Secureworks®

WHITE PAPER

Improving Detection with XDR

How XDR Provides the Next Level in Detection Capabilities

Cybersecurity demands constant vigilance and innovation, especially when it comes to detecting ever-evolving cyberthreats. Extended detection and response (XDR) solutions lead the charge, demonstrating clear advantages in holistic detection capabilities over legacy endpoint detection and response (EDR) tools.

There are many reasons why XDR platforms have become the new standard in cybersecurity, but one of the most important is their detection capabilities. Threat actors are constantly upping their game when it comes to clandestinely slipping into your network, and security analysts need a cybersecurity platform that can outpace the adversary while helping detect threats before they become major problems.

XDR offers visibility across your entire attack surface in a unified view while discovering new and emerging threats. This capability is an obvious leap in detection technology compared to pure endpoint tools and other previous technologies. However, not all XDR platforms are created the same, and one critical area where this is true is in detection capabilities. Understanding the advanced detection capabilities an XDR offers will help you choose the right platform for your security needs.

Key Attributes of Advanced Detection in XDR

There are several important elements to advanced detection in XDR that a solution must have:

- Diverse data sets
- Detection logic based on:
  1. **heuristic correlation**
  2. **Tactics, Techniques and Procedures (TTP) specificity**
  3. **confidence, and**
  4. **speed**
- Continuous enhancements

Let’s look closer at each of these areas.

Diverse Data Sets

One of the primary benefits of XDR is its ability to integrate a wide array of data sources, including endpoint data, network information, and cloud telemetry, which in turn gives you heightened visibility into potential threats. By analyzing information from various vantage points, it's possible to spot emerging threats that remain undetected by traditional tools that often limit their scope to pre-defined parameters. This comprehensive coverage is critical because it allows for the early detection of new, sophisticated threats that may otherwise go unnoticed until it's too late.

Diverse data aggregation also creates efficiency in the detection process. XDR's ability to correlate and contextualize events across different environments leads to a more streamlined approach to identifying security incidents. Instead of piecemeal analysis, XDR provides a cohesive, integrated perspective that greatly reduces the time spent on detecting threats. This helps security teams address and mitigate risks faster.

XDR provides a cohesive, integrated perspective that greatly reduces the time spent on detecting threats.

With access to diverse and richer data, security analysts can also achieve a more precise analysis, and in turn, more accurate threat detection. The comprehensive view provided by various data points allows for enhanced analytics that can distinguish between false positives and genuine threats with better precision. This accuracy is vital in sustaining a secure cyber environment and ensures that security resources are allocated effectively.

Ultimately, the diverse data utilized by XDR contributes to a robust security posture. Organizations can recognize patterns and identify potential anomalies with a broad set of data at their disposal. This recognition capability isn't just about responding to immediate threats; it's also about comprehending and adapting the organization's security strategy over time to anticipate and preempt future attacks.

Detection Logic

There are many common, unsophisticated attacks that can be identified simply and immediately with signature-based detection. However, relying on signature-based detection exclusively is no longer sufficient in the face of today’s advanced threats. Threat actors have become way too adept at crafting complex, nuanced techniques that evade conventional signature-based detection. They make subtle changes to their executables. They hijack legitimate network activity to mask their behaviors. They modify audit logs that might have left telltale indicators of their movement across your environment.

Advanced detection logic has become critical to a strong cybersecurity posture. Detection logic, after all, is ultimately the means by which the diverse, massive volume of telemetry generated by all the disparate components in your environment can be interpreted to reveal indicators of something amiss. So the better your detection logic is, the safer your organization will be, and it should have **four key attributes**:

Advanced detection logic has become critical to a strong cybersecurity posture.

1. Heuristic correlation

"Heuristic correlation" refers to detection logic that can identify relationships between multiple pieces of telemetry to determine that some type of malicious activity may be occurring in your environment. This correlation is critical because threat actors may be able to mask specific individual aspects of their activity — such as the hash of a file that they use — but it's nearly impossible for them to conceal the combination and sequence of behaviors necessary to pull off their exploit-of-choice.

2. Tactics, Techniques and Procedures (TTP) specificity

Stopping a threat actor takes more than just knowing they are in your system. You also need a reasonably accurate assessment of the specific type of attack they're trying to pull off — and how far that attack has progressed. Your detection logic's ability to perform heuristic correlation should be complemented by rich threat intelligence that can map the telemetry relationships it discovers to known TTPs.

3. Confidence levels

The ability of your detection logic to generate alerts when it detects suspicious combinations of telemetry has to be balanced against the need to avoid excessive false positives — which can significantly undermine the performance of SecOps teams. As with all good heuristics, the interpretations it provides should be complemented with a level of confidence.

4. Speed

When an attack is underway in your environment, it's important to act quickly. Your detection logic has to work fast. It can also work incrementally, so you can act on whatever aspect of the attack is known now — and then act on other aspects of the attack later when your detection logic can provide additional insight with a suitably high degree of confidence.

Consider, for example, a threat actor that follows its initial compromise with some sort of “man in the middle” exploit that captures legitimate user account credentials in order to further move laterally through your environment in search of your organization’s high-value assets. Those “man in the middle” exploits are notoriously difficult to detect, because they so closely resemble normal network activity. But they also represent a key moment in any attack — since once a threat actor successfully hijacks the right credentials, they can make very rapid progress towards their goal.

If your detection logic can identify “man in the middle” activity from a very subtle combination of disparate telemetry data-points — and if you can act decisively to interdict that attempt at credential capture before the attack can pull it off — it won’t matter that you didn’t yet precisely identify everything about the threat actor’s larger plan or intent. You will have effectively protected your organization by acting on the right information at the right time.

Continuous Enhancement

Whatever platform you use, detectors and their associated severity parameters should be continuously updated based on threat research and the empirical feedback generated from customers’ environments. This allows the detection logic to be continuously refined and keep up with threat actors’ ever-evolving behaviors.

Detectors and their associated severity parameters should be continuously updated based on threat research and the empirical feedback generated from real-world environments.

The Secureworks Taegis™ XDR platform has these guiding principles built into it as well as the four key attributes to advanced detection discussed earlier. We invest significant resources into ensuring that the detection logic we build into our Taegis XDR platform is second to none. Because we operate our own world-class threat intelligence operation, we’re able to quickly develop up-to-date insights into the latest cyber-maneuverings of both cybercriminals and state actors. And our mega-scale threat mapping engine scans trillions of telemetry events across thousands of data categories to uncover even the most subtle data relationships that can serve as indicators for the Taegis platform’s detection logic.

We also get those new enhancements to the platform’s detection logic into production quickly — so that customers are better protected against even the newest attack exploits we discover in the wild.

Examples of Advanced Detection Mechanisms

You may find it helpful to see how Taegis detection logic addresses specific types of threats. Before sharing specific examples, let's cover **two technical aspects of detector creation** that apply across all threat types:

1. MITRE ATT&CK mapping

Every threat vector is characterized by several different technical techniques common to that vector. For each threat below, you'll see the MITRE ATT&CK that we associate with that vector to ensure we're exercising appropriate technical precision in both our definition of that vector and in the data we incorporate into Taegis XDR's detection logic.

2. Data sources

The data that Taegis uses in its detection logic can be generally taxonomized into four categories:

- **Taegis Watchlist:** The Taegis Watchlist is comprised of single-event data types that our threat research team has determined warrant some level of attention – even if by themselves and without any other associated data points that inherent severity level is very low.
- **File analysis:** File contents and hashes can also provide a detection data point that can range in severity from very high to very low.
- **Taegis NDR:** Taegis NDR data points are essentially signatures of network activity that can be indicative of malicious behavior in the target environment.
- **Tactic Graphs™:** Tactic Graphs are an effective means of identifying the often subtle relationships and correlations between seemingly disparate events, telemetry and behaviors that serve as indicators of malicious activity.

Here is how Taegis detection logic leverages these **four data types** across the top three initial access vectors[1], in the context of MITRE ATT&CK techniques.

1. Commodity malware distributed via phishing

Phishing and/or other social engineering techniques represent a primary initial vector for attacks that depend on the introduction of commodity malware into the target environment. This class of initial attack vectors is commonly associated with five MITRE ATT&CK techniques: spearphishing attachments (1566:001), spearphishing links (T1566:002), user execution (T1204), autostart execution (T1547) and command/scripting interpretation (T1059).

[1] Secureworks 2023 State of the Threat Report: A Year in Review

Taegis XDR detection logic for phishing-enabled malware insertion is based on 2,200+ Taegis Watchlist data points, 450+ file identifiers, 1,100+ network activity signatures and the telemetry relationships uncovered in 25+ Tactic Graphs — each of which may assess the density of correlations across billions of data points.

As an example of one such rule, a Taegis XDR Tactic Graphs Detector looks for multiple email recipients receiving malware from the same sender within a given timeframe. Three users receiving the same file within a 12-hour window drives a higher severity alert with a higher confidence level than any individual instance would.

2. Scan and exploit

Another common attack vector of concern to SecOps teams is discovery and exploitation of a vulnerability somewhere in their organization's software stack. MITRE ATT&CK techniques associated with this vector are network service discovery (T1046), exploitation of remote services (T1210), exploitation for privilege escalation (T1068), exploit public-facing application (TT1190) and exploitation for client execution (T1203).

Taegis XDR detection logic for this vector is based on 1,100+ Taegis Watchlist data points, 450+ file identifiers, 2,900+ network activity signatures, and nine vector-specific Tactic Graphs. The comparatively high number of network signatures is logical given that would-be threat actors have to engage in so much scanning activity in their search for vulnerable systems.

Here, too, Taegis has a threshold that triggers a high-severity alert when multiple indicators occur within a given timeframe. But instead of three in 12 hours (as is the case with phishing), the more appropriate, empirically backed threshold is five scanning detections within just 15 minutes.

3. Stolen credentials

Stolen credential attacks can relate to several different MITRE ATT&CK techniques — from brute force (T1110) and unsecured credentials (T1552) to credential dumping (T1003) and the stealing or forgery of Kerberos tickets (T1558).

Taegis XDR logic for the detection of credential-based attacks is based on 600+ Taegis Watchlist data points, 400+ file identifiers, 400+ network activity signatures, and 40+ vector-specific Tactic Graphs.

In this case, rather than being enhanced by particular time-and-frequency threshold, Taegis XDR applies its own native geolocation logic to detect so-called “Superman” logins that are too far apart geographically to make sense within their timespan — as well as other indicators (such as the country from which the log-in was initiated) to drive escalation of the resulting alert.

Raising the Detection Bar with XDR

It’s clear to see how the diverse data utilized by XDR contributes to better detection and a robust security posture. It allows for increased coverage, efficiency, accuracy, scalability, and cost-effectiveness, which are essential for combating ever-emerging and advancing cyber threats. As the digital realm continues to expand, the ability to correlate and interpret data from multiple sources will remain a critical component of effective cybersecurity strategies.

As the digital realm continues to expand, the ability to correlate and interpret data from multiple sources will remain a critical component of effective cybersecurity strategies.

Organizations can recognize patterns and identify potential anomalies with a broad set of data at their disposal. This recognition capability isn't just about responding to immediate threats; it's also about comprehending and adapting the organization's security strategy over time to anticipate and preempt future attacks.

The advanced, dynamic detection logic built into the Taegis XDR platform empowers Secureworks customers to interdict hundreds of attacks every day — even as it minimizes their false positives and consolidates their low-level alerts into a smaller number of more critical and focused ones. And that translates directly into SecOps teams that keep their organizations safer as they keep improving operational efficiency.

NEXT STEPS

Request a demo to see how the Taegis XDR platform drives better detections to keep your environment secure.

Secureworks®

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that secures human progress with Secureworks® Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of thousands of organizations around the world who use its advanced, AI-driven capabilities to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

CORPORATE HEADQUARTERS

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

EUROPE & MIDDLE EAST

France
8 avenue du Stade de France
93218 Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111 00971
4 420 7000

ASIA PACIFIC

Australia
Building 3, 14 Aquatic Drive
Frenchs Forest, Sydney NSW
Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp

Availability varies by region.