ANOMALI®

Making Sense out of Chaos

Automating Intelligence-Driven Security at Scale

ANOMALI APAC

(주)한국밸런스

Over 90% enterprise have Firewall, NW IPS, Anti-virus

External Threat Actors Account for 70% of Data Breach*

Median threat dwell time is 94 days before being detected**

“What went wrong?”

* 2020 Data Breach Investigations Report (DBIR)port (DBIR)
* *FireEye Mandiant 2020 M-Trend

Ever Widening Security Gap

- External: more sophisticated and persistent attacks organized by Cyber-criminals
- Internal: lack of Knowledge and Tools to sight external threats in a timely manner

Threat Actor

- Sophisticated TTP
- Manifold C&C nodes
- Cooperated campaigns

Security Control

- Short period, event centered
- Multiple products & formats
- Performance bottleneck

Security Process

- Manual process
- Overwhelming logs volume
- Time & resource pressing

Anomali: Make Sense out of Chaos

150+ Opensource Intel
Internal Threat Database
Premium Private Intel, ISAC
STIX/TAXII/PDF/XML...etc.

Anomali Threat Intelligence Platform

Collect | Manage | Integrate

ANOMALI | LENS

THREATSTREAM

ANOMALI | MATCH

Real-time
Analyze & Sight

SIEM

Firewall

EDR

NW IPS

Millions of Event Logs
IOC database

Ahead of Threats

Intelligence Driven Security powered by TIP

SOC

Data Breach Protection

- Automatically prioritize and deploy latest threat Indicators (IOC)
- IP address, Domain, File MD5, APT profiling… etc.

CSIRT

Incident Response

- Sight and Spot any compromised symptoms in real-time
- Visualized attack TTP and Progression for prompt resolution

SECOPS

Automate end-to-end Security Process

- Data collection, conversion, analysis and response – all in a single pane of glass
- Maximize existing security investment with Threat Intel Empowerment

Anomali Threat Intelligence Platform (TIP)

80%

Reduction in False Positives

47%

Decrease in Resolution Time

Threat Actor

Identify emerging threats & security breach at the earliest

Security Controls

Automatically deploy priority indicators & intelligence at all control points

Security Process

Reduced times and silos improve IR & operation efficiency


ANOMALI®
THREAT INTELLIGENCE PLATFORM
Thank you
Contact :
㈜한국밸런스
김 형덕 영업대표
Mobile : 010-7138-8889
Email : hdkim@valence.co.kr