SAFELY ENABLING BUSINESS

SecureDetect Network

Security Research
Characterize fundamental attacker behaviors

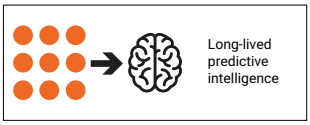
Data Science Security Research
ML models to accurately detect behaviors

Attacker Behavior Models
High-fidelity, signatureless detection

Command and control	Reconnaissance	Lateral movement	Exfiltration
Advance C2: human control	Network sweeps and scans	Stolen accounts	Data movement
Botnet C2	Advanced: AD, RPC, shares	Exploits	Methods, e.g. tunnels
		Backdoors	

Many customers base their threat detection only on logs or on endpoint data. The challenge with this approach is that not everything is logged, and not all endpoints will run detection agents. For optimal threat detection ability, customers also need to invest in network-based threat detection.

Traditional network-based detections are however failing to detect today´s threats. This is due to the fact that they are based on short-lived and reactive intelligence and that they fail to learn unique customer traffic patterns to be able to detect anomalies.

Traditional signatures	Data science
	
How the threats look	What the threats doe
Find threats that you´ve seen before	Find what all threats have in common
Snapshot in time	Learning over time
No local context	Local leadning and context

Solution

To address these challenges, SecureLink offers a Managed Service that leverages Machine Learning for detecting threats based on network traffic.

By applying supervised Machine Learning techniques, the service can detect threats that have never been seen before.

By applying unsupervised Machine Learning, and learning local behavior over time, the service can also detect threats based on behavior anomalies within the customer´s unique environment.

Service Overview

SecureLink will deploy physical or virtual sensors that are connected to a network tap. The network tap will send copies of all traffic that should be monitored to the sensor. The different sensors will extract relevant information and forward this data to the central brain that will apply different types of detection engines to detect threats across all the data. The brain is a hardware appliance that will be placed at the customer premise.

SecureLink monitors the central brain for alerts, and when detected, they will be collected, analyzed and classified by the security experts in the Cyber Defense Center 24x7.

Once a threat has been confirmed, customer will get an incident notification in accordance with the SLA for that specific priority level. This notification includes information about the threat and recommended actions.

Optional Services

The SecureDetect Network service can be complemented with the SecureRespond Quarantine service. The benefit with this is that this will give the Cyber Defense Center analysts the ability to isolate the detected threat, to limit the impact of the breach.