ONYXCUBE
SECURITY ANALYTICS

"Think like a HACKER"

## SECURITY ANALYTICS

OnyxCube is a service offering which provides insight into the assets available on a network by collating data from multiple disparate, and sometimes unique or unusual data sources available in the environment. By "thinking like a hacker" we collect information that identifies flaws and behaviours inherent to your environment that require remediation.

## ABOUT ONYXCUBE

Coming out of "shadow state" in early 2019, OnyxCube was launched to identify flaws and behaviours inherent to an environment that required remediation. OnyxCube has since seen active development to become a reliable "source of truth" in terms of system, network and environmental security analysis.

## KEY BENEFITS

- Landscape visibility
- Accurate view of assets in your environment
- Persistent liveness detection
- Insight into cyber risks
- More cost effective than a dedicated resource
- Remediation advisory
- Reveals areas of high exposure
- Leverages existing infrastructure logs
- New data ingestions included

# GAIN VISIBILITY

**ONYXCUBE OFFERS PRE-DEFINED PANELS FOR VISIBILITY**

"Out of box" visibility into your environment

Fastest path to domain admin

Vulnerability overlay against identified assets

Privileged access risk analysis

Patch management gap analysis

RMM / AV gap analysis

Software version collation

Liveness detection

Network change analysis

Available & configured data sources define the visibility available within ONYXCUBE

## LIVENESS DETECTION

We collect information relating to the basic noise generated on a client network from devices & services such as routers, switches, firewalls, DNS, DHCP or NTP

## VULNERABILITY ENGINE

Vulnerability information is gathered from the environment on a predefined schedule to enable visibility into risks, and enable remediation activities to be identified and implemented

## DASHBOARD, ALERT, REPORT

Using multiple data types for their unique purposes and capabilities, data is merged via a customized front end. Using the dashboarding framework, relevant displays are generated. Scheduled reports & alerts are generated using the same framework

## REMEDIATION ADVISORY

Included in each engagement is advisory on rapid remediation actions

## GRAPH DATABASE

Using Graph Theory concepts, relationships are identified that allow our technology to identify potential paths of attack into an organization

## DATA WAREHOUSE

Our Data Warehouse includes customized views to convert specific data sources into a common and standardized repository of information

# WHAT'S INCLUDED

- Delivered as a managed service offering
- Annual licensing for products (matched to the chosen contract term*):
  - Dashboarding Tool
  - Vulnerability Assessment
  - SQL server standard license
- Software installation, configuration and maintenance for contract duration
- Billed monthly, annual commit

*OS & associated infrastructure management (AV/RMM/etc) licensing remains the responsibility of the client

# TYPICAL DATA INGESTED

- AV Management tool integrations
- VMWare inventory
- Active Directory logs & events
- Available endpoint information from RMM
- Network Infrastructure syslogs
- We are constantly expanding inputs

Available & configured data sources define the visibility available within ONYXCUBE

## ESCALATION & ALERTING

| ESCALATION OPTIONS | COST |
|---|---|
| EMAIL | Free |
| SNMP TRAP | Free |
| SYSLOG | Free |
| SERVICE DESK SOLUTIONS (API) | Implementation |
| SMS/XT & per SMS | Implementation |
| CUSTOM | Implementation & maintenance |

# DELIVERABLES

#1

## CLIENT TAKE ON

Onboarding documentation including sections related to:

- Due diligence information and validation of proposed deliverables
- Finalize RASCI Matrix
- Support Escalation Matrix and Procedure

365

## ANNUAL

- As-built documentation
- Configuration documentation is updated annually
- Delivered within first six months of the engagement

1/4

## QUARTERLY

Overview report, including sections related to:

- Executive Overview - Recommendations & Advisories
- Operational Overview
- Open Cases
- Licensing status of all associated products used to deliver OnyxCube

24hr

## DAILY

- Assistance with troubleshooting exercises in terms of any OnyxCube implementation/ operational issues
- Alerting to any immediate concerns in terms of the OnyxCube deployment

# NOTES

011 030 8100
info@onyxcube.co.za
www.onyxcube.co.za

6 Eaton Avenue
Bryanston 2191