LOOKINGGLASS

SOLUTIONS BRIEF

# Assessing Cyber Risk for the Defense Industrial Base

## CHALLENGE

### Understanding the Cybersecurity Threats & Risks of 250,000 Defense Industrial Base Organizations

The cyber supply chain threat to all industries has become a critical risk and only grows more each day as businesses and organizations undergo digital transformations to improve their operations. However, with deep national security implications, the cyber risks associated with Defense Industrial Base (DIB) are perhaps the most urgent. Threat actors have realized that targeting vulnerable companies across the defense supply chain can be not only a profitable enterprise but also an alternate method to accessing valuable Department of Defense (DOD) information.

To manage these risks, the DOD included cybersecurity requirements and best practices, developed by the National Institute for Standards and Technology, in contracts and as part of the procurement process. To address continued concerns about implementation of cybersecurity best practices, the DOD developed the Cybersecurity Maturity Model Certification (CMMC), with third-party assessors and certifiers to provide greater assurance that DIB companies were taking cybersecurity seriously. While a big step in the right direction, the systems to fully establish and manage the CMMC process are still in development. Furthermore, should the CMMC move to a point-in-time review for certification, similar to the security and compliance checklist process that has been used to manage vendor risk over the past decade, these efforts will still fall short of the necessary continuous assessment of cyber risk needed for an industry as critical as the DIB.

## SOLUTION

### Continuous Supply Chain Risk & Exposure Assessments with Outside-In Internet Footprinting

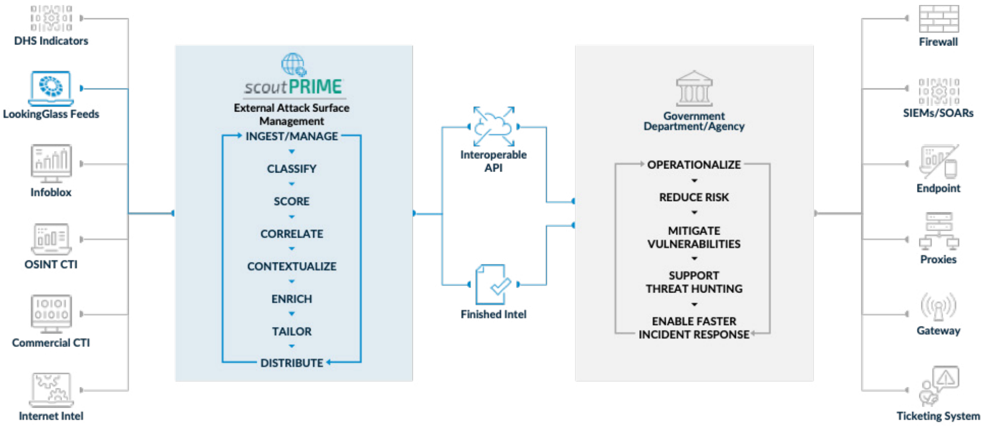
Simply understanding the cyber risk and exposures across the supply chain of 250,000 DIB companies, spanning a wide range of sectors, can be a massive undertaking. Assessing that supply chain continuously – reviewing networks, assets, and systems owned and managed by others for new exposures and vulnerabilities – only adds to the complexity. CMMC move to a point-in-time review for certification, similar to the security and compliance checklist process that has been used to manage vendor risk over the past decade, these efforts will still fall short of the necessary continuous assessment of cyber risk needed for an industry as critical as the DIB.

**LookingGlass provides insight and technical indicators to support a range of activities from high-level situational awareness to actionable recourse.**

## TECHNICAL CAPABILITIES

LookingGlass provides insight and technical indicators to support a range of activities from high-level situational awareness to actionable recourse. These can be leveraged to augment an existing security program by providing greater visibility into the threat landscape, examining a variety of vectors on the attack surface, and integrating into the existing security architecture deployments.

As a unified threat indicator system that supports the aggregation, enrichment, and correlation of cyber threat data to internet assets and passively assesses tailored groups of network assets, LookingGlass scoutPRIME® can easily monitor a sector as wide and diverse as the DIB quickly and continuously.



## *scout*PRIME

### Facilitates the ingestion, correlation, and displaying of:

- Internet intelligence (such as host enumeration, domain registration/WhoIs, pDNS, OSINT, and geolocation)
- Threat intelligence aggregation and enrichment (categorization and risk scoring)
- Tailored network footprinting
- Information sharing and collaboration
- Workflow integration via notifications and reporting and exposure.

## SECTOR FINDINGS

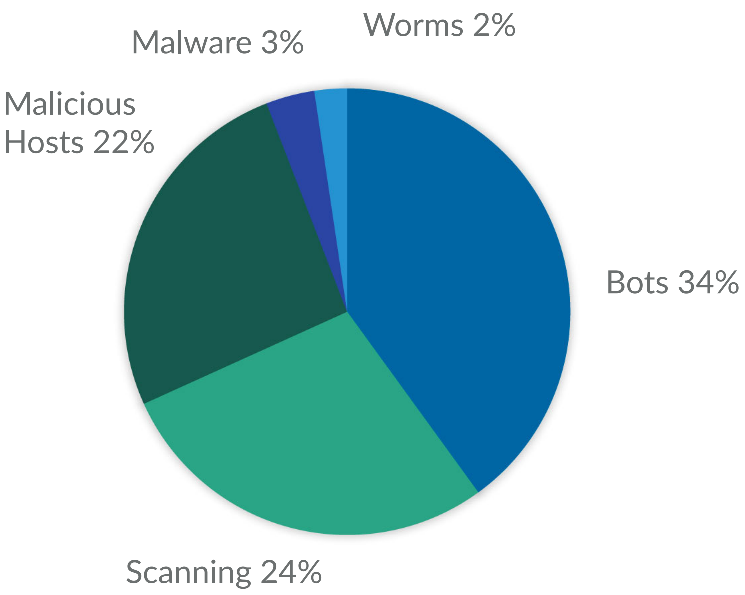
### LookingGlass's capabilities to monitor and assess the cyber risk for a sector can enable sector benchmarking and help organizations understand how they compare with the sector.

For the DIB sector, since the start of 2021, LookingGlass has found or observed:

- More than 5 million verified vulnerabilities and nearly 30 million inferred vulnerabilities or risks (e.g., risky services like Remote Desktop Protocol or open ports)
- More than 2,000 CISA AIS-reported threats/observables
- Nearly 170,000 instances of DIB assets acting as C2s for malware

## SECTOR FINDINGS

### Five Largest Threats



### Top 5 Bots

Gumblar

Sality

Xorddos

Smokeloader

Bot Zero

### 8 Observed APTs

APT1

APT28

Comfoo

EquationDrug

Pitty Tiger

Red October

Stuxnet

Wild Neutron

## OUTCOME: ACTIONABLE THREAT INTELLIGENCE

To help the U.S. federal government better understand the cyber risk across the DIB, the DOD's Cyber Crime Center (DC3) turned to LookingGlass.

Through a pilot program called Krystal Ball, DC3 leveraged LookingGlass's scoutPRIME solution to digitally footprint nearly 900 DIB companies' digital infrastructure in less than two days. This gave DC3 an outside-in view of those companies, enabling them to see what adversaries can see from the public-facing internet.

Next, each company's footprint was automatically overlaid with threat intelligence, fed from dozens of threat intelligence feeds, highlighting and identifying vulnerabilities, exposures, and threats. This feeds the LookingGlass Threat Indicator Confidence (TIC) score, providing a risk assessment that updates based on new vulnerabilities, exposures, and threats. By leveraging scoutPRIME's 24x7x365 capability, Krystal Ball enables DC3 to notify any of the participating DIB companies of vulnerabilities and threats in near real time.

## OUTCOME: ACTIONABLE THREAT INTELLIGENCE

CONTINUED...

Though only a few months along, the Krystal Ball program has already demonstrated critical mission impact. Rear Admiral William Chase III, Deputy Principal Cyber Advisor to the Secretary of Defense and Director of Protecting Critical Technology Task Force testified at the Senate Armed Services Committee, Cybersecurity Subcommittee hearing on Cybersecurity of the Defense Industrial Base in May of 2021 about the initial results of the LookingGlass program:

> *"They ... identif(ied) the vulnerabilities and threats inbound and those were used to identify and notify 13 DIB partners of Chinese malicious actors attacks on the Microsoft Exchange Server vulnerabilities. ...We must continue to pilot these concepts of operation and capabilities and then scale the successful ones. The direct provisioning of cybersecurity capabilities to contractors, including the provisioning of secure environments for development and the storage of controlled unclassified information, is incredibly promising."*

## ABOUT LOOKINGGLASS

LookingGlass is a global cybersecurity leader that provides public and private sector clients with tailored, actionable threat intelligence and active defense capabilities delivered at machine speed. For more than a decade, the most advanced organizations in the world have trusted LookingGlass to help them protect their financial, economic, and national security interests.

Find out how we can help your organization at https://www.lookingglasscyber.com