SPYDERBAT

Spyderbat Scout

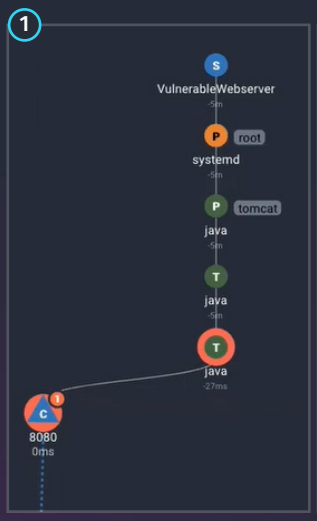
Instantly identify attacks based on chained suspicious behaviors

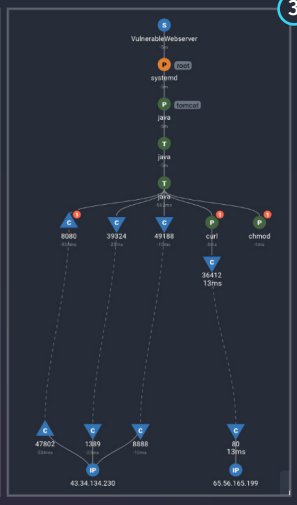
Overview

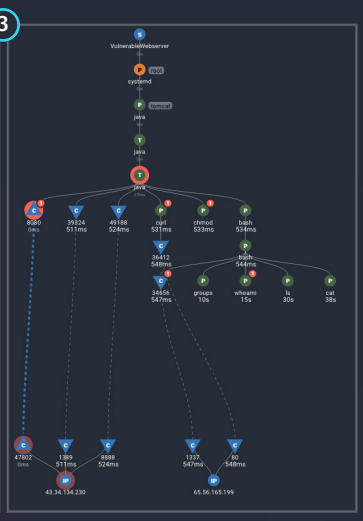
While we harden our cloud-native environments to prevent threats, the rate of change alone is enough to provide a foothold for attackers. While event logging, tracing, and correlation help to find concerning activities, they are plagued with overwhelming noise, false positives, and blind spots that mask issues and prolong investigations. Spyderbat Scout automatically chains together attack indicators for early and accurate recognition, enabling automated interception of malicious tactics, for instant action and complete threat nullification.

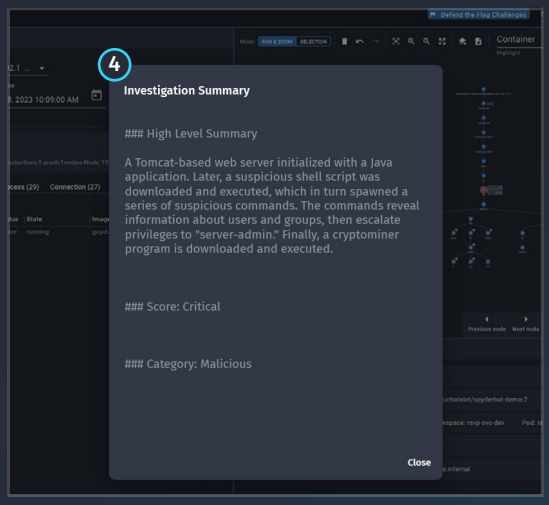
Challenge	Scout Benefits
Detect external attacks and inside threats	Precisely identifies early attack activity throughout your cloud native environments.
Reduce alert fatigue	Uniquely chains together multiple attack indicators to exponentially reduce false positives and overall alert volume.
Stop slow-and-low attacks, including supply chain compromises	Connects attack indicators even if separated by user sessions, workloads, or long periods of time (e.g. months).

Technical Details









<0 ms

2
Spyderscore: **Low**

<1 s

Spyderscore: **Medium**

After 24 Hours

Spyderscore: **High**

Resolution

Scout continuously assesses a risk score for every Spydertrace in your cloud native and containerized environments to recognize threats as they emerge, for immediate action and thorough mitigation.

1. Scout analyzes the Spyderbat Behavioral Web in real time, flagging activities and identifying attack techniques across MITRE's ATT&CK framework, such as discovery, command and control, defensive evasion, and execution.
2. Scout identifies and assesses a risk score to each individual Spydertrace in the Behavioral Web. A Spydertrace is any chained set of activities with at least one flag.
3. With any new activity, Scout reassesses the risk score based on the number of attack indicators, their severity and variance, as well as other factors such as scope and environment.
4. Scout automatically summarizes Spydertraces into a pre-built incident response report.
5. Scout triggers Spyderbat Interceptor to take automated action to stop, contain, or mitigate the intrusion.

Customer Case Study

The Situation: The platform team was inundated with alerts from cloud platform and cloud posture management tools, concealing real attack indicators due to the noise.

The Impact: A compromised third-party component detonated malware weeks after installation and was only discovered after the fact because it led to suspicious network activity.

The Resolution: Using Spyderbat Scout, the team reduced their alert volume from 12,000+ alerts to 25 high-score Spydertraces. Each trace includes a pre-made incident response report, describing the full chain of the attack progression over time. With the confidence they are catching all threats, even slow-moving attacks, the team enabled Interceptor to automate appropriate actions.