Case Study

Incident Response Company Bugsec Uses Cynet To Accelerate And Optimize IR Operations

Company Background

BugSec is the largest cybersecurity consulting company in Israel, housing best-of-breed security practitioners that provide MDR, SOC-as-a-Service, Red Team, Blue Team and research services. BugSec is trusted by numerous organizations worldwide which acknowledge human expertise is the unreplaceable factor in forming adequate cyber resilience. Whether in the context of incident response, or in assessment of existing security levels, BugSec empowers its customers to stay one step ahead of the adversary and maintain a secure environment.

The Challenge

In the typical incident response flow, the customer doesn't have the ability to tell the IR team what the problem is. The common scenario is that the customer is either alerted by a third-party entity which is oriented on the attack's impact (for example, a bank notifying a retailer that cards used by its customers feature anomalous behavior), or suspects that something might be wrong due to a secondary indication. One way or the other, the initial step of the responder is to find the suspicious needle in the haystack, before the actual investigation can start.

"When the targeted environment comprises a large number of endpoints, the initial filtering can become a challenge," explained Meir Abergel, CEO of BugSec. "We all have a rich toolkit of opensource IR tools for various parts of the investigation, but they are not very useful at this stage. In order to achieve initial visibility, you must deploy across the entire environment. Open-source tools lack both the infrastructure and the support to reliably do this. We tried to use an EDR solution to do so, but deploying them takes too long – and this is an extremely time-sensitive stage."

Website:
https://bugsec.com/

Country:
Israel

Industry:
Cybersecurity

Meir Abergel,
CEO

"The Cynet 360 platform gave us lightspeed visibility into all files, processes, network traffic and user logins. It enabled us to interact with unknown environments in a rapid and efficient manner, immediately pinpointing suspicious entities. Once there, we could start the heavy-lifting investigation and make the best of our expertise."

The Solution

With an increasing number of incidents to respond to, the BugSec IR team knew that the ability to gain rapid visibility into its customers' environment was critical. They decided to test the Cynet 360 platform across a number of incidents that occurred in middle-sized and large environments.

A Natural Complement to Responder Open-source Tools

Open-source Tools "It's important to understand that Cynet 360 is an alternative to our IR team's open-source tools," explained Abergel. "In this sense, it is actually a natural complement. While Cynet 360 is the enterprise-grade power-tool that slices through the environment to rapidly disclose suspicious entities, the open-source tools are the set of surgical instruments the responder uses to analyze these entities. Together, they are a natural fit."

Up And Running in No-time

The key success criteria for the BugSec team was the ability to be up and running rapidly, with complete coverage of entities and activities. "We were amazed by Cynet 360's deployment ease and speed," said Abergel. "On one of the incidents, the environment I worked with comprised roughly 1700 endpoints and the customer didn't have any solid starting point except a vague notion that some network traffic didn't seem right. Within less than 2-hours, I could see everything – processes, network traffic, user accounts. With a few basic queries, I isolated three endpoints that stood out in their behavior and focused my efforts there."

Respond With Extra Speed And Efficiency

On top of this, the BugSec team discovered that Cynet 360 introduced speed and efficiency into other parts of the response process. Said Abergel, "Once you have an enterprise-grade tool deployed across all assets, a lot of options suddenly open up. For example, we could use Cynet to distribute our open source-tools across the environment. Since Cynet is shipped with automated threat detection capabilities, it resurfaced part of the live malicious activity for us – another important time saver."

Remediating Threats On-the-fly

"Another important aspect is the removal of active threats," added Abergel. "In the course of an investigation, you come across infected endpoints or compromised user accounts and other malicious artifacts which you need to contain before proceeding onwards. Cynet 360's broad remediation toolset is ideal for that purpose."

Platform Of Choice

Since their initial testing of the Cynet 360 platform, it has become BugSec's solution-of-choice for initiating detection and response processes in customer environments. Today, deploying Cynet 360 is the starting point for any investigation carried out by BugSec's IR team.

Results & Benefits

BugSec employs Cynet in all its IR operations, coupling its team's skill with Cynet 360 infrastructure to gain unmatched speed and quality:

- **Rapid Visibility In New Environments**
  Cynet 360 deploys across thousands of endpoints in hours, providing responders with immediate visibility into correlated files, processes, network traffic and user logins.

- **Pinpointing Suspicious Endpoints And Traffic**
  Cynet 360 deploys across thousands of endpoints in hours, providing responders with immediate visibility into correlated files, processes, network traffic and user logins.

- **Pinpointing Suspicious Endpoints And Traffic**
  The Cynet 360 dashboard enables responders to run initial searches across endpoint and network traffic to rapidly discover suspicious entities and filter them for deeper investigation.

- **Detection Of Active Threats**
  Cynet 360 automates the detection of common attack tools and framework (Meterpreter, Cobalt, etc.), as well as executed malware and communication with malicious sites.

- **Seamless Threat Removal**
  Cynet 360 is used as the primary tool throughout the investigation to isolate infected hosts, delete files, kill processes, block network traffic and disable user accounts.