Use case
Cisco on Cisco

Effective threat investigations with Cisco Stealthwatch Cloud

Cisco Umbrella Security Operations Center (SOC) saves time with Stealthwatch Cloud

The Cisco Umbrella global network handles 200 billion internet requests per day, stemming from its 100 million global enterprise and consumer users. The Security Operations Center, or SOC, needed a tool that would give them visibility across their complicated network, and would allow for a simple quick investigation into any malicious behavior.

About the Umbrella SOC Team

Stealthwatch Cloud gives the SOC team the tools they need to conduct thorough early stage investigation on threats that may otherwise have gone unnoticed, or could be buried in the dense code that threats are able to hide in. For the SOC team, there were a few key challenges:

- Their team has to divide tasks, and picking through network traffic can be very time consuming.
- Cloud infrastructure accounts require a manual search to hunt for threats. This is an inconvenience for the team.
- There are many false positives that raise red flags for the SOC team which require just as much analysis as other real threats. The team needed a tool that could alert them on the most critical threats they actually needed to investigate.
- The team often receives threat notifications with no context. They are unable to view by host, and receive a long alphanumeric code that requires a deeper look to discover where the threat is originating.
- With numerous devices communicating with multiple cloud platforms, the SOC team often has trouble conducting forensic analysis with all of the telemetry flowing through their network.

The Solution

The Umbrella SOC team chose Cisco Stealthwatch Cloud for its ability to dive into threats early and to understand network behavior over time. The tool gives them a comprehensive threat dashboard with the ability to drill down into alerts to discover what sorts of threats are poking into their cloud infrastructure. They use Stealthwatch primarily to assess threats early on and for its simple approach to threat visualization. Here are some of the core benefits for the SOC team:

- **Faster threat detection:** The SOC team can identify threats early on, and receive customized alerts when malicious behavior is occurring. This is much easier than digging through individual cloud infrastructure accounts manually to hunt for this kind of behavior.
- **Intuitive dashboard view:** The Stealthwatch Cloud dashboard provides comprehensive visibility into the health of their network and gives the team a head-start on an otherwise time-consuming process. It can send out a ticket to the team so it can look into specific flagged instances, as well as identify similar cases.
- **Accelerated investigations:** Many cloud infrastructure platforms don't make it easy to identify regions or hosts. Stealthwatch Cloud's ability to pinpoint the region and specific account is key to the SOC team's success. Their cloud logs don't show the origin of threats, so Stealthwatch Cloud does the digging for them.
- **Forensic analysis:** The SOC team has the ability to dive into alerts in real time as they are picked up by Stealthwatch Cloud. High fidelity threat detections keep the team informed about any kind of malicious behavior. Stealthwatch Cloud also has the ability to store telemetry for long periods of time, supporting the teams' investigation workflow by replaying any activity that may have occurred in their environment hours, days or even weeks later.
- **Talos/Cognitive Intelligence integration:** Stealthwatch Cloud works seamlessly with Talos threat intelligence and the Cognitive analytics platform to allow users to easily spot blacklisted IP's and threats that might be hiding in encrypted traffic.

Conclusion

Utilizing Stealthwatch Cloud, the Umbrella SOC team gained unmatched network visibility through one simple dashboard, while holding on to the ability to dig as deep as they would like. The custom alerts let the team know as soon as something is wrong. Jumping on these threats early is a priority for the team, and Stealthwatch Cloud gives them the information they need to respond effectively.

Try it for free today!

To learn more about Stealthwatch Cloud and start a free, 60-day trial now, visit:
https://cisco.com/go/stealthwatch-cloud