FIREEYE | MANDIANT

ISSUE 12

# THE VISION

INSIGHTS DELIVERED STRAIGHT FROM THE FRONTLINES OF CYBER ATTACKS

## XDR—A TIMELY ARRIVAL FOR THE OVERSTRETCHED SOC

**EDITION HIGHLIGHTS**

Multifaceted Extortion—Definition and Solutions

When it Comes to Threat Intelligence, A Discerning Approach Pays

The Latest Success Stories from The Frontlines

# ARTICLES

All articles in this PDF are hyperlinked. Click or tap on a link to navigate to that article

# XDR—A Timely Arrival for The Overstretched SOC

With security operations experiencing the pain of too many alerts and high volumes of security data, there is a need for real innovation in the SOC and XDR solutions could not have arrived at a better time.

XDR is a hot topic in security operations and for good reason—it promises outcomes, highlighting the investigations that matter to help teams prioritize alerts. XDR ultimately represents the opportunity to approach security operations in a better way, providing deeper integration with security controls and data to improve detection and response, while reducing the pain of expensive and complex security engineering in a user-friendly SaaS format.

Although many SIEMs can collect logs from multiple vendors and technologies, they often require rule writing and content creation to get to results. XDR delivers outcomes as soon as it is deployed.

## The Relevance of XDR

To assess the need for an XDR solution, organizations need to determine the effectiveness of their existing security detection and response program. Consider the following questions:

- Are you satisfied with the effectiveness of your security control environment?
- Are your SOC teams performing well?
- Are your staff overworked or unhappy with the number of false positives they must manage?
- Is your team able to investigate every alert and event generated from your security infrastructure?
- Is your security engineering team feeling over-burdened?
- Is the investment you've put into your systems providing the outcomes you would expect?

## When selecting an XDR vendor, the importance of product evaluation and testing cannot be overstated.

Proof of concept for traditional SIEM solutions was extremely difficult to achieve and this can be the case for many native XDR tools. Consider whether the vendor's product will use your own tools or data, or if it requires a "rip and replace" exercise and a significant level of professional assistance deploy.

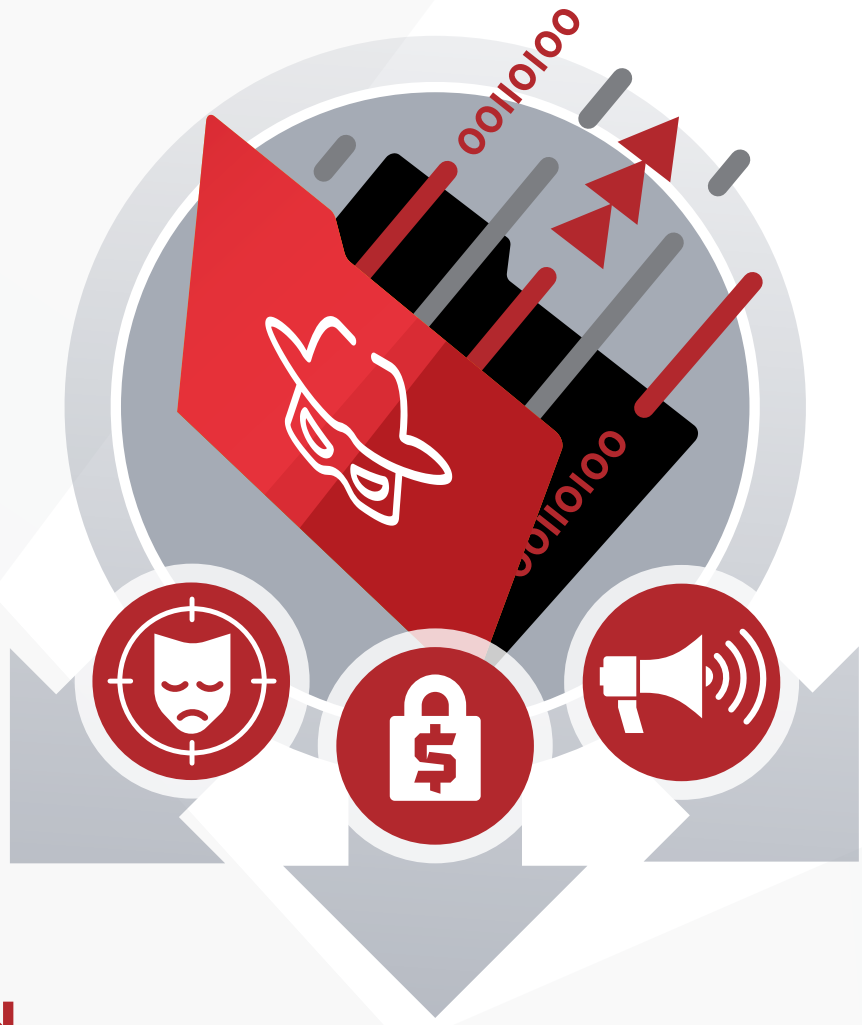
### The Mandiant Approach

Mandiant Advantage preserves and enables your freedom to work with any technology while delivering XDR outcomes. We work with many of the leading endpoint and network security vendors, SIEMs and SOAR platforms. Organizations can therefore choose best-of-breed solutions that work for them, without relying on a single vendor or the need to use tools that are unsuitable. Mandiant Advantage enables organizations to measure the effectiveness of their existing controls and ensure they are configured properly, ensuring our customers get more out of their existing investments and have the data they need to determine which future investments will have the best ROI.

Whether to outsource XDR solutions or not is an important decision because finding and retaining top SOC talent—particularly security engineering—is difficult. This is why Mandiant is constantly developing solutions such as Mandiant Advantage that work with existing tools and eliminate the need for rule writing, content creation and playbook development to make deployment easier. Mandiant Advantage is configured with pre-built data science models designed to investigate the way a Mandiant expert does, operating at machine speed and fortified with timely, relevant threat intelligence. Should a team need help, Mandiant managed services are available on-demand or as a fully managed threat detection and response solution.

**Learn more about the Mandiant approach to XDR**

LEARN MORE >




# Multifaceted Extortion—Definition and Solutions

Multifaceted extortion was one of the standout topics in the latest M-Trends 2021 report. This threat combines traditional ransomware and other extortion tactics to coerce victims to comply with hefty demands. The nature of multifaceted extortion means that standard basic disaster recovery procedures used during a ransomware attack are no longer an adequate recovery strategy.

## Attackers are innovating

The first known ransomware was documented in 1989. The ransomware hid directories and encrypted file names on a victim's computer. Users had to pay $189 to regain access to their files. Since then, attackers have matured their technology and tradecraft to demand sums up to $50M. Today, ransomware spreads quickly through environments and encrypts entire drives, crippling business operations.

Financially motivated threat actors such as FIN11 employ ransomware-as-a-service to carry out their attacks. They outsource code development eliminating the need to maintain that expertise themselves. To maintain anonymity, attackers now demand payment in cryptocurrencies such as bitcoin, making it increasingly difficult to track and locate them.

### The move to multifaceted extortion

Threat actors have realized they can demand higher ransoms by targeting larger organizations and applying additional coercion techniques. Tactics that support multifaceted extortion include:

**Impaired File Availability**
Ransomware typically encrypts a target organization's sensitive files, making them unavailable to legitimate users. This can be combatted with best practices and disaster recovery planning.

**Threats to Publish Data**
Theft of sensitive data is followed by threats to publish the data if the payment demands are not met. This form of extortion is more consequential because data breaches often carry more serious business consequences than service disruptions. According to the M-Trends 2021 report, "A data breach can result in greater reputational damage, regulatory fines, class action lawsuits, and derailed digital transformation initiatives. These consequences were not typically seen with ransomware before 2019."

**Name-and-Shame**
Attackers will post parts of the stolen data on name-and-shame websites to prove they possess the stolen data. The attackers then engage with media organizations to inflict brand damage, further coercing victims into paying a ransom. Some attackers have even notified business partners of data theft, creating friction in third-party relationships and prompting breach disclosures.

## How to protect your organization

Organizations should prioritize and take action to mitigate the risk of ransomware incidents. Based on experience with ransomware attacks through incident response engagements in 2020, Mandiant experts have observed several commonalities:

- Large numbers of highly privileged accounts in Active Directory
- Highly privileged non-computer accounts configured with service principal names (SPNs)
- Security controls not configured to minimize the exposure and usage of privileged accounts across endpoints
- Attackers modifying Group Policy Objects (GPOs) for ransomware deployment

Hardening these environments will allow you to better defend your organization from ransomware. Full ransomware resiliency combines solid defenses with technical and process-oriented controls to enable recovery and reconstitution.

A full incident response investigation should take place alongside recovery efforts, with special care to reduce the likelihood of an attacker maintaining access. This is to reduce the continued risk of future attacks.

**For details, read the full M-Trends 2021 report or access our Ransomware Defense Assessment.**

ACCESS THE REPORT >

# When it Comes to Threat Intelligence, A Discerning Approach Pays

As attacks become more sophisticated and complex, security teams have actively sought to increase the number of threat intelligence vendors used to gain improved visibility into the threats targeting their specific organization or industry.

Organizations currently subscribe to an average of 7.5[1] threat intelligence services, up 44% from 2018. This increase highlights the growing importance placed on threat intelligence by security practitioners and recognizes the benefits of threat intelligence in the ongoing fight against cyber crime.

Although the statistics seem like a positive step forward, the increase of threat data from multiple vendors contributes to information overload in the SOC. This can lead to serious vulnerability problems. Threat intelligence data is not actionable without context and piling data on top of more data does not give organizations greater protection against the latest threats; it simply tasks security teams with hours of analysis.

Historically, comparing threat intelligence providers has not been easy, but the recent Forrester report compares 12 vendors, each of which have the following in common:

- They are large, global organizations that offer a comprehensive combination of vulnerability, brand and cyber threat intelligence
- Revenue gained from threat intelligence services represented at least $10m per annum, generated by servicing over 100 clients
- Vendors employed an extensive threat intelligence team with a diverse set of skills and cultural backgrounds

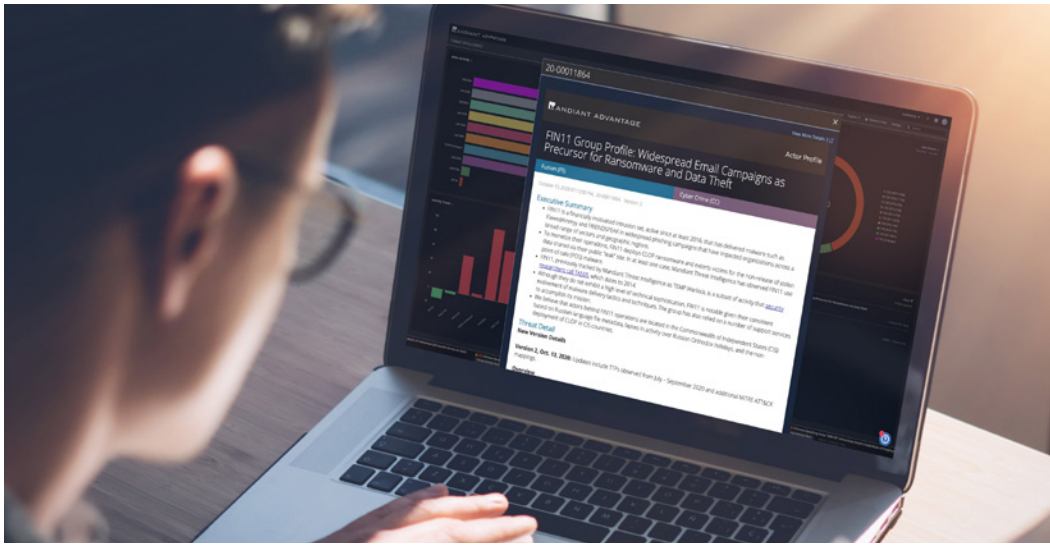
1 Forrester (March 23, 2021). The Forrester Wave™: External Threat Intelligence Services, Q1 2021

The 12 evaluated organizations were scored against 26 different criteria including: intelligence analysis, vulnerability intelligence, eliciting intelligence requirements, cyber threat intelligence, strategic partners, innovation roadmap and product vision. The criteria were grouped into three high-level categories that indicated the strength of each vendor's current offering, strategy and market presence.

The report, published earlier this year, cites FireEye's position as a leader in threat intelligence. FireEye received the highest possible scores in 18 of the 26 criteria. The Forrester report comments:

**FireEye-Mandiant's strength in threat intelligence is in large part due to the reputation and visibility provided via the company's robust incident response consultancy, security controls business, and managed security services. The visibility gained from those supporting services is ahead of the pack.**

**— The Forrester Wave™: External Threat Intelligence Services, Q1 2021**




While attackers are constantly looking for ways to evade or defeat security measures, adapting as they are discovered or when their tactics stop working, threat intelligence collection must also develop new ways to track threat actors. FireEye Mandiant continually innovates its methods of data collection, investing heavily in human expertise around the world. Our team of 260 researchers generate thousands of reports, curating data from four sources:

### Breach intelligence

Over the last 15+ years, we have gained a reputation as the industry's premier incident responder, attending 800+ incident response engagements annually.

### Machine intelligence

We have approximately four million virtual guest images deployed globally in 102 countries, generating tens of millions of sandbox detonations per hour, confirming 50,000 - 70,000 malicious events per hour.

### Operational intelligence

Our Managed Defense team performs detection and response services for over 300 customers from four international Cyber Threat Operations Centers, ingesting 99 million+ events and validating 21 million+ alerts.

### Adversary intelligence

We collect up to one million malware samples per day from more than 70 different sources.

FireEye Mandiant has a unique view into the threat landscape. The four different lenses used to analyze adversaries help us track threats throughout their lifecycle. While many threat intelligence vendors regurgitate the data they collect and leave SOC teams and analysts to sift through it, Mandiant Threat Intelligence applies unique algorithms and expert opinion to the data, transforming it into contextualized, actionable threat intelligence, complete with an M-Score—Mandiant's in-house scoring system which rates the confidence level in each threat. Our browser plugin, search and filtering features enable users to access the latest threat intelligence whenever they need it, without undertaking hours of data processing.

## FireEye offers some of the best threat intelligence.

**— The Forrester Wave™: External Threat Intelligence Services, Q1 2021**

Innovation and advances in technology are removing the need to stockpile threat intelligence data from multiple vendors. Instead, research the right vendors and ensure they deliver the tools you need to inform your team of the latest threats to your organization. This can considerably ease the burden on the SOC, giving teams more time to undertake proactive activities such as threat hunting.

**Read the full Forrester Report**

READ THE REPORT >

CUSTOMER PROFILES

# The Latest Success Stories from The Frontlines

## Kyriba

The FinTech enterprise Kyriba provides a broad range of SaaS solutions that enable customers to manage their mission-critical capabilities for cash and risk management, payments and working capital optimization. The team needed a solution that was able to effectively triage and streamline their event monitoring, capable of handling over 9 billion events every month. Read why Kyriba selected Mandiant Automated Defense to increase their security team's capacity and support rapid corporate expansion plans.

READ ON >

## Corix

When a cyber attack swept the globe in 2016, the security team at leading utility provider Corix rallied to successfully defend itself against vulnerabilities. In the process, they uncovered how difficult it would be to respond to a major attack. After identifying the need to bolster their team, their search for a strategic partner to provide an end-to-end solution and managed detection and response service led to FireEye. Read how FireEye has been working in partnership with Corix to build a robust security program that assures the safety of the communities it serves.

READ ON >

FIREEYE™ | MANDIANT®

We hope you enjoyed this edition. Get the latest cyber security news from the frontlines by reading The Vision online.

**vision.fireeye.com**

Get in touch to find out how our security solutions can help protect your organisation.

**contact-us@fireeye.com**

**www.fireeye.com**