IMPLEMENTATION & DELIVERY

Recommended steps for a successful project

IMPLEMENTATION & DELIVERY

- The purpose of this module is to provide guidance to Skurio partners on successfully delivering implementations of the Skurio Digital Risk Protection platform.
- Upon completion, you will:
  - Have an appreciation of the various implementation stages
  - Be able to make an implementation plan with outcomes at each stage
  - Get a customer online with basic DRP alerts from day zero
  - Understand Authorised Domains
  - Appreciate the implications of the Skurio Terms of Use

SKURIO IMPLEMENTATION FLOW/OVERVIEW

- Roles & responsibilities

- Before the first delivery meeting
  - Requirements gathering - Typical DRP usage and/or specific Intelligence Requirements
  - Subscription administration - BA Admin App, company creation, issuing invitations
- Kick-off call
- Early follow up
- Account review
- Quarterly reviews

TERMS OF USE, DATA PROTECTION & INFO SEC CONSIDERATIONS

- Skurio Terms of Use - https://skurio.com/tou/
  - Call out main points for emphasis
- GDPR
  - Authorised domains
  - Permission to monitor for data of individuals
    - Internal vs. external
    - Personal vs. business data
- Infosec
  - Platform security information

CONNECTIONS TO EXISTING SYSTEMS AND DATA

- None necessary
- Integrations optional, useful for automatic processing of results; i.e. email addresses checked against Active Directory
- Data can be entered directly into Skurio platform
- Good value can be achieved with public data, however specifics such as database fields can be very effective

BASIC SKURIO DRP ALERTS

- Email domain(s)
- Domains, including subdomains
- Typosquatting for main brands, products, services
- IPv4 addresses
- Keyword alert for company name(s), combined with threat indicators

USE CASE MAPPING TO ALERTS

Skurio Alerts	Login Credentials	Assets & Infrastructure	Employee Data	Customer Data
Email Addresses	• Corporate email domain	• User principal names (UPN) • Specific email addresses used to authenticate to systems	• VIP personal email addresses*	
IP Addresses		• IPv4 addresses		
Domains	• Web domains of services holding credentials	• Corporate email domain • Web domains • Sub domains • Fully qualified server names (FQDN)	• Web domains of services holding employee data	
Keywords	• Names of third-party services holding credentials	• Your company names(s) • Database column/field information • IPv6 addresses • Unique keywords or phrases describing business critical systems • Known unpatched vulnerabilities (CVEs)	• Your company name(s) • Database column/field information	• Your company names(s) • Database column/field information
Financial Information			• VIP credit card IIN/BIN with supporting identifying keywords	• Loyalty card IIN/BIN
Typosquatting		• Web domains • Product/service names		
BreachMarker			• Synthetic identities**	• Synthetic identities**

* With permission from VIP
** Create synthetic identities as BreachMarkers in Skurio platform then insert into database

GATHERING SEARCH TERMS

- IT department:
  - IT asset lists
  - Database structures
- Customer web sites
  - ‘About us’ page – board/executive, physical addresses
  - Corporate affairs to explore wider company structure
- Risk & compliance personnel
  - Information asset registry
- Open source research
  - DNSDumpster for sub-domains, IP addresses