New Generation Threat Perception System

SkyEye

Product Overview

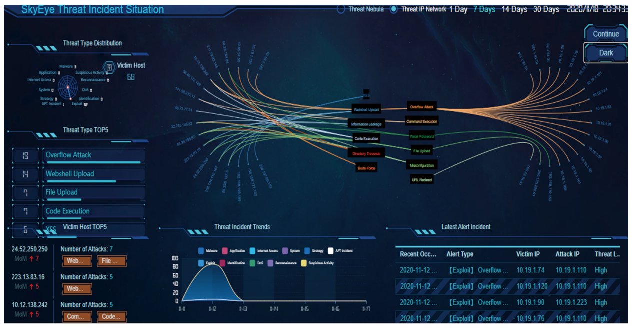
SkyEye is to establish a security analysis platform centered on protecting against APT attacks. With advanced threat detection and data analysis as its core, it provides security operation system for online assets protection, safe operation and maintenance, cyber threat detection, vulnerability discovering, analysis and traceability, response disposal, situation awareness and presentation.

System Components

Components	Description
Traffic Sensor	Retrieve and detect threats from original network traffic. Restore files from network traffic. Generate and output network logs.
File Threat Evaluator (Sandbox)	Execute static and dynamic detection for the files transferred from traffic sensor.
Analysis Platform	Analyze network logs and offer: threat summarizing, behavior analysis, threat hunting, assets management etc.
Email Threat Evaluator	Focusing on malicious mails detection including attachment examination, phishing mail detection.
The Honey Pot	The trap for attacks. Intentionally attracts access from attackers to collect attacker info for attack tracing.

Core Values

- Accurate Advanced Threat Detection
- Rapid Response on Major Security Incidents
- Retrospect and Analysis of Cyber Attacks



Recent Occ...	Alert Type	Victim IP	Attack IP	Threat L...
2020-11-12 ...	[Exploit] Overflow ...	10.19.1.74	10.19.1.110	High
2020-11-12 ...	[Exploit] Overflow ...	10.19.1.120	10.19.1.110	High
2020-11-12 ...	[Exploit] Overflow ...	10.19.1.90	10.19.1.223	High
2020-11-12 ...	[Exploit] Overflow ...	10.19.1.76	10.19.1.110	High

Advantages

Leading APT Detection and Tracking Ability

More than 40 domestic and global APT organization have been detected by Our Threat Intelligence Center.

Leading Threat Intelligence

Offering Threat Intelligence with extremely high accuracy by using multi-dimensional global data collection and cloud-based big data automated processing with auditing from top security research teams.

Cross-Device Synergy

Rapidly locating infected hosts and malware, SkyEye eliminates threats by co-working with terminal EDR, firewall NDR, and SOAR technology.

Massive Data Retrieval and Computing

Offering efficient retrieval ability for terabyte-level of data with solid technical support for local large-scale data retention, attack evidence retention, and real-time correlation analysis.

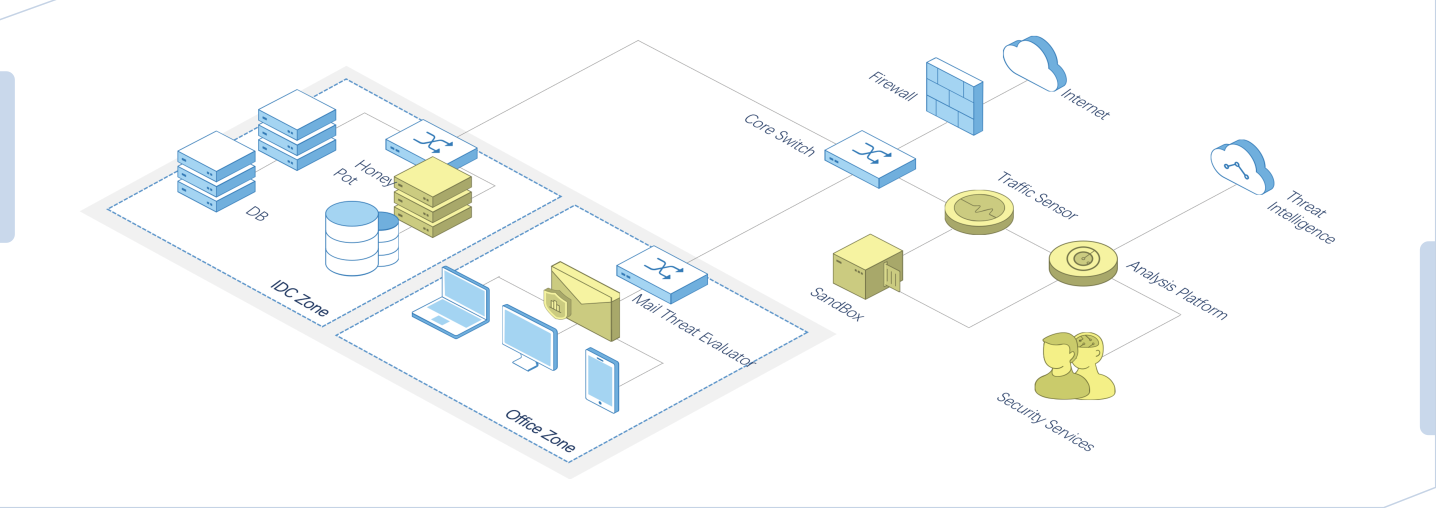
Machine Learning Algorithm

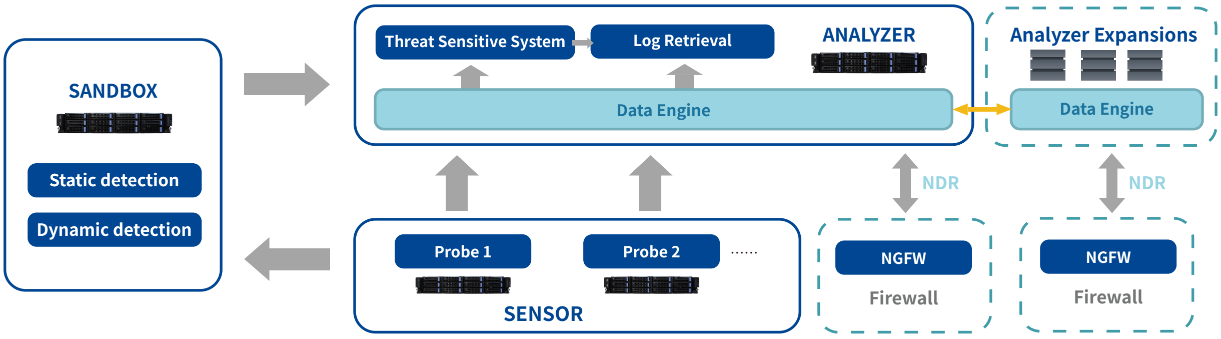
Enabling machine learning on detection of specific types of threats. Trained with massive data, machine learning algorithms provides highly efficient and accurate detection for the threats that can easily escape from rule checking.

Rich Industry Cases

1000+ customer cases in over every industry.

Typical Deployment





- DI IS resolution
- TCP/UDP traffic
- Network and Web access
- File transfer
- LDAP behavior
- Login action
- Email behavior
- DB operation
- SSL encrpytion

- Threat Logs

- USB logs
- Email logs
- IM file transfer
- Proceedings
- Passive DNS

Hardware Specifications

Product	Sensor		Sandbox	Analysis
Model	TSS10000-S53	TSS10000-S56	TSS10000-D57	TSS10000-A58/A58E
Memory	32G	64G	128G	256G
Storage	4TB	4TB	4TB	4TB*12
Interface Modules	2MGT+2*10/100/1000 M Base-T+2*10G SFP	2MGT+2*10/100/1000 M Base-T+2*10G SFP	4*10/100/1000M Base	4*10/100/1000M Base
Performance	4Gbps	8Gbps	Motion detection: 2w files per day Static detection: 100w files per hour	1G of traffic can be kept for 3 months A58E for Extension only

Note: the above contents are for reference only, subject to the actual product