THREATLOCKER®

Secure AI Starts With Control

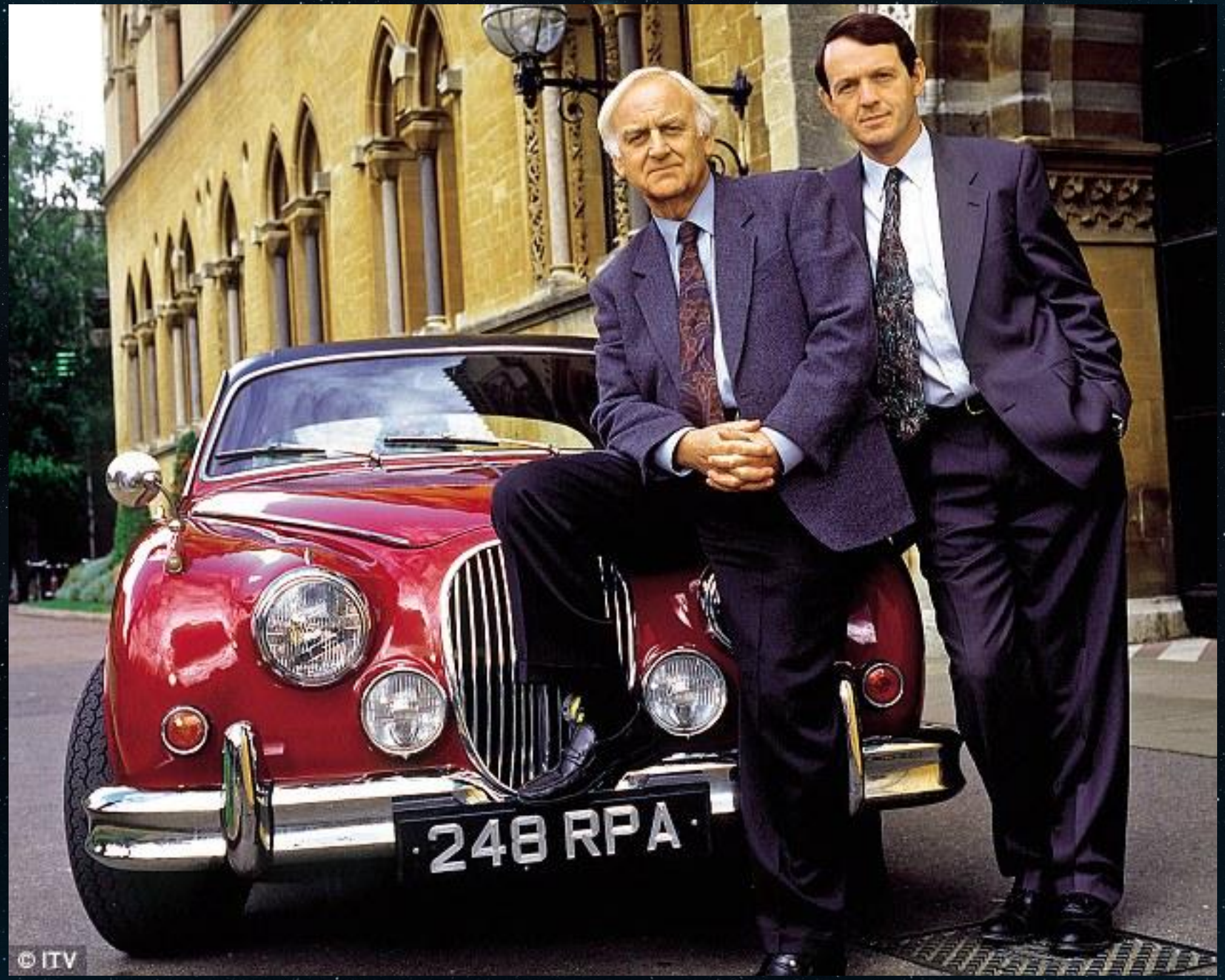
Default Deny, Ringfencing, and Zero Trust

Eoin McGrath

Solutions Engineer

Why do we care?

- Zero Day Vulnerabilities
  - Exploits targeting undisclosed software flaws
- Supply chain risks
  - Attacks via 3rd party vendors software or hardware
- These remain the top threats as of early 2026


248 RPA
© ITV

Jaguar Land Rover

- August/September 2025
- Costs of £1.9 Billion to the UK economy – that’s about $2.6
- Production halted for 5 weeks
- Lively hood of 1000’s of workers and related companies threatened

How it happened

- The attack was attributed to “Scattered Lapsus$ Hunters” a combination of known groups like Scattered Spider, Lapsus$, and ShinyHunters.

- Primarily known for social engineering attacks

Techniques

- Social Engineering – reports of employee's social media being studied beforehand
- Credential Compromise – weak MFA and token theft

Configuration Manager

Defense Against Configurations (DAC)

Techniques

- Exploitation of misconfigurations, weak network segmentation, and vulnerable systems
- Unsupported version of SAP NetWeaver
- Zero-day in an RMM

ThreatLocker Patch Management

Network Control

Ringfencing™

Defense Against Configurations (DAC)

Techniques

- Lateral movement across the network, eventually reaching the critical IT systems tied to manufacturing and ERP
- Deployed ransomware and other malicious software to take down core systems. Production couldn’t be isolated due to “Smart Factory” setup

Allowlisting

Ringfencing™

Storage Control

Network Control

Conclusion

- This wasn’t an OT attack – but rather an attack on vunerable IT systems that cascaded

Dealing with Zero Days

Adopt Zero Trust

Application Allowlisting

Vulnerability Management & Patching

Enhanced Monitoring and Detection

Defence Strategies Against Supply Chain Risks

Third Party Risk Management

- Vet and monitor vendors continuously.
- Use questionnaires on secure development practices; require SBOMs (Software Bill of Materials) for transparency. Conduct regular audits.
- Identifies weak links early; mandates zero-day response capabilities from suppliers.

Supply Chain Visibility Tools

- Track components and dependencies.
- Implement SBOM generation; use tools like Dependency-Track for open-source scanning.
- Reveals hidden vulnerabilities; essential for AI/ML components in 2026.

Secure Development and Acquisition

- Integrate security from the start.
- Follow NIST's Secure Software Development Framework (SSDF); reduce third-party apps unless business-critical.
- Prevents built-in flaws; applies to both commercial and open-source software.

Honeytokens and Deception Tech

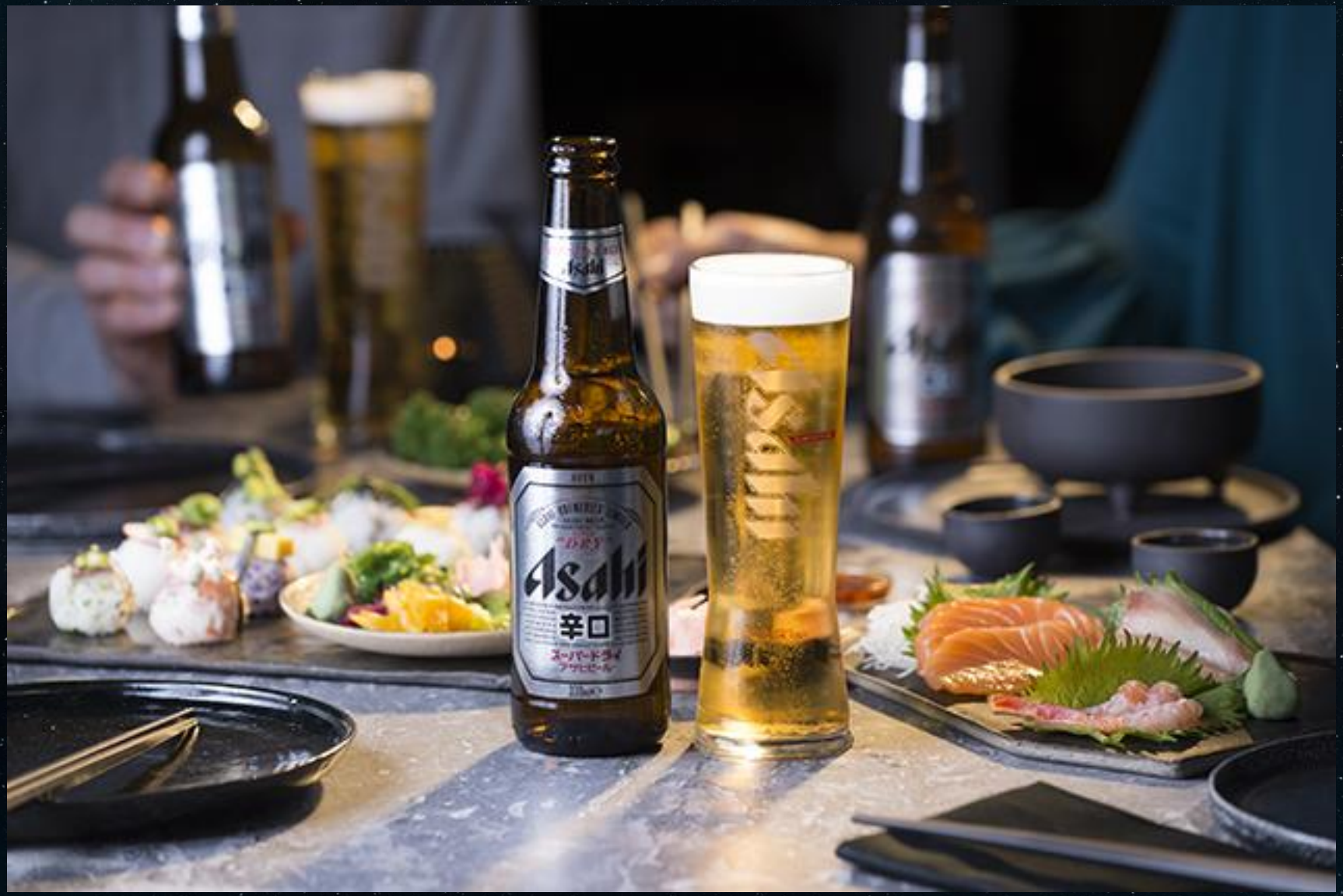
- Deploy traps for early detection.
- Use honeytokens in code; set up decoy systems in supply chains.
- Alerts to unauthorized access; disrupts attackers probing chains.

Backup and Segmentation

- Isolate and protect critical assets.
- Enforce network segmentation; store backups off-site with 30-day retention.
- Limits blast radius; enables recovery from chain compromises.

Overlapping and Integrated Strategies

- **Defence-in-Depth**
  - Layer controls (e.g., ZTA with EDR/NDR) to handle unknowns. Combine with threat intelligence sharing.
- **People and Processes**
  - Train on social engineering; assume breach in planning. Use frameworks like CISA's POEM for insider threats.
- **Emerging Tech Integration**
  - Leverage AI for anomaly detection, but govern models to avoid new risks.
- **Metrics and Continuous Improvement**
  - Measure with exposure surface reduction and response SLAs. Budget 10-15% for vulnerability management.


Asahi
辛口

Asahi Group

- September 2025
- Halted production at 30 factories in Japan
- Forced manual order processing (pen & paper)
- Personal data of over 2 million people was exposed

How it happened

- Qilin (a Russia-linked RaaS operation active since ~2022, known for high extortion demands) claimed responsibility around early October 2025
- Initial access was via Network equipment at on of the groups sites, this gave a toehold to the data centre network

Techniques

- Common Initial Vectors
  - Credential-based intrusion, likely starting with phishing/vishing
  - Fake service provider pages to harvest credentials, or MFA bypass/interception (e.g., OTP trapping)
- Once inside, attackers misused remote-access tools or exploited weak segmentation.

Network Control

Ringfencing™

Defense Against Configurations (DAC)

Techniques

- **Escalation and Lateral Movement**
  - From the initial entry point, they moved laterally across the network, reaching core data centre servers and connected PCs/devices.
- **Ransomware Deployment**
  - On September 29, ransomware was deployed **simultaneously** across multiple active servers, encrypting files and causing widespread outages. This affected ERP/logistics systems critical to ordering, shipping, and production coordination.
- **Data Exfiltration**
  - Prior to or during encryption, attackers stole data (confirmed by Qilin's leak site postings and Asahi's traces of unauthorized transfers).

Network Control

Ringfencing™

Allowlisting

Storage Control

Conclusion

- Mirrors trends in 2025
  - human-targeted entry (social engineering over zero-days), rapid encryption of business-critical IT, double-extortion (encrypt + leak), and severe operational fallout in manufacturing/consumer goods.

Resources

Jaguar Land Rover

- **Wikipedia Entry** (detailed overview with sources): https://en.wikipedia.org/wiki/Jaguar_Land_Rover_cyberattackCovers the attack timeline, claimed responsibility by "Scattered Lapsus$ Hunters," economic impact (£1.9 billion to UK economy), and production halts.
- **BBC News - Heavy Loss After Cyber-Attack** (November 2025): https://www.bbc.com/news/articles/ckg1w255gy1oReports on financial losses, production shutdowns lasting over a month, and why it's considered the costliest UK cyber incident.
- **Reuters - Economic Cost to UK** (October 2025): https://www.reuters.com/sustainability/boards-policy-regulation/jaguar-land-rover-hack-cost-uk-economy-25-billion-report-says-2025-10-22 Independent report estimating £1.9 billion ($2.55 billion) damage, supply chain effects on thousands of organizations.
- **Cybersecurity Dive - Q3 Sales Slump** (January 2026): https://www.cybersecuritydive.com/news/jaguar-land-rover-q3-sales-slump-cyberattack/808864 Updates on lingering sales impacts and recovery from the 2025 attack.
- **TraceSecurity - The Hack Explained**: https://www.tracesecurity.com/blog/articles/the-jaguar-land-rover-hack-explainedBreaks down the breach, data theft, and claims by a collective of hacker groups (Scattered Spider, Lapsus$, ShinyHunters).
- **Claroty - 5 Security Takeaways**: https://claroty.com/blog/5-security-takeaways-from-the-jaguar-land-rover-cyberattackFocuses on lessons for manufacturing/OT security and network segmentation.

Asahi Group

- **Official Asahi Statement - Investigation Results** (November 27, 2025): https://www.asahigroup-holdings.com/en/newsroom/detail/20251127-0204.html Direct from the company: confirms ransomware, encryption details, data exposure (up to ~1.9 million records, including 1.5+ million customers), and future security measures.
- **BBC News - 1.5 Million Customers' Data Potentially Leaked** (November 2025): https://www.bbc.com/news/articles/ce86n44178no Covers the attack's operational disruption (production halts, manual processes), Qilin ransomware claims, and drinks shortages in Japan.
- **Reuters - Logistics Restoration Target** (November 2025): https://www.reuters.com/world/asia-pacific/personal-details-15-million-asahi-group-customers-may-have-been-leaked-2025-11-27 Updates on recovery timeline (aiming for February 2026 normalization), no ransom paid, and Qilin attribution.
- **The Asahi Shimbun - Possible Leak of 1.91 Million Records** (November 2025): https://www.asahi.com/ajw/articles/16184778 Japanese perspective on the apology from CEO, data types exposed, and Qilin responsibility.
- **Industrial Cyber - Suspension of Operations**: https://industrialcyber.co/manufacturing/brewer-asahi-suspends-domestic-operations-after-cyberattack-disrupts-ordering-and-shipping Early reporting on initial disruptions to ordering, shipping, and call centers.

Resources

Nist & CISA

- **NIST SP 800-161 Rev. 1 (Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations)**: Comprehensive guide on identifying, assessing, and mitigating supply chain risks, including strategy, policies, and risk assessments. https://csrc.nist.gov/pubs/sp/800/161/r1/final (Updated version with enhancements for C-SCRM integration.)
- **CISA - Defending Against Software Supply Chain Attacks**: Joint CISA/NIST resource with recommendations for customers and vendors using NIST C-SCRM Framework and Secure Software Development Framework (SSDF).https://www.cisa.gov/resources-tools/resources/defending-against-software-supply-chain-attacks
- **CISA Zero Trust Maturity Model Version 2.0**: Details Zero Trust Architecture (ZTA) pillars, including micro-segmentation, continuous verification, and implementation for reducing zero-day and lateral movement risks.https://www.cisa.gov/zero-trust-maturity-model
- **CISA Zero Trust Microsegmentation Guidance (Part One: Introduction and Planning, July 2025)**: Practical steps for micro-segmentation in ZTA to limit blast radius from exploits. https://www.cisa.gov/sites/default/files/2025-07/ZT-Microsegmentation-Guidance-Part-One_508c.pdf

Industry

- **Google Threat Intelligence - 2024 Zero-Day Trends** (relevant for 2025–2026 outlook): Analysis of enterprise-focused zero-days targeting security/network products. https://cloud.google.com/blog/topics/threat-intelligence/2024-zero-day-trends
- **Verizon 2025 Data Breach Investigations Report**: Covers zero-day exploits on edge devices/VPNs and supply chain implications. https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf