

LOOKINGGLASS

# scout **PRIME**®

## A GLOBAL ATTACK SURFACE MANAGEMENT PLATFORM

scoutPRIME is global attack surface management platform that provides an "outside-in" view of an organization's security vulnerabilities. With scoutPRIME, you can assess and manage, on a 24/7/365 basis, risk to your organization, subsidiaries, partners, suppliers, and other parties of interest. scoutPRIME empowers you to identify and manage risk associated with systems outside of your perimeter with visibility, context, and actionable intelligence.

The platform centralizes the collection and normalization of structured and unstructured data as well as other commercial data feeds you already ingest.

scoutPRIME's workflows allow analysts to configure notifications, schedule reports, and collaborate. Export threat intelligence in a variety of formats, via an API that allows for tailored data sets or through a third party system integration to orchestrate active defense via your security appliances.

### STAY AHEAD OF THREATS

scoutPRIME offers continuous visibility into 11 categories of risk and compromises to help your organization stay ahead of threats. Map the network assets of any entity of interest and continuously monitor each entity's IPs, domains, CIDRs, websites, and mail servers.

#### ENHANCE SECURITY OPERATIONS

scoutPRIME provides rich context and deep data analytics to enhance existing SOC operations. Integration with existing SIEM and big data solutions provides deeper insights and a broader view of the potential threats and risks associated with any single Internet asset or a collection of assets.

#### TAKE INFORMED ACTION

scoutPRIME empowers your team to take informed action with customizable, real-time alerting on observed risks and threats associated with assets of interest. Optimize your reporting and decision-making with unlimited, on-demand or scheduled reports to threats from any public-facing Internet element or collection of elements.

VISUALIZE ASSETS ON YOUR NETWORK FOR ACTIONABLE INSIGHTS TO PRIORITIZE AND MANAGE THREATS TO YOUR ORGANIZATION.

Workspace C	ollection Health	Collection	Management	Element D	etails Incid	ient Management Re	ports					
	ones (6)										Actions	
HREATS (1.6K)					NTS (5.6M)			COLLECTIONS (112)				
19~	· 145 ·		1.4K		.1K~	190.5K~	5.3M	38~	13	<b>13</b> ~ 61		
CRITICAL ELEWATED		NORMAL		CRITICAL		ELEVATED	NORMAL	ORITICAL	ELE	ELEVATED NORMAL		
ASSOCIATIONS ADDED TODAY		THREAT ASSOCIATIONS (25)						VEN	ALL (1.5M)	THREAT ASSOCIA	TIONS BY RISK CATEGOR	
		TIC	Threat	TIC	Bement	Collection(s)	First Seen	Last Seen		Spamming activity		
		33 Daily Sources		33 107.0.80.126		2 Collections ~	10/10/2019 19:58:44	01/22/2020 18:59:59		702.4K Malware hosting/distribution		
54.	.8K	33	Daily Sources	33	99 58 107 229	ATT	01/22/2020 18:59:59	01/22/2020 18:59:5	,	57 Malicious/scanning behavior 698.1K Vinus/bothet infection 98.2K		
NEW ASSOCIATION		33	Daily Sources	33	73 238 33 92	2 Collections ~	01/22/2020 18:59:59	01/22/2020 18:59:5				
		33	Daily Sources	78	115.133.53.171	TMAET AS AP TM	01/22/2020 18:59:58	01/22/2020 18:59:5				
	N COONT BY DAP	33	Daily Sources	70	202.60.105.134	to greater than 50	06/13/2019 19:21:23	01/22/2020 18:59:5	3	Questionable asset use 6.4K		
1.1		33 Daily Sources		50 65-43.37.189 76 50.237.172.82		ATT 2 Collections ~	09/01/2019 19:58:21	01/22/2020 18:59:51 01/22/2020 18:59:51		Command-and-control activity 728 Vulnerable service		
ינויא פריד בריא פריא ה		33 Daily Sources					11/25/2019 9.41:23					
	ours and ours	33	Daily Sources	56	117.193.69.175	BSNL MB Nation	01/22/2020 18:59:50	01/22/2020 18:59:50		511.4K Phishing activity		
ASSOCIATION CO		33	Daily Sources	33	73 243 168 138	2 Collections ~	01/11/2020 11:33:41	01/22/2020 18:59:4	9	37 Suspicious domain registrations 27		
	OUNT CHANGE	33	Daily Sources	82	12.248.54.118	лт	01/10/2020 17:34:40	01/22/2020 18:59:4	5			
-129.5K		33	Daily Sources	54	122.111.121.42	Micropies Networ	01/22/2020 18:59:45	01/22/2020 18:59:4	5			
O DOWN 7% P		33	Daily Sources	70	78.157.75.29	2 Collections ~	08/29/2019 13:49:51	01/22/2020 18:59-4				

SEE NETWORK ELEMENTS, THREATS, AND COLLECTIONS, WHICH ARE BEING CONTINUOUSLY MONITORED, AT A GLANCE.



FEATURES	BENEFITS
Customizable Footprinting	• Monitor only the parts of organization or the systems that matter so you receive the information that is relevant to your organization
TIC Scoring	• Proprietary to LookingGlass, TIC Scoring allows analysts to rank threats based on factors such as an organization's environment, threat landscape, and security posture, reducing alert noise and fatigue
Investigation Tools	• Analysts can access tools like Shodan, pDNS, WhoIS and Reverse WhoIs, and geolocation information within the platform, assisting in their day-to-day tasks
Aggregated Threat Data	• Access to dozens of included threat intelligence sources from a wide variety of providers, including LookingGlass proprietary indicators and feeds
Real-Time Alerting	• Receive instant alerts whenever an asset, system, or company you care about has a new threat or risk observed, or when the risk rises above your chosen threshold
Relationship Monitoring	• Organize assets and companies into groups and sub-groups to understand risks in different areas of your business as they relate to one another, and see the aggregated risk of vendors, business units, or peers in your industry
STIX and TAXII 2.0 Support	• Rapidly discover new and emerging cyber threats with industry threat intel sharing
Extensible API	Easily integrate with other security analytics tools
Unlimited Reports	• Produce unlimited management reports, scorecards, and other reports on any frequency with both manual and automated scheduling to any distribution or destination

# ABOUT LOOKINGGLASS

LookingGlass is a leader in intelligence-driven risk mitigation, including global attack surface monitoring, threat modeling, and network defense. Our full-service portfolio integrates threat intelligence, analysis, and a robust set of tools to operationalize threat mitigation in the network. With standard and custom solutions, LookingGlass makes cyber security smart and seamless for governments and enterprises.

Learn more at <a href="https://www.LookingGlassCyber.com">https://www.LookingGlassCyber.com</a>