ThreatConnect: Helping to Deliver on the Promise of XDR

In this first of two articles, ThreatConnect's Director of Security Architecture Chris Adams breaks down the primary requirements of an XDR as defined by Gartner and gives a bit of color as to why those are important and how ThreatConnect meets them, sometimes with integration partners.

On the surface, it's no surprise that Extended Detection & Response (XDR) has picked up steam as a promising solution combining products across multiple security disciplines. That's because security teams have realized that greater interoperability is paramount towards squeezing more value out of the assortment of products acquired over time.

However, like any shiny new object that garners everyone's attention, it's important to perform some due diligence to understand what the hype is all about before committing capital to it. That being said, let's take a look at how Gartner defines XDR:

> *"Extended detection and response describes a unified security incident detection and response platform that automatically collects and correlates data from multiple proprietary security components",* says Gartner in their innovative insight research report.[1]

It's most likely easier to say that sentence than it is to envision what's required to produce that capability for your security organization. That's because some products can perform bits and pieces of that description, but none of them do it all. Furthermore, many products have overlapping capabilities and it's difficult to determine which product should be leveraged to perform the job.

"Unified" is one of the more promising, yet elusive, terms in that definition. Like Einstein's unified field theory, which promised to unite each of the four natural forces, what's sought in XDR is a desire to unify security processes and technologies that have traditionally operated independently.

Primary Requirements

To start, let's take a look at the three primary requirements of an XDR according to Gartner

[1] https://www.gartner.com/en/documents/3982247/innovation-insight-for-extended-detection-and-response

1. *Centralization of normalized data, but primarily focusing on the XDR vendors' ecosystem only*
2. *Correlation of security data and alerts into incidents*
3. *A centralized incident response capability that can change the state of individual security products as part of incident response or security policy setting*

Centralization of normalized data

Normalization helps ensure that data elements map together effectively. Think about someone's name spelled differently in separate tables of a database that actually represent the same person. If searching for unique names, an application may conclude these are two different people. Normalization is the process of the system determining it's actually the same individual. Within the security domain and the advent of multiple data sources and formats, normalizing data is a big deal when trying to align apples-to-apples across disparate systems.

C*entralization* is a somewhat subjective term that implies data is managed within a single data store or available via a single access point. The reality is data can be managed in a federated sense and still achieve 'centralization'. This characteristic dictates that security data be consolidated from multiple sources to establish a single source of truth and that when changes are made updates are sent to dependent systems. I'd argue that the key point of this requirement is to identify critical, contextualized security data and manage it in a centralized manner with supporting processes to keep that data fresh and 'operational'.

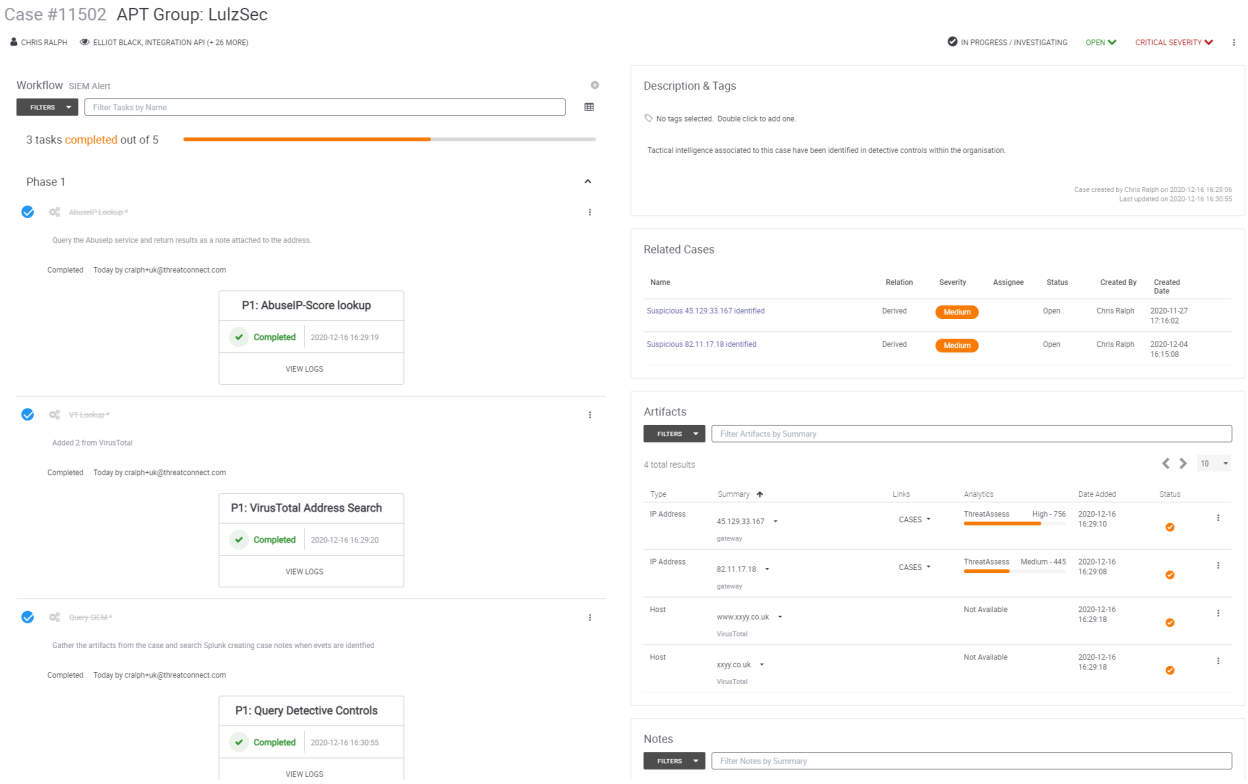
ThreatConnect performs both of these roles when ingesting threat intelligence data from sources and potential indicators of compromise (IOCs) from SIEMs, endpoints, or other internal sources. Data is normalized as it is ingested and our analytics and enrichment services provide context about that data, providing a centralized store or source of truth regarding the data that is most pertinent to the organization. For example, an event from a SIEM is captured by ThreatConnect based on a rule where the event contains a known Command and Control indicator (C2). That IP Address is persisted in ThreatConnect's Threat Intelligence Platform (TIP) with context about the indicator even after the data is purged from the SIEM (something that happens after a few months, typically).

Correlation of security data and alerts into incidents

Correlating security data and alerts into incidents drives home the desire for processes that bind these typically separate security functions. Why is that important? Because incident responders need to prioritize their focus and efforts and have all pertinent information in front of them on demand. Today, in most environments, it's a scramble to collect pieces of data from disparate systems and perform the correlation manually. Having it done for you using the advantage of orchestration, correlation can be done automatically giving time back to the incident response team.

Returning to our previous example, imagine that the C2 involved in the SIEM event is determined to be registered to a well known threat actor, information that is provided by threat intelligence collected by the platform. That's a pretty serious finding and someone would want to create a case and escalate it for further investigation where the case contains all related data and threat intelligence (indicator, threat actor, context, etc.) even linkage to other incidents where that indicator may have appeared previously.

What problem did we solve here? The correlation of threat intel, event data, incident data — data from systems that you typically don't find correlated in a single pane of glass. With ThreatConnect, one can pivot on the event data, the IOC, or the incident case and see those correlations as the graphic below depicts.



A centralized incident response capability that can change the state of individual security products as part of incident response

Changing state or security policy implies that we are modifying the controls that define our security posture. Just like late at night when you are home alone watching *The Shining* and you hear a bump in the other room (incident) which motivates you to get up and bolt lock the back door (control), we are prompted to modify our security posture in response to a clear and present danger (or one we imagine). Likewise, we want to be able to modify the security controls of our enterprises based upon incident data in a simple and straightforward manner.

In our example, if the IP Address that we identified as an active C2 of a known threat actor within our case raises our fear level to a degree that something must be done, we'd likely want to block access to that IP from our enterprise to prevent outbound/inbound connections to it. With ThreatConnect, orchestration provides the mechanics to push that indicator to a blocking device from within the case (incident) with a simple click, effectively modifying our security control. Playbooks provide a means to interact with any security controls your enterprise uses (given the control provides an API).

Collectively, each of these requirements prescribe a need for tight interoperability between common security technologies and processes that aren't commonly achieved with a single security vendor. ThreatConnect's threat intelligence platform, orchestration, and case management capabilities help customers meet these requirements by tightly integrating with other security sensors and controls to achieve the intent of what XDR promises.