A FEDERAL CYBER CENTER

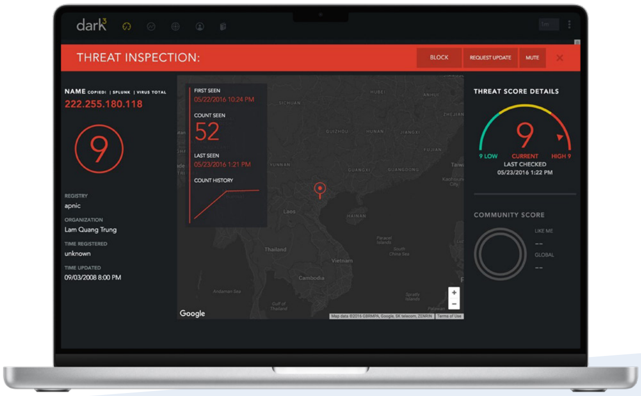
DoD CYBER CRIME CENTER

DoD–Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

DCISE^3 SIMPLY INTUITIVE CYBERSECURITY

DCISE recognizes the unique challenges faced by the small and medium businesses (SMBs) within the collective DIB, and has partnered with Dark Cubed to provide an automated threat detection, scoring, and blocking solution to our DIB CS Program participants at no cost.

Unlike other solutions and approaches, Dark Cubed is purpose-built for SMBs that don't have big budgets or security analysts. Even if a company doesn't have a single cybersecurity resource, DCISE^3 can provide significant value.



THREAT INSPECTION:

NAME COPIED! | SPLUNK | VIRUS TOTAL
222.255.180.118

9

REGISTRY
apnic

ORGANIZATION
Lam Quang Trung

TIME REGISTERED
unknown

TIME UPDATED
09/03/2008 8:00 PM

FIRST SEEN
05/22/2016 10:24 PM

COUNT SEEN
52

LAST SEEN
05/23/2016 1:21 PM

COUNT HISTORY

THREAT SCORE DETAILS
9
9 LOW CURRENT HIGH 9
LAST CHECKED
05/23/2016 1:22 PM

COMMUNITY SCORE
LIKE ME
--
GLOBAL
--

OFFERED AT NO COST TO DIB CS MEMBERS

38,109
AVERAGE NUMBER OF THREATS IDENTIFIED AND BLOCKED PER MONTH IN 2022

How Does It Work?

DCISE^3 integrates with a company's existing firewall and captures a real-time stream of metadata associated with network traffic that contains the IP address and domains with which communications are occurring.

DCISE^3 automatically aggregates this metadata and provides fully automated risk scoring capabilities for every network connection without requiring any human interaction. Risk scoring takes into account over **60** sources of threat intelligence (including DCISE indicators), years of historical data, and predictive algorithms to detect emerging threats.

- 15 Minute Deployment
- Agentless Approach

WE PROVIDE

Federal Compliance

Real-time Visibility

Traffic Analysis

Auto Blocking

Pub Date: 3 January 2023

DCISE^3 – SIMPLY INTUITIVE CYBERSECURITY

How DCISE^3 Supports NIST SP 800-171 Security Objectives

NIST SP 800-171	Requirement	DCISE^3 Helps
3.1.12	Monitor and control remote access sessions.	✓
3.3.1	Create, protect and retain information system audit records to the extent needed.	✓
3.3.3	Review and update audited events.	✓
3.3.5	Correlate audit review, analysis, and reporting processes.	✓
3.3.6	Provide audit reduction and report generation to support on-demand analysis and reporting.	✓
3.3.8	Protect audit information and tools from unauthorized access, modification, and deletion.	✓
3.3.9	Limit management of audit functionality to a subset of privileged users.	✓
3.13.1	Monitor, control and protect organizational communications at the external boundaries and key internal boundaries	✓
3.13.6	Deny network communications traffic by default and allow traffic by exception	✓
3.14.3	Monitor security alerts/advisories and take appropriate response actions	✓
3.14.6	Monitor the information system communications traffic	✓
3.14.7	Identify unauthorized use of systems	✓

How Can I Learn More?

DCISE is eager to support our Partners by offering **DCISE^3** as a service. Please contact us by email at **DC3.DCISE@us.af.mil**.

ABOUT DCISE

The DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE), a directorate within the DoD Cyber Crime Center, is the operational hub of DoD's Defense Industrial Base (DIB) Cybersecurity Program. DCISE develops and shares actionable threat products, performs cyber analysis and diagnostics, and provides remediation consultation for DIB participants.