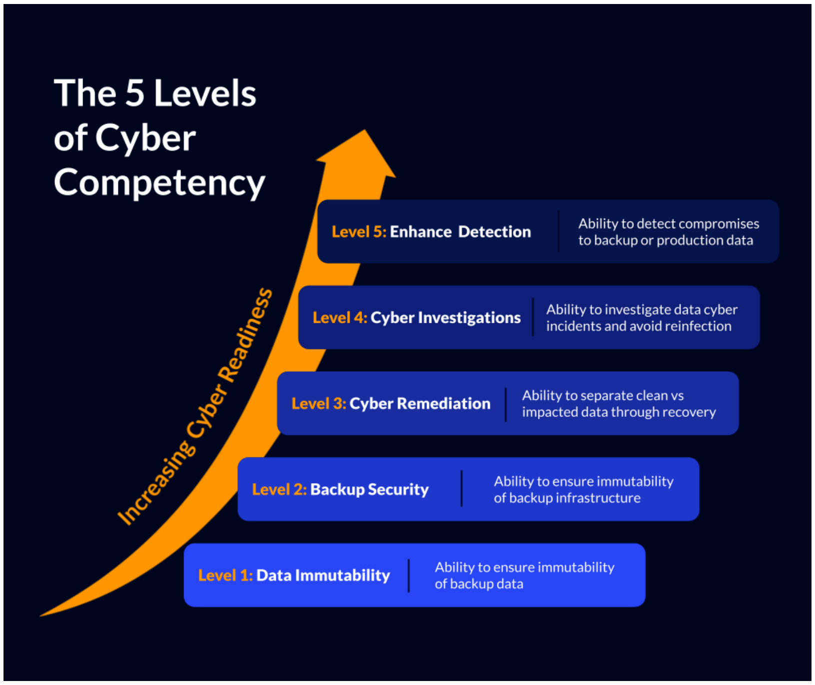
Achieving Cyber Resilience — Cyber Investigations — L4

Ability to Investigate Data Cyber Incidents and Avoid Reinfection

After implementing remediation processes, the next priority is cyber investigation. Investigating data breaches and preventing reinfection are critical tasks that often involve complex analysis across multiple data points and resources. Security teams must reconstruct a clear incident timeline to understand the breach and determine the most effective response. Throughout this process, it's essential to ensure regulatory compliance to meet legal and industry requirements.

Monitoring for Threats: Proactively monitor for unusual access patterns to detect potential threats early. Access attempts from unfamiliar locations, for example, can be an early indicator of a compromise. Early detection helps reduce dwell time, identify attacks more quickly, and minimize potential damage. As your investigation and threat-hunting capabilities mature, you'll be in a stronger position to enhance overall threat detection, further safeguarding against future attacks.


The 5 Levels of Cyber Competency
Increasing Cyber Readiness
Level 5: Enhance Detection
Ability to detect compromises to backup or production data
Level 4: Cyber Investigations
Ability to investigate data cyber incidents and avoid reinfection
Level 3: Cyber Remediation
Ability to separate clean vs impacted data through recovery
Level 2: Backup Security
Ability to ensure immutability of backup infrastructure
Level 1: Data Immutability
Ability to ensure immutability of backup data

Druva Can Lead You to Cyber Remediation

After strengthening your cyber investigation capabilities, focus on enhancing threat detection, especially through backups. Bad actors often target backups by deleting, encrypting, or changing retention policies to hinder recovery. Establish strong tools and processes to thoroughly **investigate** and understand breaches, ensuring that recovery is not only fast but also free from reinfection. These **incident investigation capabilities** are essential for minimizing the impact of an attack and ensuring regulatory compliance. However, this level also sets the stage for **next-generation threat detection** that can spot compromises earlier in the attack lifecycle.

Key questions for your team:

- How do you gather insights from backup data to investigate incidents and prevent reinfection?
- Can your security team easily assess and understand the scope of compromised data?
- How do you ensure that recovery is safe and tested in a secure environment?

Strengthen Cyber Resilience with Druva

Druva's Data Security Cloud provides a robust, cloud-native platform that addresses critical gaps in incident response and recovery workflows. Built on secure AWS infrastructure and using a zero-trust security model, it delivers comprehensive protection to help organizations advance through every level of cyber competency.

druva Sales: +1-800-375-0160 | sales@druva.com

Americas: +1-800-375-0160
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300

Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com

Druva is the leading provider of data security solutions, empowering customers to secure and recover their data from all threats. The Druva Data Security Cloud is a fully managed SaaS solution offering air-gapped and immutable data protection across cloud, on-premises, and edge environments. By centralizing data protection, Druva enhances traditional security measures and enables faster incident response, effective cyber remediation, and robust data governance. Trusted by over 6,000 customers, including 65 of the Fortune 500, Druva safeguards business data in an increasingly interconnected world. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.