Mandiant

SECURITY VALIDATION FILTERS AND DIMENSIONS

Filters

Content Source

- System Default
- User Created
- Outside Import
- Threat Intel

Action Types

- Network
- Endpoint
- Email
- DNS
- Protected
- Captive IOC
- Cloud (This type is only available for Cloud Validation Module)

Controls

- ATP
- DLP
- DNS-FW
- Email
- Endpoint
- IDS/IPS
- NGFW
- Proxy
- WAF

Last Run Status

- Never Ran
- Completed
- Errored
- Cancelled

Dimensions

Attack Vector

- General
- Application
    - General
    - Desktop
    - Web
- Browser
    - General
    - Chrome
    - Firefox
    - IE
    - Safari

- DB
  - General
  - DB2
  - MS-SQL
  - MySQL
  - Oracle
  - PostgreSQL
- Directory Services
  - General
  - Active Directory
  - Kerberos
  - LDAP
- Email
- IaaS (Infrastructure as a Service)
  - Cloud API
  - Cloud Storage
  - Cloud Workload
  - IAM
- OS
- Protocols
  - General
  - DNS
  - HTTP(S)
  - ICMP
  - SMB
  - SNMP
- Remote Access
  - RDP
  - SSH
  - VPN
- Web Framework
- Web Server
  - General
  - Apache
  - IIS
  - Nginx

Attacker Location

- General
- External
- Internal

Behavior Type

- General
- Authentication & Authorization

    - General
    - Brute Force
    - Impersonation
    - Privilege Escalation

- Command & Control Comm
    - General
    - Beaconing
    - Control

- Data Exfiltration
    - General
    - Download-Exfil
    - Upload-Exfil

- DoS
- Malicious DNS Query
- Malicious File Transfer
    - General
    - Download-MFT
    - Upload-MFT

- Malware Execution
- Man-in-the-Middle
- Phishing
- Policy Evasion
    - General
    - Peer-to-peer
    - Protocol Abuse
    - Restricted sites/media streaming

- Remote Access
    - General
    - Reverse Shell
    - Web Shell

- Scanning & Enumeration
    - General
    - Fingerprinting
    - Ping Sweeps
    - Policy Discovery
    - Port Scans
    - Vulnerability Scanners
    - Web Crawlers

- Web Attack
    - General
    - Command Injection
    - CSRF
    - SQL Injection

    - XSS

Covert

- No
- Yes

OS/Platform

- General
- Cloud
    - AWS
    - Azure
    - Google Cloud
- Linux
- Mac
- Windows

Stage of Attack

- Reconnaissance
- Delivery
- Exploitation
- Execution
- Command & Control
- Action on Target