Orange
Cyberdefense

Case study

Intelligence-led security in practice: safeguarding a French multinational in consumer products from the SolarWinds compromise.

88,000
employees working in major hubs in EU, AME, APAC, ME, Africa.

~3 million
IT assets are used within the networks of this global player.

37 billion
events are generated each month, making it a real challenge to focus on the signals in all the noise.

Moving to digital

The customer is a French-based global player with international locations and hubs in Europe, the Americas, Asia, the Pacific, Middle East and Africa.

A commonly found challenge throughout all sectors of business is the need for robust capabilities and security in regards to online presence and digital business in general. This need has been intensified through the COVID-19 pandemic. Along this transition some key challenges have to be mastered. An additional urgency was added through the SolarWinds incident and the potential compromise it could cause.

Challenges

As a global player the customer found itself confronted with about 3 million IT assets, generating 37 billion events per month. Orange Cyberdefense was called in to help cutting through the noise and focusing the limited resources to prioritize and respond to a potential compromise. A special focus was put on the potential exposure to SolarWinds Orion.

Narrowing down the focus

Orange Cyberdefense experts helped to identify 100,000 - from the before mentioned 3 million assets - which were potentially affected. Among these, 20,000 were found to be critically important for the business. With this increased focus it was possible to effectively make use of resources by prioritizing the most vulnerable and important assets.

Intelligent protection

Combining deep insight into the threat landscape and intimate knowledge of the customer environment and needs enabled Orange Cyberdefense to provide proactive protection and faster response. Using relevant, targeted and actionable intelligence practically boosted the effectiveness of security in all aspects.

Taking care of SolarWinds

Intelligence-led vulnerability management in action

1. Vulnerability Intelligence Watch alerted us about a new vulnerability on SolarWind Orion. It's only one out of 1,113 vulnerabilities published in the month it was reported. This organisation has a challenge in keeping track of this and as well the other thousand new ones reported that month.
2. The volume of information is overwhelming, and prioritisation is not a simple matter. With Threat & Vulnerability Management, we did a proactive scan on all customer's assets, only 15 assets have been found vulnerable.
3. Then there is the question of impact to their specific organisation and context – to give an idea, 6% of vulnerabilities are ever exploited on a wide scale. Most vulnerabiities therefore don't need to be patched immediately, but choosing the wrong ones can be catastrophic. In this, case, it needed to be addressed urgently.
4. The CyberSoc analysed attack vectors and written new rules to detect these new IoCs. Operational teams took over proactively to protect our customers: configuring, patching, tuning their security and threat hunting accross client estates and mitigate risks before a major breach.
5. We defined the remediation plan with the customer who patched 14 assets (the 15th has been removed).
6. With Threat & Vulnerability Management, we did a new scan on all customer's assets to ensure no more assets were at risk.

Day 1

Vulnerability discovered
The Vulnerability Intelligence team releases an advisory on a new vulnerability in SolarWind's Orion.

Scanning set up
We ran a proactive scan on all the customer's assets, only 15 were found vulnerable.

Day 3

Exploit discovered
The intelligence team advises an exploit is available and used "in the wild". The operations teams was notified.

Day 4

Detection rules deployed
Potential attack vectors where analyzed and new rules defined by the CyberSOCs for quick detection.

Day 5

Remediation defined
Targeted remediation advised, 14 assets patched (the 15th was removed). A new scan showed no more assets were at risk.

Risk mitigated, security restored

Resources focused where they have most impact

"Given the speed with which attackers are exploiting vulnerabilities, this window of exposure is significantly exacerbating problems like ransomware. Beyond timing, there is also the element of being able to focus resources where it matters: detecting the signals in the noise and targeting them with the right mitigation actions."

Charl van der Walt | Head of Security Research, Orange Cyberdefense