DATASHEET

STAMVS NETWORKS

Scirius Threat Radar

Scirius Threat Radar is the top tier of the Scirius Security Platform, building upon the foundation of Scirius Probe Management and Scirius Enriched Hunting.

With Scirius Threat Radar, security professionals are able to transition from the traditional approach of managing security events to a threat-based approach that delivers response-ready insights and identifies assets under attack mapped to phases in the cyber kill chain.

Scirius Threat Radar adds three important concepts to the Scirius Security Platform:

ADVANCED THREAT DETECTION

Inspects all network activity and threat alerts to cut through the noise and automatically identify the critical threats targeting your assets. This dramatically reduces the number of potential incidents that your team must investigate.

ASSET-ORIENTED ATTACK INSIGHTS

Shifts the focus from millions of indicators of compromise to a handful of compromised assets. Group those assets-under-attack by phases of the cyber kill chain to help analysts prioritize their investigations.

CUSTOM THREAT DEFINITIONS

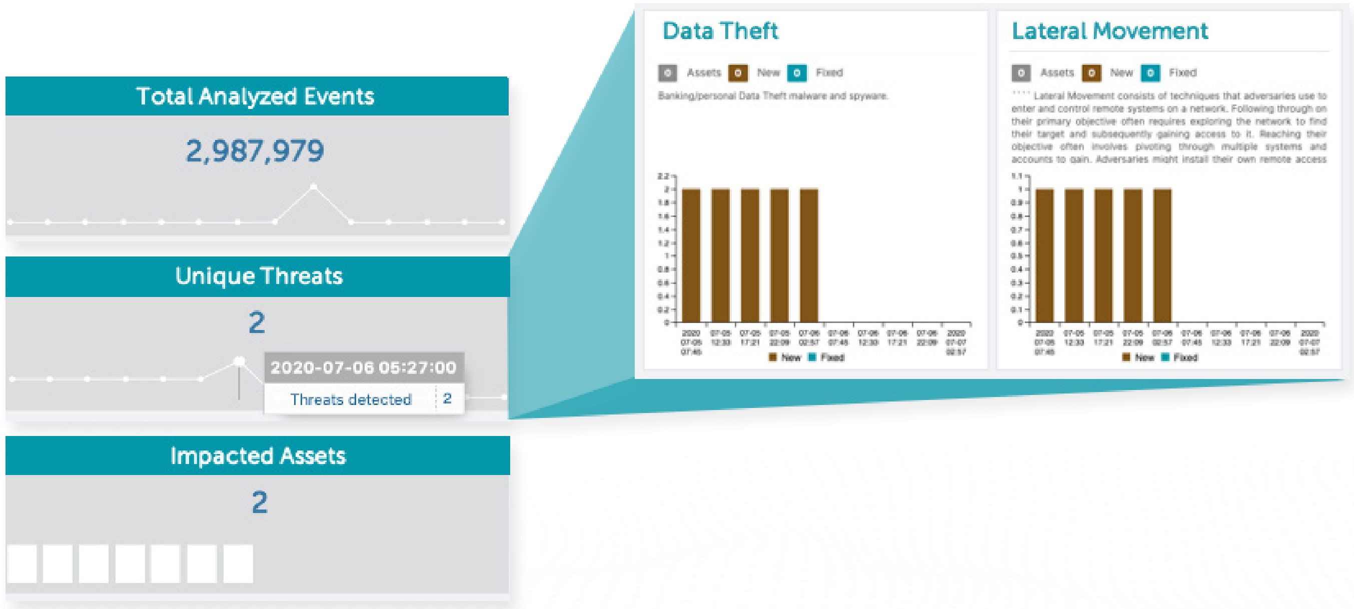
Empowers expert analysts to create organization-specific threat definitions and apply it to both historic and future network traffic. This improves detection, speeds response and strengthens the contribution of less-experienced analysts.

ADVANCED THREAT DETECTION

Scirius Security Platform deployments capture millions of threat alerts every day. This is simply too many events for any security team to monitor and manage.

With Scirius Threat Radar, users get high-level threat algorithms developed by the Stamus Networks threat research team and the opportunity to develop custom threat definitions. Scirius Threat Radar automatically applies these algorithms to all network activity and threat alerts to spot critical threat activity targeting your assets.

This new layer of threat detection saves users time and allows them to quickly identify the impacted assets, know when they were impacted, and take corrective actions.



Total Analyzed Events: 2,987,979

Unique Threats: 2

2020-07-06 05:27:00 — Threats detected: 2

Impacted Assets: 2

Data Theft

Banking/personal Data Theft malware and spyware.

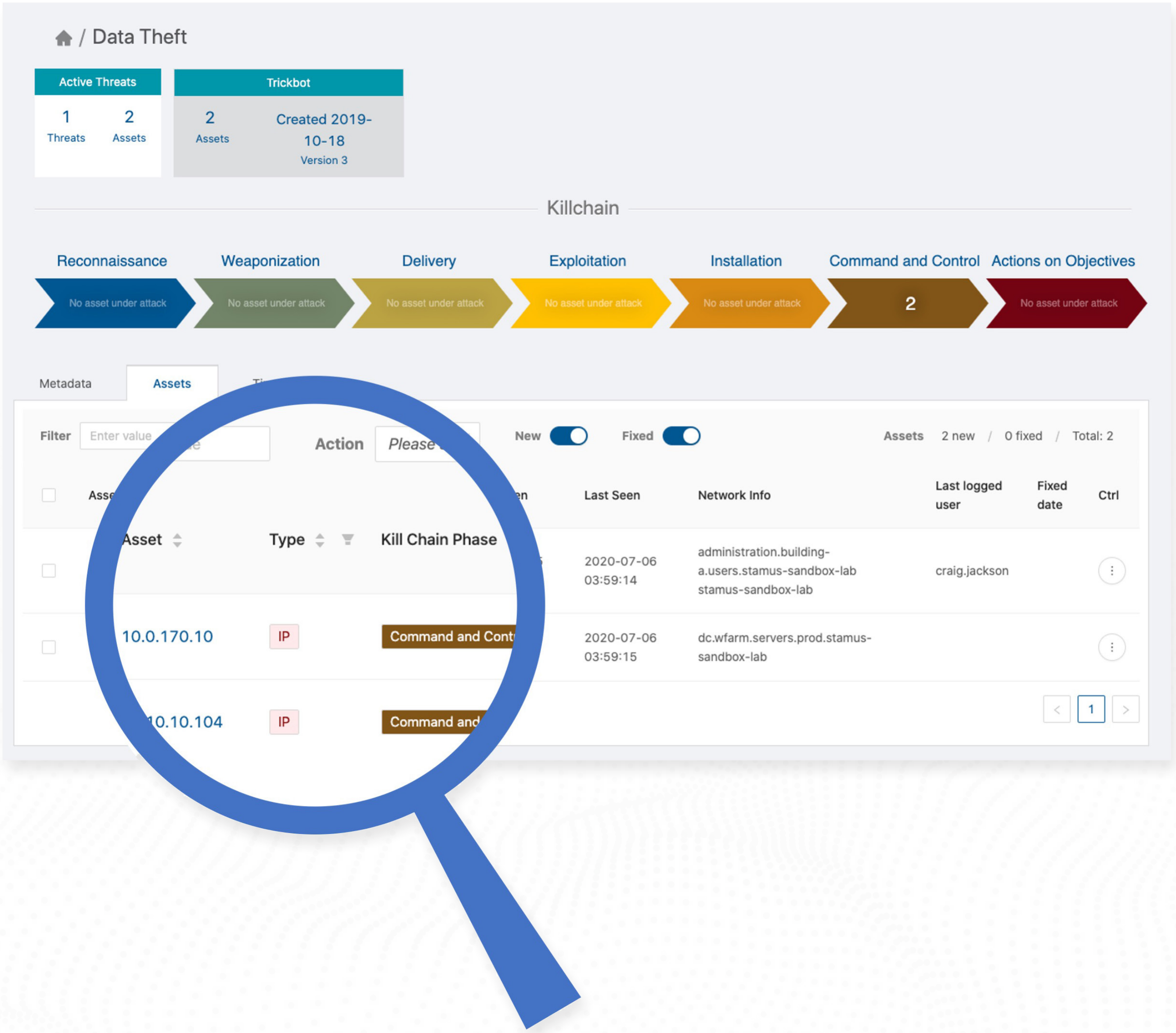
Lateral Movement

"""" Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain. Adversaries might install their own remote access

ASSET-ORIENTED ATTACK INSIGHTS

The advanced threat detection allow Scirius Threat Radar to identify all the hosts/assets that are impacted by each threat. Just as importantly, it associates each asset/host being attacked with the relevant phase of the cyber kill chain.

This mapping allows the analyst to prioritize their review of hosts that are, for example, under attack in the “command and control” phase before those which appear earlier in the kill chain such as the “delivery” phase. And by shifting the approach from one that is alert-centric to Scirius Threat Radar’s asset-centric approach, the analyst can more clearly understand the potential impact of the threat and accelerate incident response.



/ Data Theft

Active Threats	
1 Threats	2 Assets

Trickbot	
2 Assets	Created 2019-10-18 Version 3

Killchain

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control	Actions on Objectives
No asset under attack	No asset under attack	No asset under attack	No asset under attack	No asset under attack	2	No asset under attack

Assets 2 new / 0 fixed / Total: 2

□	Asse	en	Last Seen	Network Info	Last logged user	Fixed date	Ctrl
□			2020-07-06 03:59:14	administration.building-a.users.stamus-sandbox-lab stamus-sandbox-lab	craig.jackson		⋮
□			2020-07-06 03:59:15	dc.wfarm.servers.prod.stamus-sandbox-lab			⋮

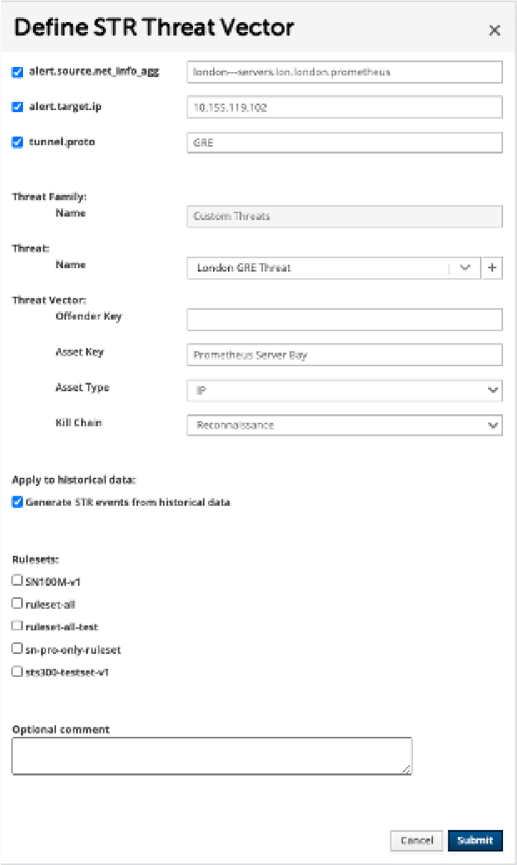
Asset	Type	Kill Chain Phase
10.0.170.10	IP	Command and Cont
0.10.104	IP	Command and

CUSTOM THREAT DETECTION

Even a modern well-researched threat detection can not cover the needs of every organization. Scirius Threat Radar includes a built-in mechanism for users to easily transform data filters they create while threat hunting into custom threat definitions for Scirius Threat Radar. These new threat definitions can be applied to both historic and future data.

By applying the custom threat definitions to historical data, the analyst will uncover assets under attack that should be investigated by the team. And when applied to future data, this threat definition allows the analysts to follow the threat activity over time.

This feature is another great way for Tier 3 analysts to empower Tier 1 analysts. Once a Tier 3 analyst has created these custom threat definitions in the Scirius Security Platform, the Tier 1 analyst is able to more quickly assess the organization's threat posture.



Define STR Threat Vector

☑ alert.source.net_info_agg: london---servers.lon.london.prometheus

☑ alert.target.ip: 10.155.119.102

☑ tunnel.proto: GRE

Threat Family:
Name: Custom Threats

Threat:
Name: London GRE Threat

Threat Vector:
Offender Key:
Asset Key: Prometheus Server Bay
Asset Type: IP
Kill Chain: Reconnaissance

Apply to historical data:
☑ Generate STR events from historical data

Rulesets:
□ SN100M-v1
□ ruleset-all
□ ruleset-all-test
□ sn-pro-only-ruleset
□ sts300-testset-v1

Optional comment

Solid foundation - It is critical to build the foundation of any network detection and response system on the best and most up-to-date threat intelligence. So, while you will always have the option to deploy additional rulesets and develop and deploy your own signatures, all users of Scirius Threat Radar also receive a fully automated subscription to the highly-respected Proofpoint ETPro ruleset.

With Scirius Security Platform, organizations can further reduce the complexity and cost of implementing a network detection and response process. Scirius Threat Radar helps security teams know more, respond sooner, and mitigate the risk to their organizations.

ABOUT STAMUS NETWORKS

Stamus Networks believes cybersecurity professionals should spend less time pouring through noisy alerts and more time mitigating risks by responding to real threats targeting their organization's critical assets. Founded by the creators of the widely-deployed open-source SELKS platform, Stamus Networks offers Scirius Security Platform that collects event data from enhanced Suricata detection (IDS), real-time network traffic analysis (NTA) and organizational context into an advanced analytics engine to create a powerful enriched threat hunting solution. With Scirius, you get unprecedented visibility and meaningful insights, giving you the tools to rapidly respond to incidents and mitigate your risk.

5 Avenue Ingres
75016, Paris
France

14807 Newport Dr
Westfield, IN 46074
United States

✉ contact@stamus-networks.com
www.Stamus-Networks.com