Signal Sciences

Security That Works Together: Signal Sciences and Cisco

Bring real time web application attack data into Cisco Threat Response

cisco Partner

Solution Partner

SUMMARY

Give your Security Ops team immediate visibility into attacks across all web application workloads with Signal Sciences and Cisco Threat Response.

WOULD YOU WANT TO KNOW IF:

- You were the target of a large-scale credential stuffing attack that put your customers at risk for account takeover and identity theft?
- You were the subject of an application DDoS botnet campaign sourced from hundreds of TOR nodes across the globe?
- You had a website that was vulnerable to a known exploit that might expose sensitive customer data to an attacker?

AND IF YOU KNEW, WOULD YOU WANT TO:

- **Analyze** and **correlate** event data using context from integrated Cisco security products and industry leading threat intelligence from Cisco Talos.
- Open a case to collect and store key **investigative** information, orchestrate resources for incident response, and manage and document your progress and findings.

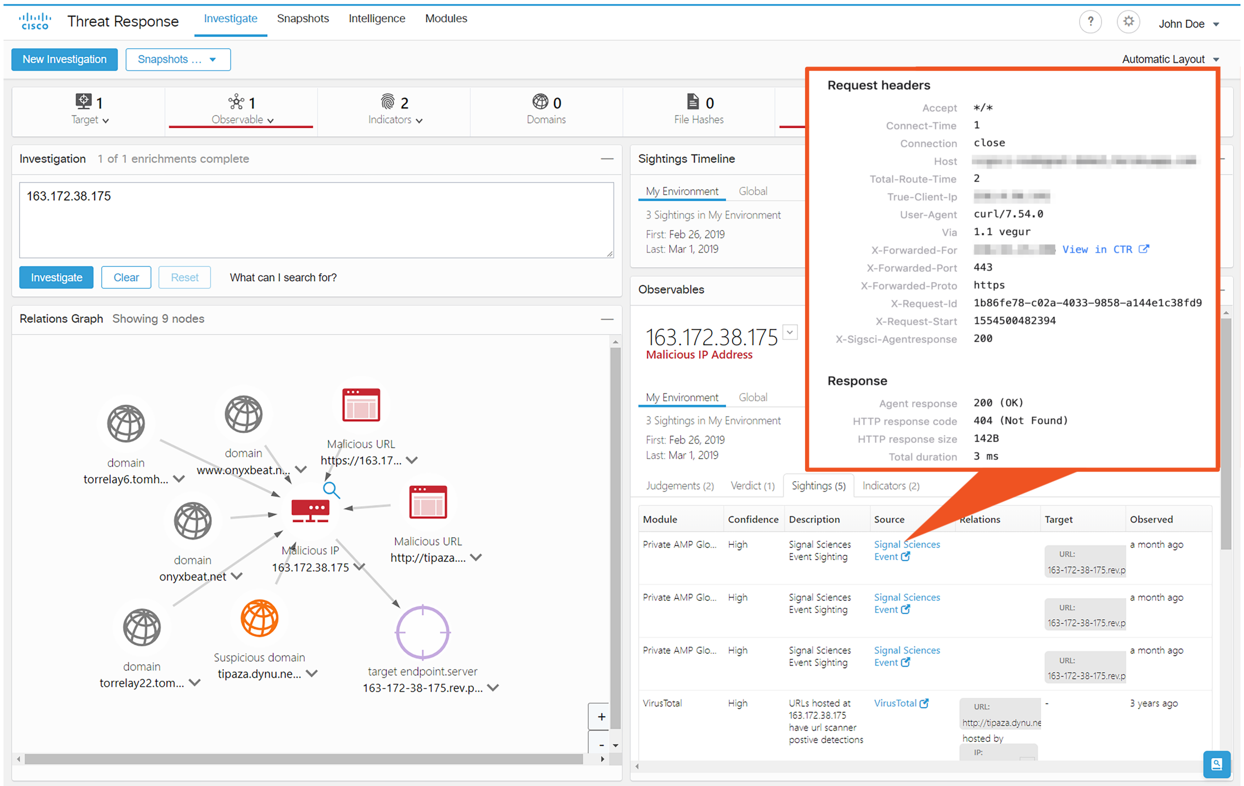
Solution Overview

With the rise of agile and DevOps development models, cloud and microservices infrastructure, and rapid build and deployment velocities, traditional development programs have changed drastically. Effective web application security requires innovation and integration. Signal Sciences integration with Cisco Threat Response enables security operations teams to quickly detect and respond to today's rapidly evolving threat landscape.

How It Works

Cisco Threat Response gathers, combines, and correlates threat intelligence available from the Cisco Talos Intelligence group, other Cisco products, and third parties to accelerate security operations functions around threat detection, investigation, and remediation. It brings together threat intelligence and local security context and control into one place for security analysts.

The integration of Cisco Threat Response and Signal Sciences brings real time web application attack data to help organizations quickly triage threats targeting applications.



163.172.38.175

Request headers

Accept	*/*
Connect-Time	1
Connection	close
Host	[redacted]
Total-Route-Time	2
True-Client-Ip	[redacted]
User-Agent	curl/7.54.0
Via	1.1 vegur
X-Forwarded-For	[redacted] View in CTR
X-Forwarded-Port	443
X-Forwarded-Proto	https
X-Request-Id	1b86fe78-c02a-4033-9858-a144e1c38fd9
X-Request-Start	1554500482394
X-Sigsci-Agentresponse	200

Response

Agent response	200 (OK)
HTTP response code	404 (Not Found)
HTTP response size	142B
Total duration	3 ms

Module	Confidence	Description	Source	Relations	Target	Observed
Private AMP Glo...	High	Signal Sciences Event Sighting	Signal Sciences Event		URL: 163-172-38-175.rev.p	a month ago
Private AMP Glo...	High	Signal Sciences Event Sighting	Signal Sciences Event		URL: 163-172-38-175.rev.p	a month ago
Private AMP Glo...	High	Signal Sciences Event Sighting	Signal Sciences Event		URL: 163-172-38-175.rev.p	a month ago
VirusTotal	High	URLs hosted at 163.172.38.175 have url scanner postive detections	VirusTotal	URL: http://tipaza.dynu.ne hosted by IP:	-	3 years ago

As attacks are detected and blocked, Signal Sciences next-gen web application firewall (WAF) sends relevant attack data to Cisco Threat Response including IP address, block reason, and additional metadata. Within Cisco Threat Response the incident is captured as an observable which can then be aggregated with all other sightings.

An incident responder can then open a casebook on the observable and initiate a cross-functional investigation. At the same time, a workflow can be triggered within Cisco Threat Response to take any corrective actions needed. If more details are needed, the investigator can jump straight to the event in Signal Sciences from Cisco Threat Response at the click of a button.

Conclusion

Businesses constantly innovate and find new ways to attract, engage, and transact with their customers through web and mobile applications. As a result, a dramatic shift has occurred in how applications are developed and deployed. Now more than ever, security teams need a solution that can protect modern application workloads and provide actionable insights to the professionals responsible for investigating and responding to threats. Cisco Threat Response combined with Signal Sciences next-gen WAF redefines expectations for addressing this challenge.