What is Threat Detection and Response?

Attackers nowadays are good at setting up camp in networks and stealing important information. This means you need to be on your toes with top-notch threat spotting.

You need something that can handle the whole attack process, from when they first break in to when they move around and take data.

32% of cyber-incidents that involved data theft and leak, indicated that more attackers favor stealing and selling data, rather than encrypting it for extortion pointing to a critical need for implementation of robust threat detection.

Threat detection and response (TDR) defined

What is Threat Detection?

Threat detection is the process of monitoring a security ecosystem holistically in order to identify hostile users, aberrant activities, and anything else that may compromise a network. Threat detection is based on threat intelligence, which includes tools that are strategic, tactical, and operational. Threat detection and response tools focus mostly on very evasive cyber threats.

What is Threat Response?

Threat response refers to the mitigation efforts taken to neutralize and prevent cyber threats before they cause vulnerabilities. These efforts continuously monitor systems and generate alerts when cyber threats or malicious conduct are detected. Threat response is also based on threat intelligence.

“Threat detection and response is a cybersecurity process that examines user behavior to identify attacks, prevent breaches, and improve endpoint security, hence enhancing overall security.”

How does Threat Detection and Response Work?

Most organizations rely on a SOC to battle the progression of cyber threats and other security issues. This centralized team enhances your firm’s overall cybersecurity through the prevention, detection, and response to threats.

A SOC is not only just reactive but keeps watch for emerging cyber threats and identifies vulnerabilities in the organization. Most onsite and outsourced SOC teams operate twenty-four hours a day, seven days a week.

The SOC uses threat detection and response tools combined with threat intelligence to detect any attempted, successful, or in-progress breaches. In fact, when the security team detects a cyber threat, they take measures to eliminate or mitigate the problem. Human expertise is crucial in interpreting alerts related to detected threats and integrating these threats into incident response workflows to mitigate security breaches.

4 Keys to Automating Threat Detection, Threat Hunting and Response

- Maturing Advanced Threat Defense
- 4 Must-Do’s for Advanced Threat Defense
- Automating Detection and Response

[Download the Whitepaper Now!]

This is how the process of threat detection and response usually works:

- **Detection**

The first step of cyber security detection and response is risk detection and possible breach identification. Security tools monitor everything – endpoints, identities, networks, apps, and even the cloud environments. Advanced threat detection and response tools also help teams discover complex cyber threats that might otherwise slip through.

- **Investigation**

  Once the threat is detected, the SOC acts to verify the validity of the threat. Using AI and other technologies, they ascertain how the breach happened and then evaluate which company assets are actually affected. This is a huge part of threat detection investigation and response.

- **Containment**

  They would therefore eliminate the access of the infected devices, identities, or networks to the rest of the organization to prevent further damage. This terminates the cyber attack process.

- **Elimination**

  After containment, the SOC would remove the cause of the breach. They would, therefore, strive to ensure that the bad actor is fully wiped out of your environment and patch vulnerabilities that could lead to a related attack in the future.

- **Recovery**

  Once the SOC is satisfied that the threat has been neutralized, isolated systems and devices that were affected are put back into service.

- **Incident Report**

  Incident teams will document the event and report to their leaders, executives, or even the board depending on the gravity of the incident. The objective here is to try and paint a vivid picture of what happened and how it was addressed.

- **Risk Mitigation**

  The SOC also sees this incident as a learning experience. They reflect on what can be done better and what needs to be improved so that they build an environment that could stop the next attack before it even begins. Continuous process improvement helps streamline the overall threat detection and response solutions in any organization.

With this, your organization will not only be able to react to cyberattacks but also strengthen its defenses going into the future. The good news, having a well-defined threat detection and response strategy, really makes all the difference when it comes to reducing risk and staying out ahead of threats.

What are the 5 Best Types of Threat Detection?

Extended Detection and Response (XDR)

XDR is a solution for security operations teams that could identify, order, and remediate threats

with more efficiency from the standpoint of endpoints, networks, email, cloud workloads, and lots more.

Read more about XDR

Network Detection and Response (NDR)

An NDR solution keeps tabs on and identifies suspicious traffic over the network infrastructure with the help of AI, ML, or other non-signature-based approaches. Organizations utilize various methods, such as continuous monitoring and human expertise, for detecting threats in real time

Read more about NDR

Endpoint Detection and Response (EDR)

EDR solutions continually monitor and gather data at endpoints and apply rules-based automated responses. EDR is an endpoint security product that helps to safeguard an environment's perimeters.

Read more about EDR

Email threat detection

Email threat detection is offered as a standalone product or as an integral part of XDR solutions. Email threat detection scans emails to detect, quarantine, and contain inbound, outbound, or internal messages.

Read more about Email Threat detection

Vulnerability Management

VM refers to the process of finding and tracking, researching, prioritizing, and rectifying known and unknown vulnerabilities in the IT system and infrastructure before or after an exploit has occurred.

Read more about Vulnerability Management

4 Threat Detection and Response Challenge

The more assets your organization puts into the cloud, the more damage it will be open to from cyber-attacks, especially with regard to data breach incidents. Following are five of the major challenges you will have to face in threat detection and response-illustrated with examples aimed at identifying and addressing them:

1. Endpoint Protection

Considering remote and hybrid work arrangements are almost becoming the new normal, you probably have your work cut out for you when it comes to keeping track of all of those devices that are accessing your network.

For example, one of your workers works remotely using a personal laptop that is not fully secured. If it gets compromised, then they may get an entry point up to your sensitive data. That

is why you need strong cyber security detection and response strategies in place to ensure you have full visibility and control over all endpoints.

2. Network Detection

Your network is probably more complex than it's ever been, and it's tough to try to keep track of every device and every connection. You might also be encrypting more traffic in order to keep data secure, but that same encryption can blind you from detecting the hidden threats. Visualize an attacker concealing malware inside that encrypted traffic-without the proper threat detection and response tools, you may not find it until it is too late.

3. Unidentified Threats

With the rise of AI and machine learning, you are up against new types of cyber threats that are actually designed to slip past traditional methods of threat detection. For example, an APT might sit inside your network for months stealing valuable data without ever setting off any alarm. This is where it becomes so important to understand what threat detection and response is-and take extra measures to ensure your threat detection and response solutions are up to the task.

4. Tool Sprawl

You could be working with several cybersecurity tools to operate threat detection, investigation, and response, but a lot of unconnected tools create inefficiencies. Imagine running different networks for monitoring endpoints, performing threat intelligence, and having poor interactions among these systems.

Poor integration will leave your responses slow to the identified threats for your organization. It is for this reason streamlined threat detection and response solutions are critical.

What Threats Do TDR Solutions Detect and Contain?

Threat detection and response (TDR) solutions are the eyes and ears of your cybersecurity team-consistent alerting to identify and disrupt cyber threats before they can cause significant damage. Traditional prevention tools often miss the mark, while advanced threat detection and response technologies can catch even the most elusive cyber threats that normally fly under the radar.

In fact, TDR tools lie at the very heart of your cybersecurity detection and response strategy. They provide real-time visibility into stealth attacks and help drive down your response time to levels that minimize business disruption and risk. Let's dive deep into what kinds of threats a Threat Detection and Response solution can help you find and contain:

- **Malware:** Spyware, Trojans, and other types of viruses-the catch-all term for malicious software that infect systems and networks in order to steal data within them.
- **Ransomware:** A particularly odious type of malware used by cyber bad guys to lock up important business data, exfiltrate it, and then threaten to sell unless a ransom to decrypt or not sell is paid.
- **Phishing:** This is very often the first step in any larger attack. Essentially, phishing tricks users into divulging sensitive information such as their login credentials. Later on, this information is used to install malware or breach systems.
- **Denial of Service (DoS):** A DDoS attack will flood your systems with traffic. It can overload your services and bring down servers.
- **Botnets:** These are the infected device networks that, rather commonly, are utilized by

the attacker for spamming, DDoS attacks, data theft, and even cryptojacking.
- **Advanced Persistent Threats:** Long-term, focused cyber-attacks allow malicious actors continuous access to a network for long-term exfiltration of data.
- **Zero-day Threats:** Security vulnerabilities that developers have not yet discovered. They are the most dangerous ones because patches for them are not available.
- **Living-off-the-Land (LotL) Attacks:** Bad actors use legitimate tools already on your network to do their dirty work by taping legitimate programs to perform malicious activities. That makes such an attack much harder to detect.

Key benefits of Threat Detection and Response

It can be noted that effective threat detection and response can help an organization improve its resilience and minimize the impact of breaches in the following several ways.

Early threat detection

One of the most crucial ways to reduce the impact of an incident is by stopping cyber threats before they actually become a full breach. With the aid of modern detection and response tools and a dedicated team, SOCs increase the chances that they will find threats early when it is more manageable.

Compliance with Regulations

Countries and regions are enforcing strict privacy legislations that require strict data protection controls and procedures to detect, respond, and remediate security breaches. A non-compliant company can incur massive penalties. A threat detection and response program enables organizations to adhere to the mandates of these regulations.

Increased Detection Efficiency

The most destructive cyber-attacks typically originate from those incidents in which the bad actors spent the most time undetected within a digital environment. This dwell time needs to be reduced as much as possible to limit damage. Threat detection and response processes, like threat hunting, help SOCs detect such bad actors earlier and limit their impact.

Improved visibility

Tools that protect from known bad and unknown threats, like SIEM and XDR, will give security operations much more visibility into their environment, so they don’t only detect them early but also find vulnerability items like old software to be replaced.

Data protection of sensitive data

Data is often one of the organization’s most valuable assets. The proper detection and response tools and procedures in place help security teams catch bad actors before they have access to sensitive data, thus bringing less chance for this information to be released or sold on the dark web.

Proactive Security Posture

The concern of threat detection and response is also able to highlight emergent threats and what the malevolent actors are seeking or looking for to gain entry into the digital environment of an organization. This offers insights to SOCs to strengthen the organization and prevent the progression of attacks.

Cost savings

Organizational costs of a successful cyber attack can literally go very high, in terms of the actual money spent on ransom, regulatory fees, or recovery efforts. It can also lead to lost productivity and sales. With the detection of threats and their responses at the very early stages of the cyberattack, the costs could be cut for organizations on security incidents.

Reputational management

A breach of personal data – especially one that is very high-profile in nature – can cause severe reputational damage to companies or governments. People stop trusting other institutions they don’t believe handle personal information well. Threat detection and response can help decrease the chances of a newsworthy incident and provide customers, citizens, and others with confidence that personal information is indeed protected.

Threat Detection and Response Capabilities and Features

When it comes to threat detection and response (TDR), having the right features and capabilities in place is crucial to minimizing risk and keeping your organization safe. An effective TDR program represents multiple strategies and technologies running together in keeping your organization safe. Below are the components that make up a capable TDR solution:

Real-Time Monitoring

One of the most fundamental capabilities of threat detection and response is real-time monitoring. In this way, you can catch the first signs of some suspicious activity or IOCs before they blow out of proportion. Real-time monitoring integrates with SIEM systems in order to correlate events for effective threat detection.

Threat Intelligence

Another piece of the puzzle is threat intelligence. It feeds into your TDR about the newest tactics, techniques, and procedures that are being used by cybercriminals. For this reason, integrating your cyber security detection and response tools with threat intelligence feeds enables these to identify and spot arriving threats in an instant.

Threat Hunting

Waiting for threats to come to you isn't enough anymore. That's where threat hunting comes in. TDR tools don't just react; they actively search for signs of trouble, like IOCs or anomalous activity. This proactive approach helps you catch breaches—or signs of breaches—before they can cause too much damage.

Root Cause Analysis

Once you've identified a threat, the next step is figuring out where it came from. That's what root cause analysis is all about. With TDR, you get forensic capabilities that allow your security team to dig deep and understand the origin of an incident, which is key to preventing future attacks.

Sandboxing

Since sandboxing safely analyzes suspicious files or code, TDR solutions generally include this feature. Let's allow running potentially malignant code in a safe environment where it simply cannot do any harm. Your team can assess the threat-apply analytics and machine learning-and let the sandbox do its work without putting your network at risk.

Fidelis Sandbox: Malware Detection in the Cloud or On Premise

- Understand malware behavior
- Share malware forensics
- Detect Threats that Other Tools Miss

Download Datasheet

Automated Response

Speed is everything in threat detection, investigation, and response. That’s why TDR platforms often come with automated response capabilities. These can isolate and block threats almost instantly, reducing the time it takes to detect and respond to an attack. Integration with security orchestration, automation, and response (SOAR) platforms further enhances this, making your TDR practice even more efficient.

Vulnerability Management

Finally, good vulnerability management lies at the very heart of effective threat detection and response. Finding and remediating the weaknesses in your systems is crucial to prevent the bad guys from leveraging them. This forms one of the major components of any advanced threat

detection and response strategy.

Advanced Threat Detection Techniques

In the ever-evolving landscape of cybersecurity, advanced threat detection techniques are essential for identifying and mitigating sophisticated cyber threats that traditional security measures might miss. These techniques leverage cutting-edge technologies and methodologies to stay ahead of malicious actors.

1. **Machine Learning and Artificial Intelligence**
2. **Behavioral Analysis**
3. **Anomaly-Based Detection**
4. **Predictive Analytics**
5. **Threat Intelligence Integration**

4 Threat Detection and Response challenges

Despite the advancements in threat detection and response technologies, security teams face several significant challenges in identifying and mitigating cyber threats. Here are four of the most pressing challenges:

1. **Volume and Complexity of Data**: Modern systems and networks generate an overwhelming amount of data. The sheer volume and complexity make it difficult for security teams to sift through and identify potential threats. Effective threat detection requires advanced tools and techniques to manage and analyze this data efficiently.
2. **Evasive Threats**: Sophisticated cyber threats are designed to evade traditional security measures. These threats, such as advanced persistent threats (APTs) and zero-day exploits, can remain undetected for extended periods, causing significant damage. Advanced threat detection techniques are essential to uncover these hidden dangers.
3. **Limited Visibility and Context**: Security teams often struggle with limited visibility into system and network activities. Without comprehensive context, it becomes challenging to identify potential threats accurately. Enhanced visibility through continuous monitoring and integrated security solutions is crucial for effective threat detection and response.
4. **Resource Constraints**: Many security teams operate with limited resources, including personnel, time, and budget. These constraints can hinder their ability to respond to threats promptly and effectively. Automating routine tasks and leveraging AI-powered tools can help alleviate some of these resource challenges, allowing security teams to focus on more complex and high-value tasks.

Threat Detection and Response Best Practices

Organizations with effective threat detection and response develop practices that help their teams work well together, as the effort and cost of cyberattacks is reduced. Here’s how it goes:

Maintain Regular Training

While the SOC team carries much of the responsibility to protect your organization, everyone in the company has a role to ensure organizational security. Most security incidents begin with an employee being a victim of a phishing scam or using an unapproved device. Your entire workforce will always be updated on possible threats, and they will be able to notify the security team when something seems not to add up. More importantly, it keeps your security professionals on top of what is new in terms of tools, policies, and detection and response

procedures against threats.

Create Incident Response Plan

When a security incident finally occurs, things can escalate pretty fast. There is always less guessing about how to handle it when there is a well-defined incident response plan. It should contain containment, eradication, and recovery stages. It further gives HR, communications, legal, and senior leadership clarity to determine how they may need to communicate via updates as accurately as possible to both employees and other stakeholders in relation to regulatory compliance. This is a kind of structured approach toward strengthening your overall cyber security detection and response.

Promote Strong Collaboration

Effective threat detection, investigation, and response rely heavily on good cooperation and communication between your security team. Everyone must be on the same page regarding how threats are to be valued and addressed. Beyond the SOC, collaboration should extend to other departments that can help in identifying threats or assist in the response efforts. Building this teamwork makes it easier to stay ahead of emerging threats and coordinate an effective advanced threat detection and response.

Continuously Improve

Each security incident is a learning experience and an opportunity for improvement. As soon as you close an incident, take time to reflect on what went well and what didn't. Make updates to your process and close vulnerabilities accordingly. Threat detection and response solutions such as XDR can facilitate that by making post-incident security improvements part of the workflow, so you're always in the best position to optimize your security posture.

How to Start your Threat Detection and Response Practice?

- ### Security Posture Assessment

  Find vulnerabilities as well as gaps in your present security setup. Utilize Fidelis Elevate for broad visibility and detection to fill the gaps.

- ### Set Objectives

  Well-defined objectives, such as a reduction in mean time to respond and improvements in visibility, are some examples. Realize these goals using highly customized capabilities for threat detection and response with Fidelis Elevate and Fidelis Network.

- ### Installation of Detection Solutions

  Install real-time tracking, quick response to threats with Fidelis Endpoint and Fidelis Network. Protect your network using the threat detection and response solution – analytics strength with automated response tools.

- ### Develop an incident response plan

  Develop a plan to detect and recover from any incident. Engage Fidelis Elevate for

efficient incident management through automated threat response and streamlined workflows.

- **Monitor and Improve**

  Continue improving your security measures from time to time. Fidelis Elevate gives continuous improvement and continuous threat intelligence so that one does not lag behind emerging threats.

Give Us 10 Minutes – We'll Show You the Future of Security

See why security teams trust Fidelis to:

- Cut threat detection time by 9x
- Simplify security operations
- Provide unmatched visibility and control

Book a Demo Now!

Frequently Ask Questions

How TDR differ from traditional security?

Traditionally, security is based on a rule-based detection and siloed tools, whereas TDR relies on advanced analytics, automation, and integration across multiple sources such as endpoints and networks to get the threat either prophylactically or inaccurately detected and responded. TDR reduces the manual work and increases the efficiency of identifying the threats.

What is Advanced Threat Detection and Response?

Advanced threat detection encompasses the methodologies and instrumentation applied by security professionals to detect advanced persistent threats that involve far-reaching, sneaky type of hacks in order to create damage over a long time period. Such threats are usually more critical and may feature espionage or data theft.

What is the difference between TDR and SOC?

TDR focuses on threat identification and response processes using automated tools and threat intelligence. A SOC is a team or facility responsible for managing total security, including monitoring, analysis, and incident response, which usually use TDR solutions as part of their operations.

What is the difference between TDR and EDR?

TDR stands for threat detection and response – the process of identifying cybersecurity threats to an organization and acting on those threats in a way that begins to address and mitigate them before they actually cause real damage. EDR stands for endpoint detection and response, the category of software products which monitor all endpoints of an organization for potential

cyberattacks, surface those cyberthreats to a security team, and automatically respond to specific types of cyberattacks.

What is the difference between detection and incident response?

Threat detection refers to the identification of potential security threats. Such can include an activity that may be an indication of compromise in a device, application, network, or identity. While incident response refers to the steps that are undertaken by the security team and automated tools to contain and eliminate the cyberthreat.