elastic security labs

Elastic Security protections added:

MAY 2025

Rule additions and MITRE ATT&CK emphasis

52 rules added

SIEM

44
new rules

+18 to Defense Evasion

EDR

8
new rules

+4 to Execution
+4 to Defense Evasion

elastic security labs

Notable updates for SIEM rules

- Detections for **BadSuccessor,** which targets **Windows Active Directory 2025** and abuses delegated managed service accounts (dMSAs).

- Expansion in **Linux threat detection** for covert SSH tunneling, kernel abuse, PAM backdoors, suspicious process trees, and stealthy file activity. Stronger detections for obfuscated scripts, container artifacts, and abuse of system paths.

- Broad coverage added for **PowerShell obfuscation techniques**, **Windows Sandbox** abuse for evasion, suspicious **WebDAV** activity, abnormal **ADS** usage, and potential data exfiltration. Key rules tuned for accuracy around startup behavior, registry changes, and backup manipulation.

elastic security labs

Notable updates for EDR rules

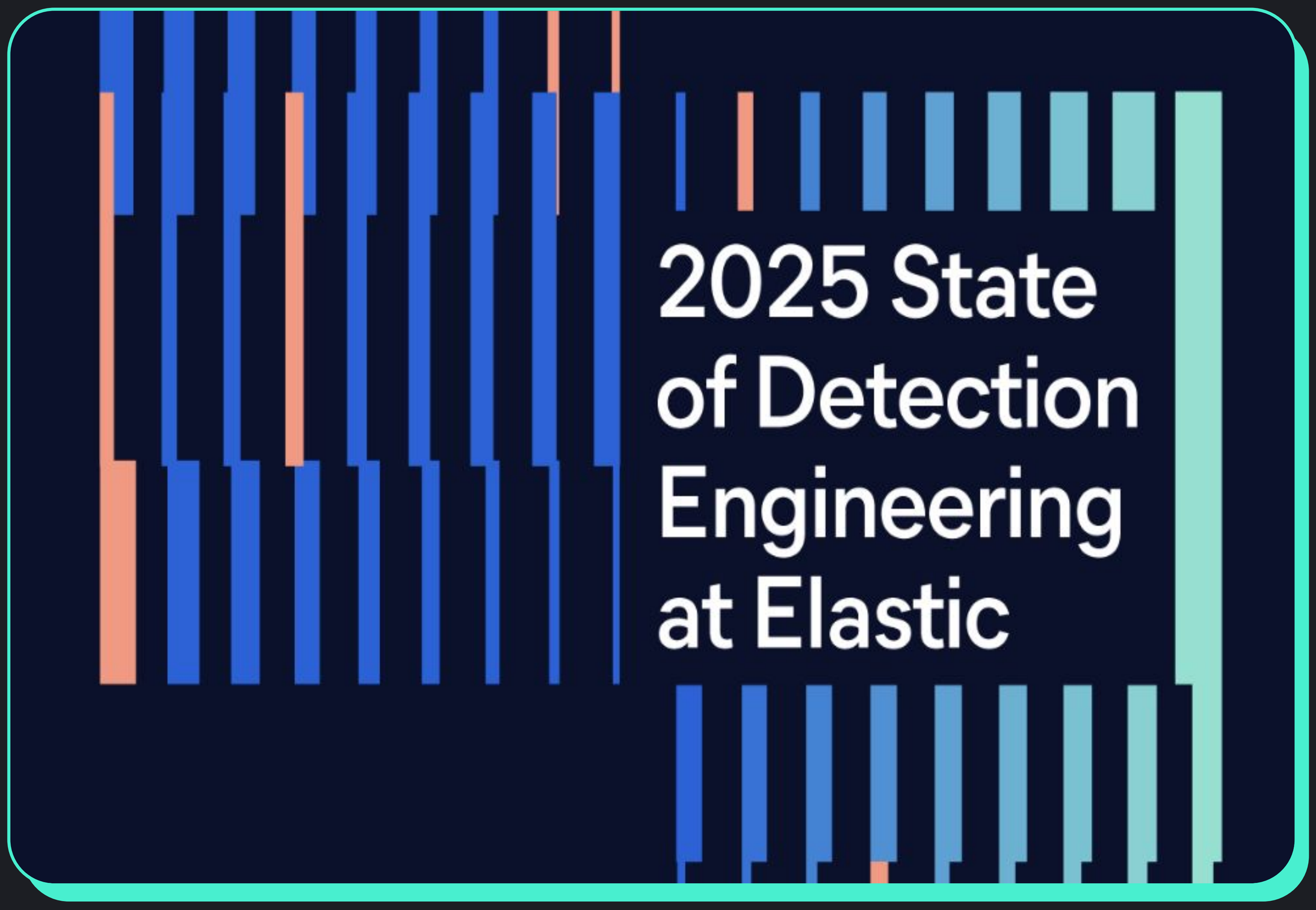
New Linux coverage for **Netcat** file transfering, several Privilege Escalation techniques, container escapes, SSH tunneling, base64 obfuscation, and system binary masquerading.

Improved Windows visibility into **PowerShell Empire** usage, obfuscated and malicious script execution (including PHP), API evasion via sleep hooking, and memory tampering through unsigned DLLs. Identify suspicious asynchronous procedure calls and potential NetNTLMv1 downgrade attacks.

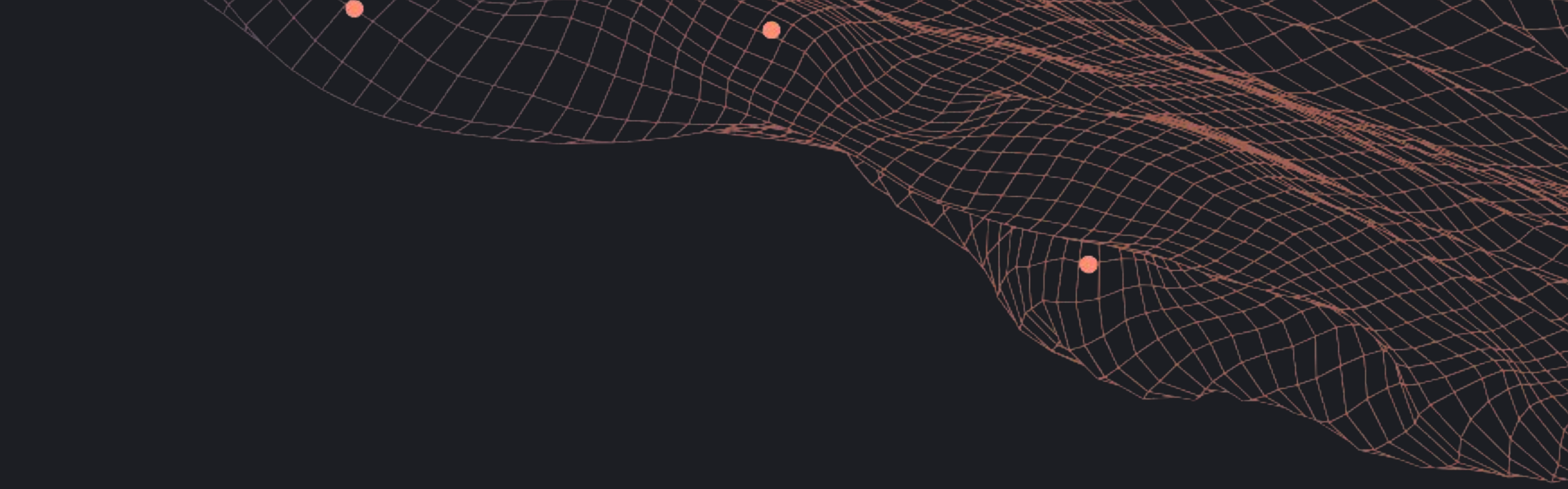
Diagnostic and production tuning trimmed noisy rules and **improved detection precision across macOS, Linux, and Windows** — maintaining Elastic's trend toward quieter, higher-fidelity alerting.

elastic security labs

See how we maintain these rulesets at **ela.st/sdee**



elastic security labs



Learn about the latest discoveries

elastic.co/security-labs

elastic security labs