How Cisco XDR's AI Empowers SOC Analysts to Work Faster and Smarter

Contents

Introduction

A plethora of security incidents happen every day in IT environments. A security analyst must process multiple such incidents every week, where each incident is comprised of several security events.

A Security Operations Center (SOC) analyst's bootstrapping process on a new incident is challenging because the analyst must understand and interpret the various events that make up an incident. When the analyst is done dealing with an incident, they must write up an incident report. The process of writing up the report is generally time-consuming and often much disliked by the typical analyst.

How can the analyst be made more productive in getting up to speed on a security incident and, when done, efficiently writing up an incident report? An effective Extended Detection and Response (XDR) solution can help the analyst with both tasks.

An effective XDR will have the ability to find the correct set of related events to organize into an incident. Further, the XDR should be able to summarize the events in an incident to create a "rapid insertion point" for the analyst. Finally, the XDR will be able to initiate incident reports on the analyst's behalf. Cisco® XDR is one such XDR solution. As we'll see in this document, Cisco XDR uses Artificial Intelligence (AI) in interesting ways to assist SOC analysts.

More on the problem

A 2022 survey of SOC analysts found that 64% of analysts spend over half their time on tedious manual work (see references [1], [2]). The same study also found that 66% of analysts believed that half of all their tasks could be automated. Finally, the survey discovered that for most analysts, “reporting” was the task that consumed the most time during a typical day. Interestingly, analysts found reporting to be the second least enjoyable task (after “triaging”).

Lacking an effective tool, one of the manual tasks that an analyst goes through is understanding the scope of a newly reported security incident. The individual events that make up the security incident are often not readily available. When the events are available, it takes manual work to sift through and understand each event and develop an overview of the incident.

Once the analyst is done dealing with an incident, they must write up the incident report as the “paper trail” for their management and as documentation for future analysts. Many analysts would prefer to avoid the report-filing process. An analyst must find the proper metrics and capture notes to build a high-quality report. Doing so takes time that the analyst doesn’t have because of the multiple incidents they have to chase down.

Many SOCs function in an ad-hoc manner. In such SOCs, there isn’t a standard process to preserve knowledge garnered during an incident. Without knowledge preservation, the task of follow-on analysis and the jobs of future analysts become even more challenging. The SOCs’ management is also hindered in their attempts to improve productivity and justify additional investments.

[1] Over 60% of SOC Analysts are Planning to Quit Next Year, Information Security Magazine, 4 March 2022.

[2] Voice of the SOC Analyst, tines, 2022.

More on the solution

Competent SOC analysts are a precious resource, and it only makes sense to reduce their manual work with automated tools such as an XDR.

An effective XDR should be able to triage security events, automatically correlate important events into incidents, and prioritize incidents by impact. Further, an effective XDR should be able to summarize the events in an incident so that analysts can quickly bootstrap themselves into a new incident. Finally, an effective XDR should be able to use the events tied to an incident, the previously generated incident summary, and the analyst's actions taken in response to an incident to automatically create an incident report (see Figure 1). Of course, the analyst should be able to edit this report and add color before submitting it.

With an XDR in place, an analyst can expect to save time while launching into a new incident and closing it. Further, a SOC's management can expect repeatable standard incident reporting processes to be instilled in the SOC's staff.

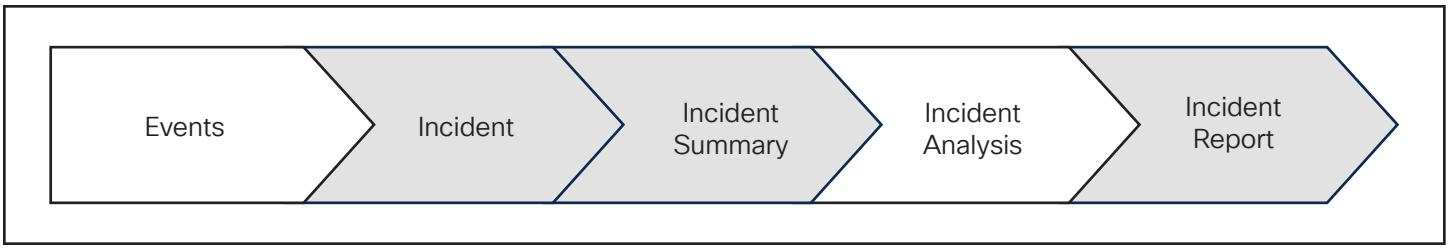


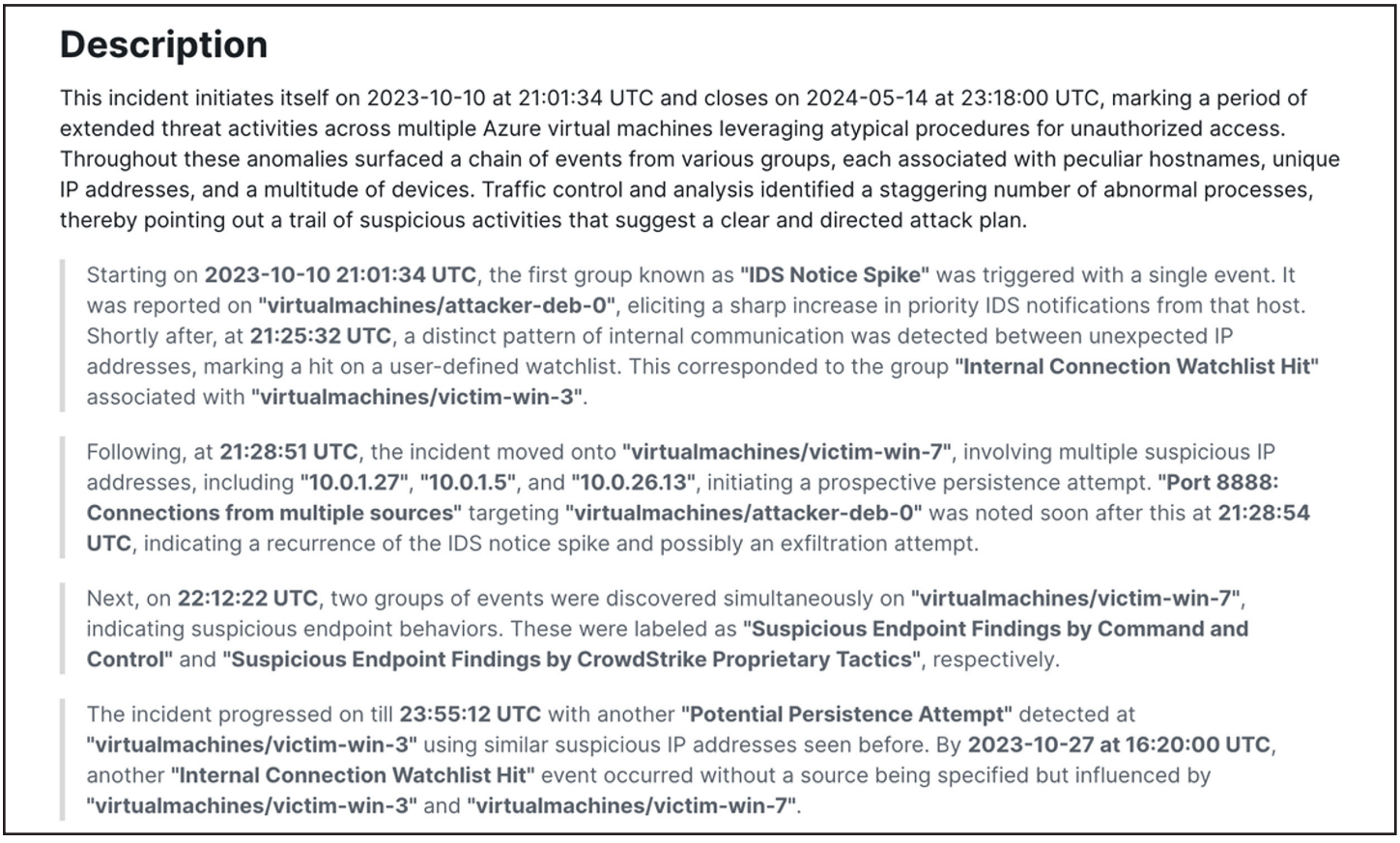
Figure 1. Security incident progression: the grey blocks correspond to the topics covered in this paper

Cisco XDR

Cisco XDR has all three of these essential capabilities to empower analysts (see references [3], [4]).

First, Cisco XDR can correlate related security events into security incidents (see Figure 1) and automatically prioritize the incidents with respect to impact to an organization. The events are supplied by Cisco's network, cloud, endpoint, and email security solutions and select third-party tools that integrate with Cisco XDR. Events are deemed related and belonging to the same security incident when they fit a threat scenario such as ransomware or a pattern of attacker tactics indicative of threat progression. Typically, related events share specific properties, such as source or destination Internet Protocol (IP) addresses.

Second, Cisco XDR has an AI-powered facility that enables it to summarize a security incident (see Figure 2). Cisco XDR takes the events in an incident and their associated data and passes them to a Large Language Model (LLM) to produce an appropriate incident title, description, and summary. The prompts sent to the LLM are tuned to elicit summaries that are useful to human analysts bootstrapping into new incidents. Multiple prompts with slightly different configurations are sent to the LLM, and the most appropriate responses are chosen for presentation to the analyst. During testing, LLM-generated titles, descriptions, and summaries were evaluated by experts and found to be useful to SOC analysts.



Description

This incident initiates itself on 2023-10-10 at 21:01:34 UTC and closes on 2024-05-14 at 23:18:00 UTC, marking a period of extended threat activities across multiple Azure virtual machines leveraging atypical procedures for unauthorized access. Throughout these anomalies surfaced a chain of events from various groups, each associated with peculiar hostnames, unique IP addresses, and a multitude of devices. Traffic control and analysis identified a staggering number of abnormal processes, thereby pointing out a trail of suspicious activities that suggest a clear and directed attack plan.

> Starting on **2023-10-10 21:01:34 UTC**, the first group known as **"IDS Notice Spike"** was triggered with a single event. It was reported on **"virtualmachines/attacker-deb-0"**, eliciting a sharp increase in priority IDS notifications from that host. Shortly after, at **21:25:32 UTC**, a distinct pattern of internal communication was detected between unexpected IP addresses, marking a hit on a user-defined watchlist. This corresponded to the group **"Internal Connection Watchlist Hit"** associated with **"virtualmachines/victim-win-3"**.

> Following, at **21:28:51 UTC**, the incident moved onto **"virtualmachines/victim-win-7"**, involving multiple suspicious IP addresses, including **"10.0.1.27"**, **"10.0.1.5"**, and **"10.0.26.13"**, initiating a prospective persistence attempt. **"Port 8888: Connections from multiple sources"** targeting **"virtualmachines/attacker-deb-0"** was noted soon after this at **21:28:54 UTC**, indicating a recurrence of the IDS notice spike and possibly an exfiltration attempt.

> Next, on **22:12:22 UTC**, two groups of events were discovered simultaneously on **"virtualmachines/victim-win-7"**, indicating suspicious endpoint behaviors. These were labeled as **"Suspicious Endpoint Findings by Command and Control"** and **"Suspicious Endpoint Findings by CrowdStrike Proprietary Tactics"**, respectively.

> The incident progressed on till **23:55:12 UTC** with another **"Potential Persistence Attempt"** detected at **"virtualmachines/victim-win-3"** using similar suspicious IP addresses seen before. By **2023-10-27 at 16:20:00 UTC**, another **"Internal Connection Watchlist Hit"** event occurred without a source being specified but influenced by **"virtualmachines/victim-win-3"** and **"virtualmachines/victim-win-7"**.

Figure 2. Example incident summary

[3] Cisco XDR, retrieved September 2024.

[4] Cisco AI Assistant in XDR Demonstration, retrieved September 2024.

Third, Cisco XDR has an AI-powered incident reporting facility that generates a draft incident report (see Figure 3). Similar to AI-powered incident summarization, all the events and associated data are passed to an LLM along with a custom prompt to produce the incident report. Also similar to incident summarization, extensive prompt fine-tuning and results evaluation have been carried out to ensure that the generated reports are helpful to human readers. The SOC analyst who investigates the incident in question can use the generated report as a template to create the final report. Most of the information needed is already in place. The analyst only needs to add information to the report that could not be captured by the security infrastructure. AI-generated reporting has the added benefit of encouraging standardization in reporting—as the AI-generated reports produce similar templates for different incidents, of course, with other data populated into the template.

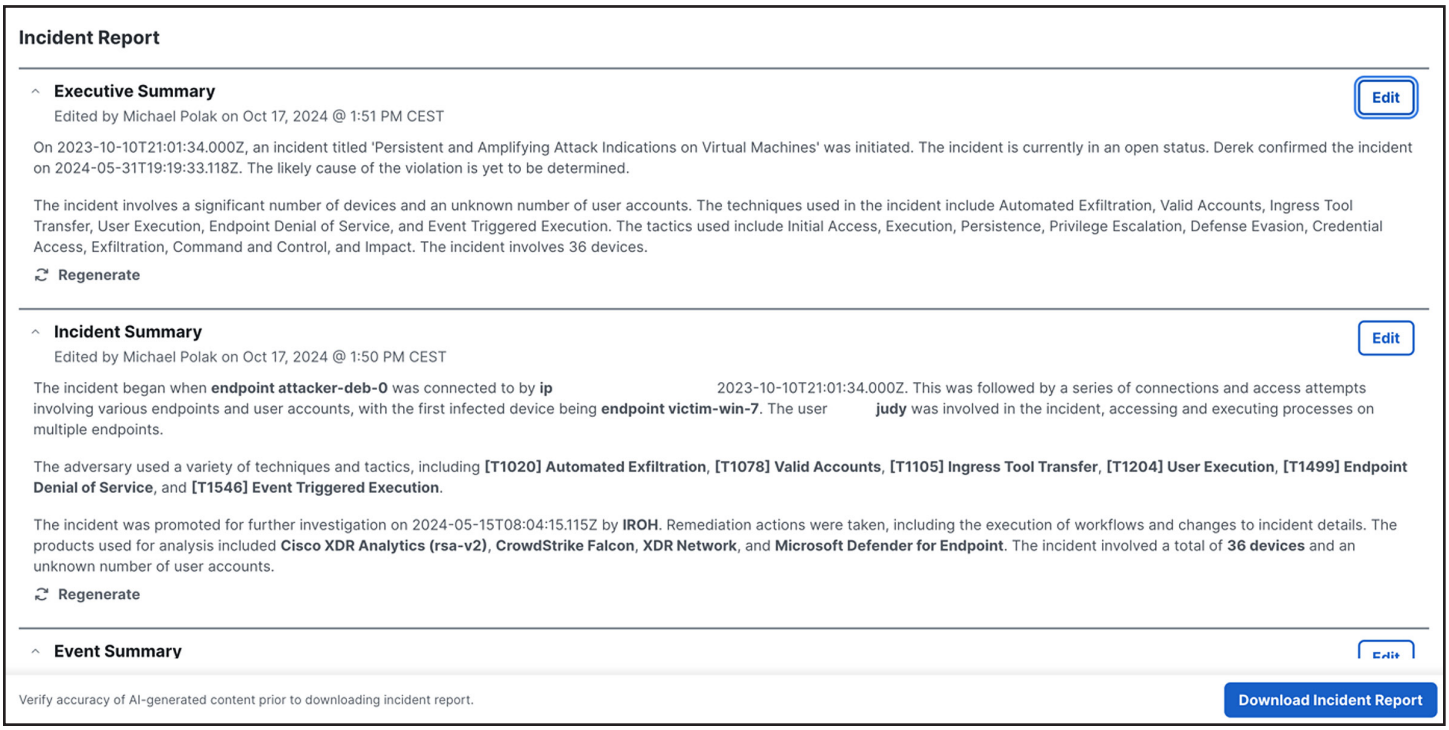


Figure 3. Example incident report

The capabilities in Cisco XDR discussed above save SOC analysts valuable time, help them work through incidents quickly, and standardize the incident reporting process. The time saved enables analysts to focus proactively on higher value tasks.

In closing

Cisco has been working on security technologies for over thirty years. In recent years, it has invested heavily in AI for Security. Cisco uses AI to assist security administrators, augment human ability to detect incoming threats, and automate mundane and repetitive security tasks.

Cisco XDR's incident summarization and reporting is an example of using AI techniques to automate security tasks. Here, AI enables SOC analysts to quickly bootstrap into new incident analysis and helps the analysts file incident reports when they are done handling the incident.

C11-4781565-00 11/24