DarkForce Cyber AI [CONFIDENTIAL]

Vol. XIV - Protocols

Order 66, Inc.

# Product Overview

Order 66’s **DarkForce Cyber AI** technology brings *nation-state security* to the enterprise. DarkForce learns your business IT *so you don’t have to*, premptively recognizing and disrupting novel threats “before they happen.” DarkForce “zero-config” technology means that even the tiniest threats are **automatically identified and exploded**, without relying on pre-built models or “detection rules.”

## Control Protocol

Control messages are bincode-encoded structs exchanged on port 19696/udp.

pub enum Request {  
 GetRules,  
 AddRule { rule: Rule },  
 DeleteRule { label: String },  
 GetTapEndpoint,  
 GetLogEndpoint,  
 SetLogEndpoint { address: String, port: u16 },  
}  
  
pub enum Response {  
 GetRules { rules: Vec<Rule> },  
 AddRule,  
 DeleteRule,  
 GetTapEndpoint { address: String, port: u16 },  
 GetLogEndpoint { address: String, port: u16 },  
 SetLogEndpoint,  
 Error(String),  
}  
  
pub struct Rule {  
 pub label: String,  
 protocol: IpProtocol,  
 source\_address: ipnetwork::IpNetwork,  
 target\_address: ipnetwork::IpNetwork,  
 source\_port: Option<u16>,  
 target\_port: Option<u16>,  
 content: String,  
}  
  
pub struct CompiledRule {  
 pub rule: Rule,  
 content\_regex: regex::bytes::Regex,  
}  
  
pub enum IpProtocol {  
 Tcp,  
 Udp,  
}

## Tap Traffic

Tap endpoints run on 19697/udp by default, and should be provided L3 traffic.

## Log Protocol

Logging endpoints receive a stream of detection messages via UDP.

pub struct Detection {  
 pub rule: String,  
 pub source\_address: u32,  
 pub target\_address: u32,  
 pub source\_port: u16,  
 pub target\_port: u16,  
 pub content: Vec<u8>,  
}