per day

All this information helps security analysts to **minimize the vulnerability window** between the launch of an attack and deployment of appropriate protection capabilities, and offer real-time protection of the entire infrastructure as soon as a new threat is identified, optimizing resource consumption in terms of overhead.

Bitdefender Advanced Threat Intelligence **improves decision-making** and accelerates incident response and forensic capabilities with contextual threat indicators, enabling organizations to stay ahead of sophisticated threats by accessing accurate, actionable, and relevant threat intelligence. It can also help defend against attacks even before they are initiated, by enabling access to a **global intelligence** outside of the United States to detect targeted, evasive malware and zero-day attacks across the world.

Unifying the **entire Bitdefender technology stack**, including Network Sandbox Analyzer, Network Traffic Security Analytics, cyber-security partners, global law enforcement agencies, and a Global Protective Network (GPN) of over 500 million machines, Bitdefender Advanced Threat Intelligence delivers **top-rated security data and expertise** by leveraging:

- Award-winning anti-spam, anti-phishing and anti-fraud technologies
- IoCs identified on Bitdefender's global install base
- Internal crawling systems
- Email traps, honeypots and data from monitored botnets
- Advanced heuristics techniques and content analysis

- Internal virtual machine farm that executes prevalent malware and collects threat information
- Extensive collaboration with other cybersecurity industry players, international organizations and law enforcement agencies.

Advanced Threat Intelligence is platform-agnostic and compatible with any SIEM familiar with consuming a REST API, allowing organizations to easily integrate threat intelligence data within minutes on any platform or infrastructure.

For security teams interested in trying the new service first, we offer a **no-fee proof-of-concept evaluation** at oemsales@bitdefender.com.

Bitdefender is a global cybersecurity and antivirus software leader protecting over 500 million systems in more than 150 countries. Since 2001, Bitdefender innovation has consistently delivered award-winning security products and threat intelligence for people, homes, businesses and their devices, networks and cloud services. Today, Bitdefender is also the provider-of-choice, used in over 38% of the world's security solutions. Recognized by industry, respected by vendors and evangelized by our customers, Bitdefender is the cybersecurity company you can trust and rely on. Bitdefender is a global cybersecurity and antivirus software leader protecting over 500 million systems in more than 150 countries. Since 2001, Bitdefender innovation has consistently delivered award-winning security products and threat intelligence for people, homes, businesses and their devices, networks and cloud services. Today, Bitdefender is also the provider-of-choice, used in over 38% of the world's security solutions. Recognized by industry, respected by vendors and evangelized by our customers, Bitdefender is the cybersecurity company you can trust and rely on. http://www.bitdefender.com.

Bitdefender-Whitepaper-ThreatIntel-CREAT3470-en-EN