DRAGOS

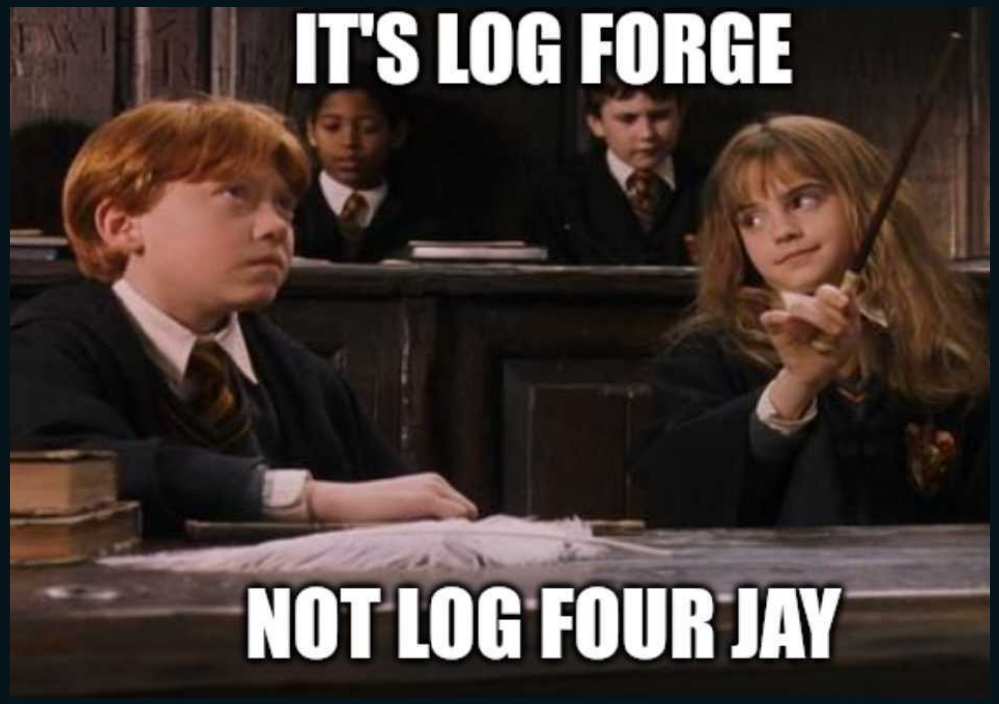
THE LOG4J VULNERABILITY

IMPLICATIONS FOR OT NETWORKS

Seth Lacy
Principal Adversary Hunter

Kai Thomsen
Director,
Global Incident Response Services

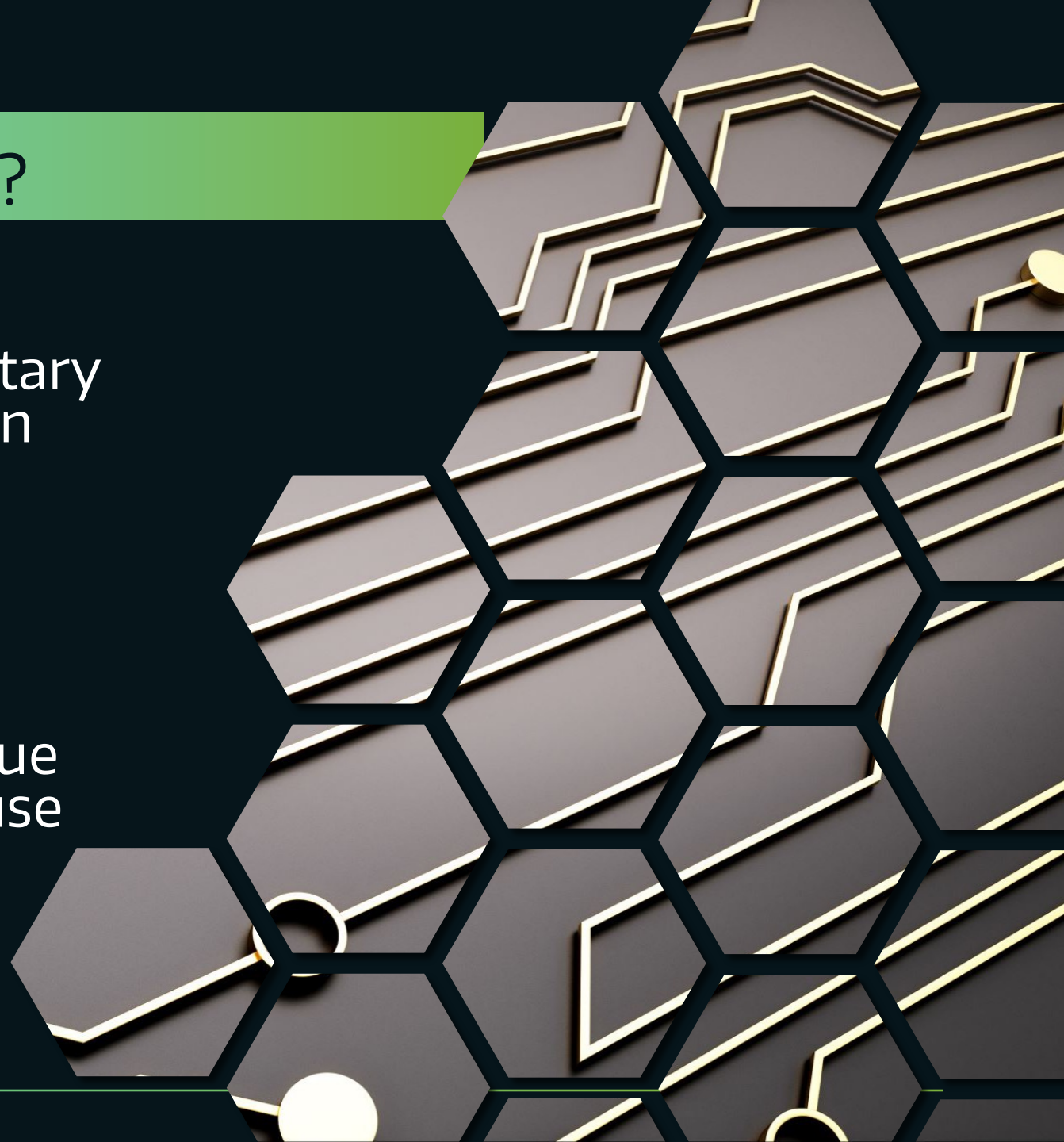
WHAT IS LOG4SHELL?



- Vulnerability allows remote code execution through specially crafted data request packets.
- Java naming and directory interface (JNDI) lookup feature allows variable retrieval.
- Log4j tries to connect to the provided resource to fetch whatever is needed to resolve the variable.
- An adversary can send data containing a malicious JNDI reference to a server using any protocol.

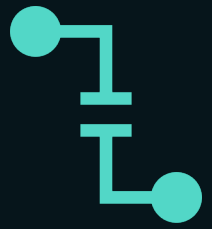
WHAT IS THE RISK TO ICS?

- Log4j is found in popular proprietary and open-source software used in industrial applications.
- OT vendors have just begun to disclose the impact of this vulnerability.
- Additional disclosures will continue as vendors work to identify the use of Log4j across their product lines, but this will take time.



HOW CAN THIS BE MITIGATED?

Weigh all mitigation steps against the potential to cause an unintentional operational impact.



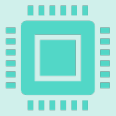
Potential to become a persistent vulnerability within industrial control systems environments.

More **details** on potential **remediations/mitigations** are included in **our blog post.**

HUNTING FOR LOG4J IN ICS ENVIRONMENTS

- Approach this issue with an "assume-breach mentality."
- Focus on egress traffic - hunting for outbound signatures of successful exploitation can help improve the signal to noise ratio.
- Vulnerability could also be leveraged for lateral movement.
- Hunt for traditional markers of post-exploitation activity.

HUNTING FOR LOG4J IN DRAGOS PLATFORM



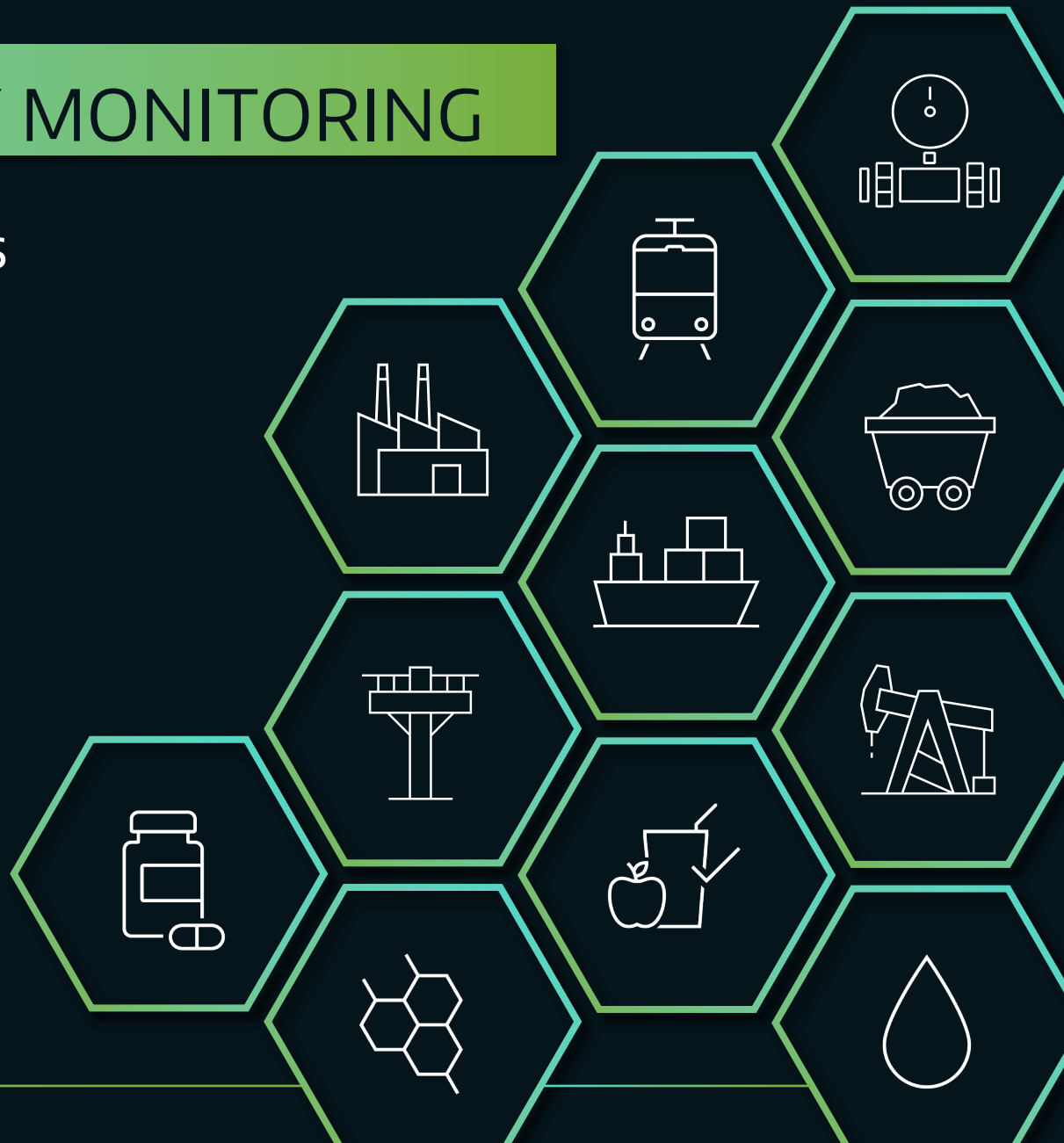
As part of the next Dragos Knowledge Pack (KP), we will be providing network-based detections for ICS-based active Log4j exploitation, including some of the obfuscated exploit attempts that we have observed.

We expect the KP to be available this week for early access (EA) deployment to the Dragos platform.

Prior to having the KP, Dragos platform customers can leverage Log4j hunt queries that have been provided to the System Architect team to search for active Log4j exploitation within their ICS environments.

GENERAL ADVICE ON SECURITY MONITORING

- We are very early in the lifecycle of this vulnerability
- Exploit methods will change over time
- For more stable detection, focus on post-exploitation techniques, tactics, and procedures (TTPs)
- We have seen LDAP(S), RMI, and DNS used as channels. Focusing monitoring efforts on LDAP(S) is not sufficient!



INCIDENT RESPONSE RECOMMENDATIONS

Ensure you have a dedicated ICS Incident Response Plan and everyone in your org is aware of the plan and their role in it

Know what your most important systems (“Crown Jewels”) are

Know what data is available from the Crown Jewels to conduct incident analysis

Have a safe method established, trained, and tested to acquire forensic data (as a minimum memory and key OS artifacts) from ICS systems

Q&A

- What applications are affected?
  - Most comprehensive list is at https://github.com/NCSC-NL/log4shell/blob/main/software/README.md
  - There will be many more applications added and many more vulnerable applications so niche that they are not added to the list!
- Are other derivative libraries like Log4Net affected by this?
  - Not that we know. It is best to monitor the web sites for these libraries regularly for security updates as the situation develops.

READ THE RELATED BLOG

dragos.com/blog/industry-news/implications-of-log4j-vulnerability-for-ot-networks/