MOSAICS
2020
INDUSTRY
DAY

dark3

Lessons Learned from Protecting the Defense Industrial Base Using Fully Anonymized, Machine-to-Machine Cybersecurity Analytics and Automated Protection

Dark3, Inc. (“Dark Cubed’)
Presented By: Vince Crisler, Founder & CEO

MOSAICS
2020
INDUSTRY
DAY

dark3

BLUF

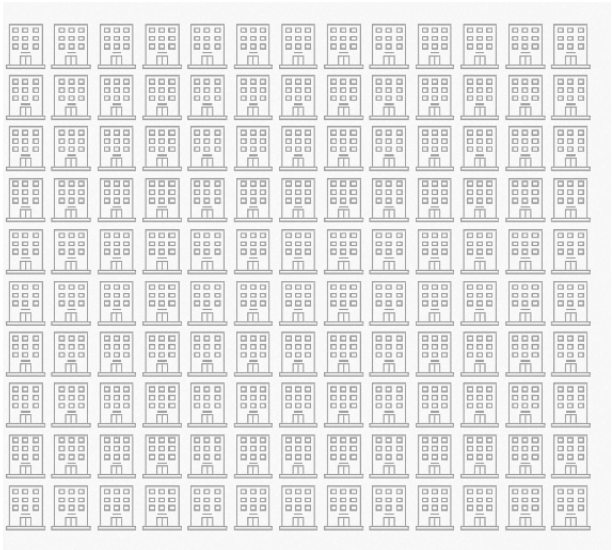
1. **Automated Two-Way Information Sharing:** Dark Cubed solves the problem of enabling automated two-way information sharing and protection for small and medium enterprises that make up Critical Infrastructure and the DIB.
2. **Analytics and Threat Hunting:** Dark Cubed's patented anonymization technology enables real-time analytics and threat hunting using network traffic without compromising the identity of participating companies.
3. **Unique Value:** Dark Cubed delivers unique value for automating and orchestrating cyber security analytics and protection for the mass market at a value that other solutions are unable to match.

MOSAICS
2020
INDUSTRY
DAY

dark3

Dark Cubed: Simple Concept, Massive Benefit

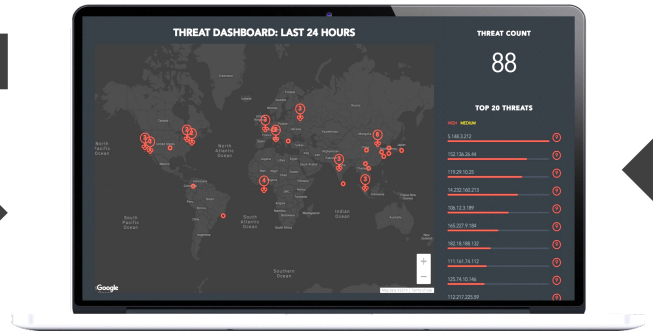
Industry / DIB / ICS Companies



Automated Machine-to-Machine Protection

Patented Anonymization Technology

Elegant SaaS Platform
(Available in AWS GovCloud)



Fully Automated Analytics

Enterprise-Grade Intelligence & Analytics

Dark Cubed is Commercially Available Today.

About the Pathfinder

1. Started in July 2019, currently ends in December 2020.
2. Originally funded for 10 companies, rapidly increased to 41
3. Goals and Objectives:
    1. Demonstrate ease of deployment
    2. Process and analyze live network traffic data (firewall logs / netflow)
    3. Fully automate threat intelligence integration and analytics
    4. Support two-way, machine-to-machine information sharing
    5. Integrate GFI related to threat intelligence
    6. Develop custom workflows and dashboards for DoD analysts

MOSAICS

2020 INDUSTRY DAY

dark3

Status

1. Parsed over 146 trillion unique network transactions
2. Actively monitoring 54 unique DIB company firewalls
3. Currently processing an average of ~6K events per second
4. Over 7 million unique IPs and Domains analyzed
5. Over 500,000 high threats identified in network traffic
6. Deployed proof of concept dashboarding and analytics capability containing ALL historical data from the pathfinder
7. Integrated automated scoring for GFI threat indicators for DIB company participants (over 68K indicators incorporated to date)

MOSAICS
2020
INDUSTRY
DAY

dark3

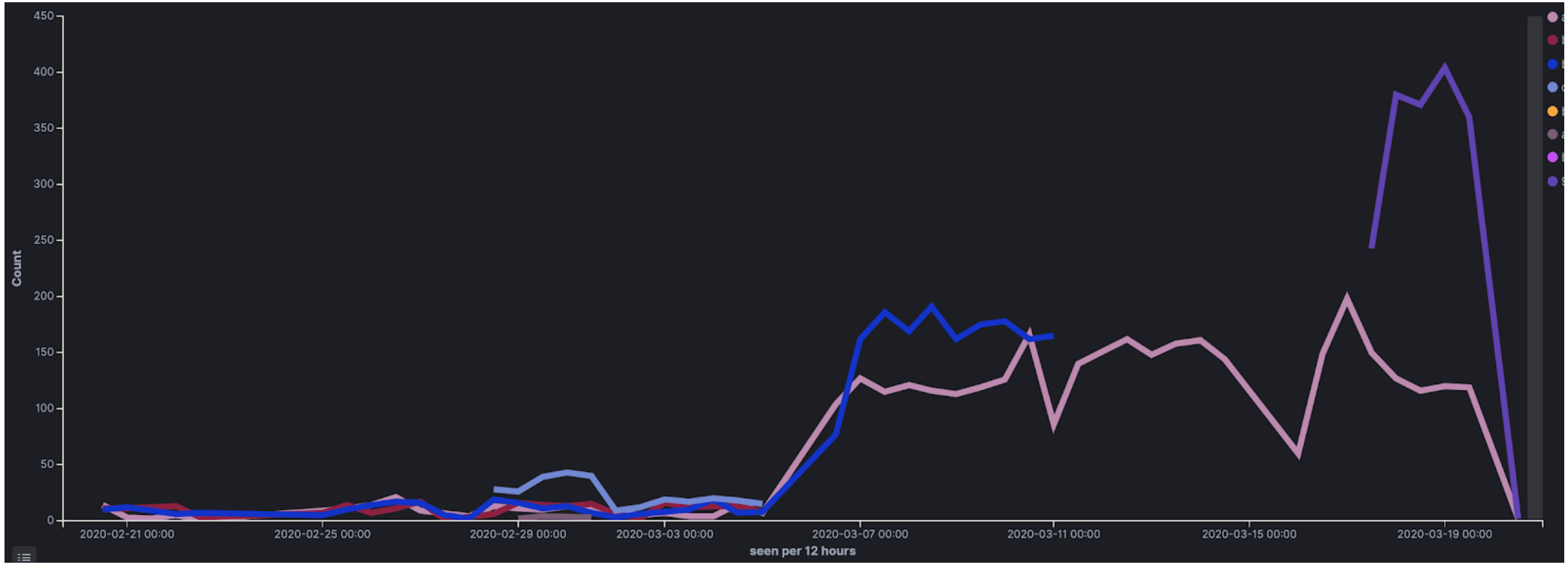
Key Findings

- **GFI Provides Value:** Only 27.8% of the GFI cybersecurity threat indicators provided by the DoD were identified in open-source data sets.
- **The DIB is Unique:** Network traffic associated with GFI indicators were disproportionately observed as active on DIB networks.
- **Two-Way Automated Sharing Works:** Small and midsized DIB companies participating are realizing value from the visibility and protection provided by this program.
- **The Analytics are Powerful:** The ability to perform analytics on anonymized network traffic across a diverse set of DIB companies provides powerful insight into threats and trends.

MOSAICS
2020
INDUSTRY
DAY

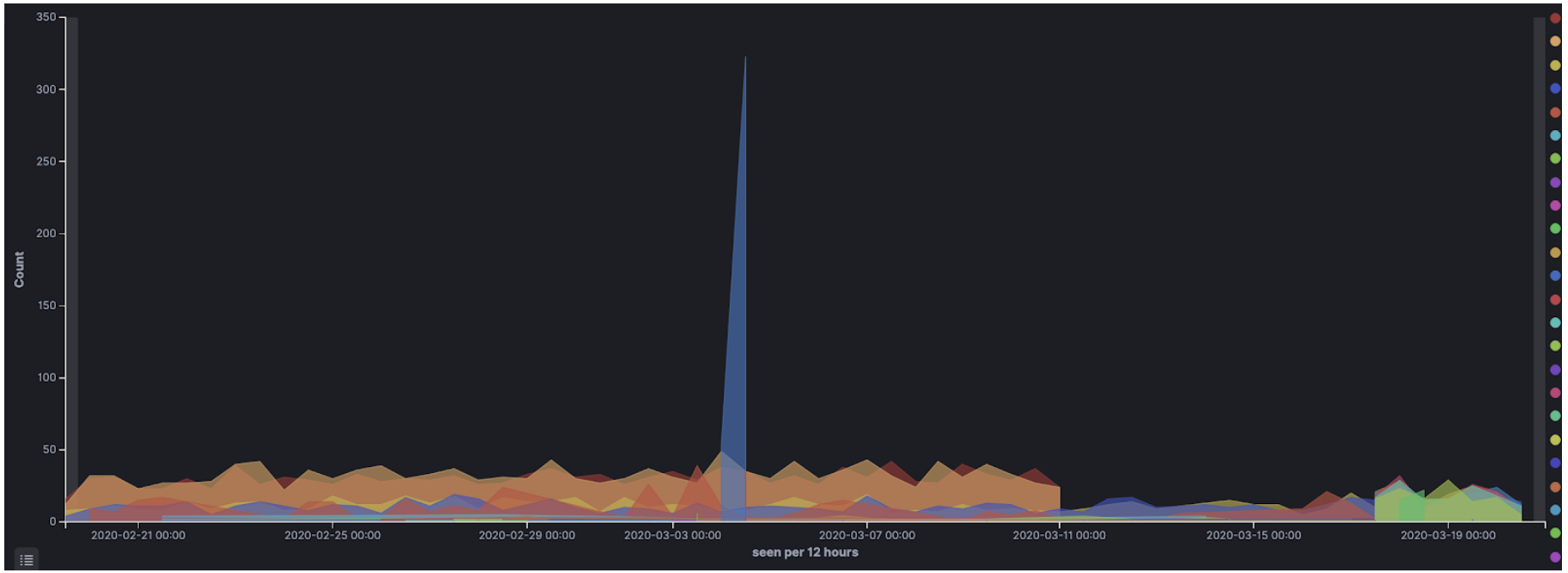
dark3

Example 1: Monitoring Activity of a Specific IP



dark3

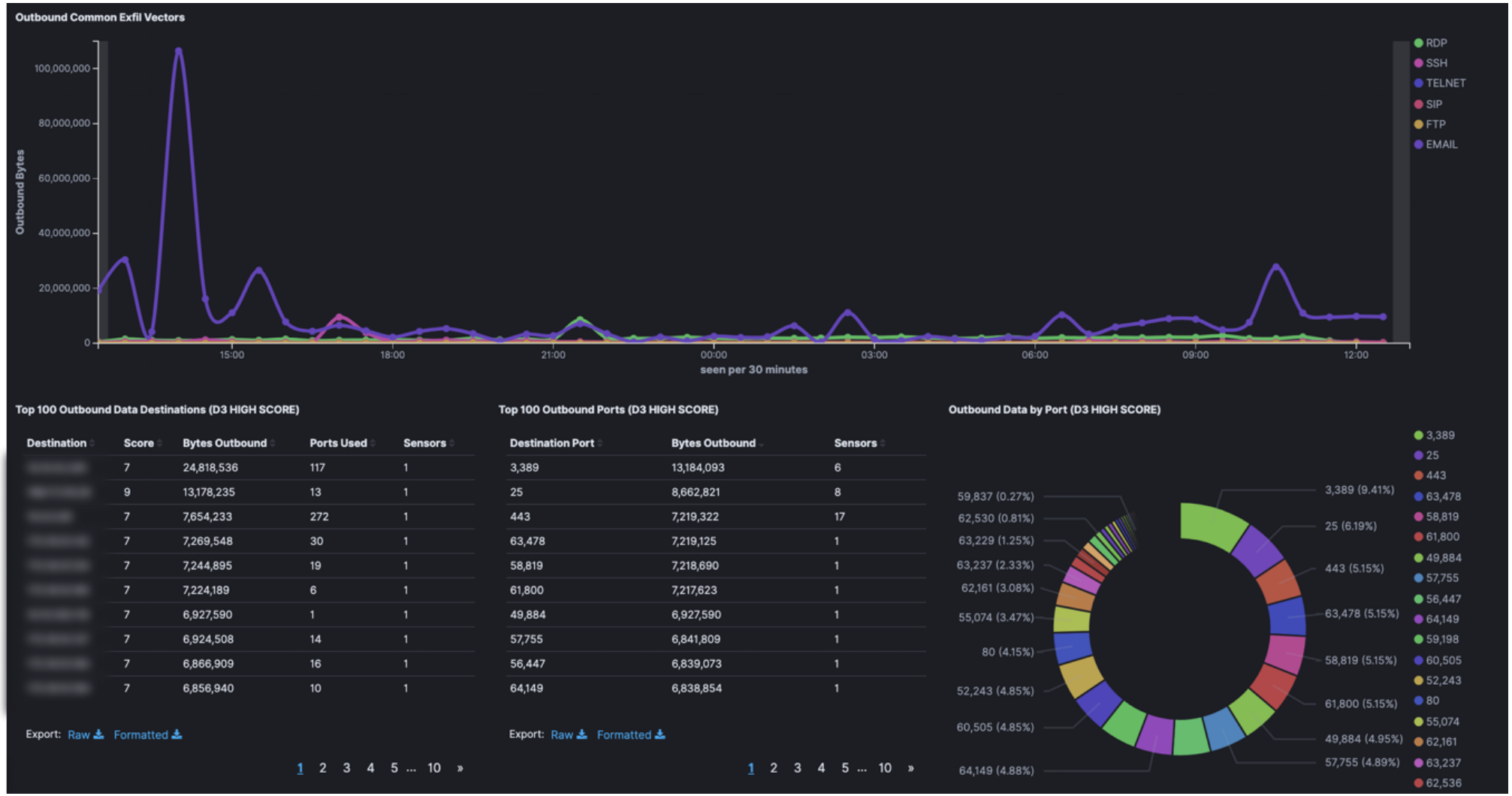
Example 2: Port 3389 Brute Force Attempt?



MOSAICS
2020
INDUSTRY
DAY

Example 3: Data Exfiltration

dark3



Top 100 Outbound Data Destinations (D3 HIGH SCORE)

Destination	Score	Bytes Outbound	Ports Used	Sensors
[redacted]	7	24,818,536	117	1
[redacted]	9	13,178,235	13	1
[redacted]	7	7,654,233	272	1
[redacted]	7	7,269,548	30	1
[redacted]	7	7,244,895	19	1
[redacted]	7	7,224,189	6	1
[redacted]	7	6,927,590	1	1
[redacted]	7	6,924,508	14	1
[redacted]	7	6,866,909	16	1
[redacted]	7	6,856,940	10	1

Export: Raw Formatted

1 2 3 4 5 … 10 »

Top 100 Outbound Ports (D3 HIGH SCORE)

Destination Port	Bytes Outbound	Sensors
3,389	13,184,093	6
25	8,662,821	8
443	7,219,322	17
63,478	7,219,125	1
58,819	7,218,690	1
61,800	7,217,623	1
49,884	6,927,590	1
57,755	6,841,809	1
56,447	6,839,073	1
64,149	6,838,854	1

Export: Raw Formatted

1 2 3 4 5 … 10 »

MOSAICS
2020
INDUSTRY
DAY

dark3

Where To Go From Here

1. Expand to more companies for more complete analysis and protection
2. Increase capabilities (advanced analytics, AI/ML integration, API development for orchestration)
3. Help DoD satisfy pending requirements from 2021 NDAA (Two Way Information Sharing and Threat Hunting)

MOSAICS
2020
INDUSTRY
DAY

MOSAICS & Dark Cubed

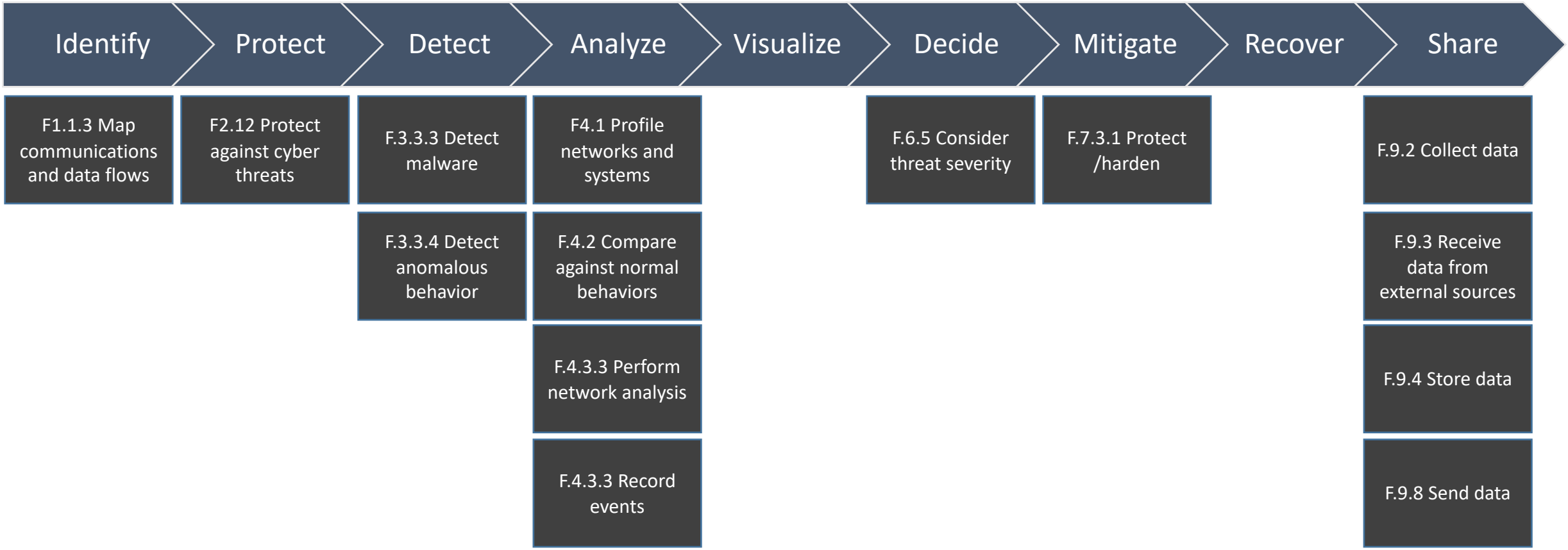
dark3

1. **Overlap of IT and OT:** Critical infrastructure represents a unique combination of IT and OT, with threats potentially affecting both infrastructures
2. **Influence of SMB:** A majority of CI/KR is made up of small and midsized companies with limited IT staff and security capabilities
3. **Proven Success:** Dark Cubed has proven an approach to automation and orchestration and two-way information sharing that works in the MOSAICS environment without impossible investments
4. **Anonymization is a Game-Changer:** Dark Cubed's patented anonymization approach enables real-time information sharing without the privacy and legal concerns

MOSAICS
2020
INDUSTRY
DAY

dark3

Alignment to Functional Requirements



dark3

What If?

Imagine what we could do with the ability to anonymously monitor, analyze activity associated with IPs, ports, and protocols in real-time across critical infrastructure at speed and scale?

Imagine being able to complement that with automated blocking and protection at network boundaries at machine speed without requiring humans in the loop?

MOSAICS
2020
INDUSTRY
DAY

dark3

POC

Vince Crisler
Founder and CEO
vince@darkcubed.com
(703) 398-1101

https://www.darkcubed.com
@darkcubedcyber