Cyber Defence

UK CYBER DEFENCE · EMILYAI IN NUMBERS

EmilyAI in Numbers: August to October 2026

What EmilyAI and our SOC analysts did for our clients in three months, in figures and stories · Published 30 October 2026

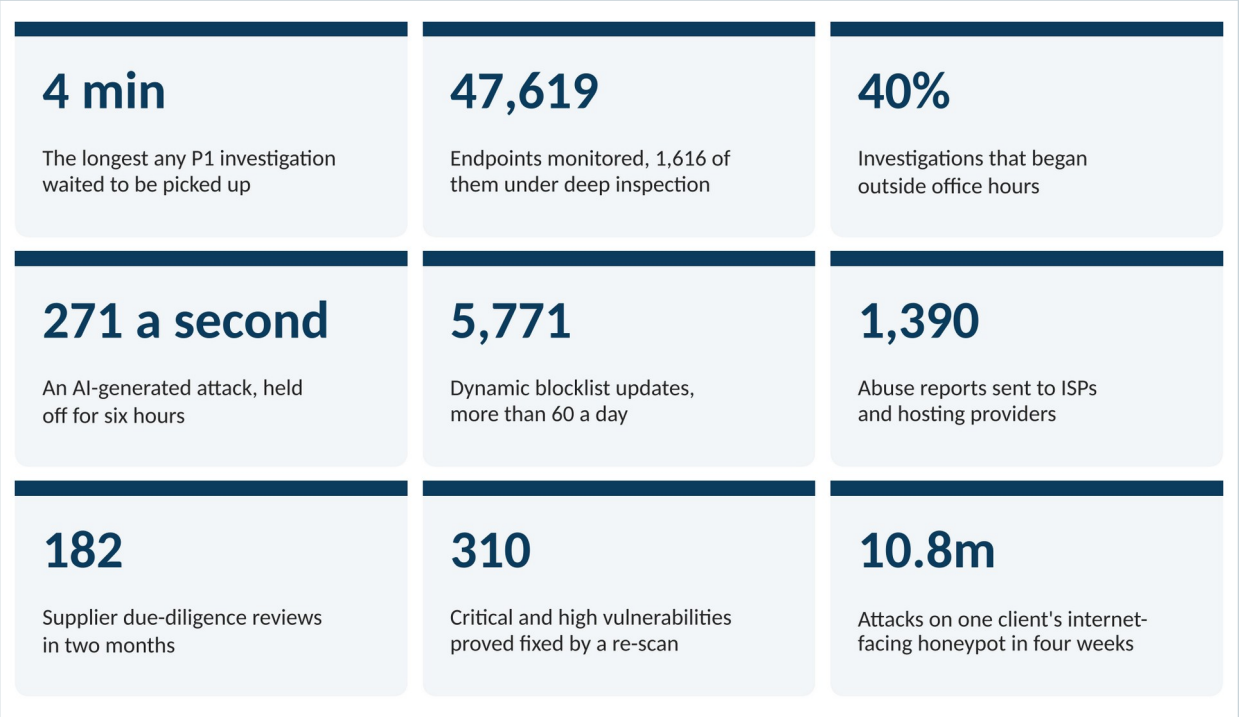


Figure 1. The quarter in nine figures.

In brief. EmilyAI is the AI at the heart of our security operations centre, in service since April 2018. From August to October 2026, EmilyAI and our two SOC analysts opened 63 security investigations and threat advisories for 11 client organisations, and Emily, EmilyAI's AI analyst, first raised 56 of them. Every priority 1 investigation was picked up within four minutes, and every priority 2 within the hour. Around three in four alarms turned out to have a legitimate cause, and each client got that answer with the evidence rather than a list of red alerts.

EmilyAI's automated defences updated firewall rules 95 times, updated dynamic blocklists 5,771 times and sent 1,390 abuse reports to the ISPs and hosting providers behind attacking machines. In September Emily held off an AI-generated attack running at 271 attempts a second for six hours.

In the same three months Emily completed 137 supplier reviews, proved 310 critical and high vulnerabilities fixed by re-scanning, and watched one client's internet-facing honeypot take more than four attacks a second, around the clock.

UK Cyber Defence
soc@cyber-defence.io
https://www.cyber-defence.io

The Officers Mess, Royston Road, Duxford, Cambridge, CB22 4QH

Cyber Defence

The quarter at a glance

The figures in this paper come from Pulse, the portal our SOC runs on, and from EmilyAI's own records of the actions it took. They cover August to October 2026. No client is named: clients appear only by sector, for example "a UK Financial Service Firm".

What	Figure	What it means for you
Client organisations	21 active, in the UK and Europe	Banking, pensions, insurance, legal, healthcare, logistics, transport, engineering, leisure, retail, gaming and technology
Endpoints monitored	47,619 in all, 1,616 of them under deep inspection across 12 organisations	Every endpoint is monitored; those under deep inspection are watched closely for anything suspicious
Security investigations and threat advisories	63, across 11 organisations	Every alarm is looked at, and each advisory is checked against the client's own systems
Priority 1 investigations picked up	4 of 4 within 4 minutes	The most serious alarms are picked up almost at once
Priority 2 investigations picked up	11 of 11 within the hour, 9 within 15 minutes	High-priority alarms never wait long
Investigations raised outside office hours	25 of 63 (40%), 7 at weekends	The SOC does not keep office hours, so you do not have to
Investigations closed within 24 hours	45 of the 62 closed	Most alarms have an answer by the next morning
Investigations first raised by Emily, our AI analyst	56 of 63 (89%)	Emily sweeps every client's data every minute and hands each finding to a human analyst
AI-generated attack	271 attempts a second for six hours, in September	11 automated responses updated the firewall, and the attack was successfully defended
Firewall rule updates	95	Blocks put in place by EmilyAI's automated defences, about one a day
Dynamic blocklist updates	5,771	More than 60 a day
Abuse reports sent to ISPs and hosting providers	1,390	Attacking machines reported to the networks that host them, about 15 a day
Supplier due-diligence reviews	182 requested, covering 175 suppliers; 137 complete	A quarter of the finished reviews took about half an hour
Vulnerabilities proved fixed by a follow-up scan	310 critical and high (111 critical, 199 high)	Emily scans, then scans again to prove that the fix worked
Attacks on one internet-facing honeypot	10.8 million in four weeks, from 37,124 addresses	What any server left open to the internet faces: more than four attempts every second

UK Cyber Defence
soc@cyber-defence.io
https://www.cyber-defence.io

The Officers Mess, Royston Road, Duxford, Cambridge, CB22 4QH

Monitoring and detection

The SOC opened 63 security investigations and threat advisories in the quarter, across 11 client organisations. 46 began with an alarm in a client's own data. The other 17 were threat advisories, where a newly published vulnerability was checked against the client's systems.

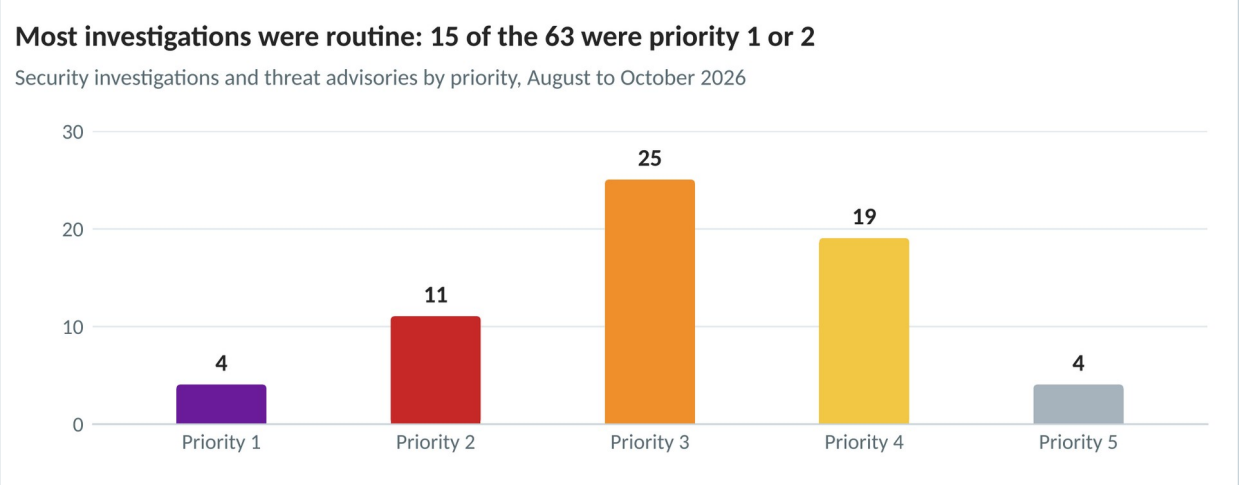


Figure 2. Security investigations and threat advisories by priority, August to October 2026. Priority 1 is the most urgent.

The urgent ones were picked up fast. All four priority 1 investigations were picked up within four minutes, and all 11 priority 2 investigations within the hour, nine of them within 15 minutes. Of the 62 investigations closed by 29 October, 45 were closed within 24 hours.

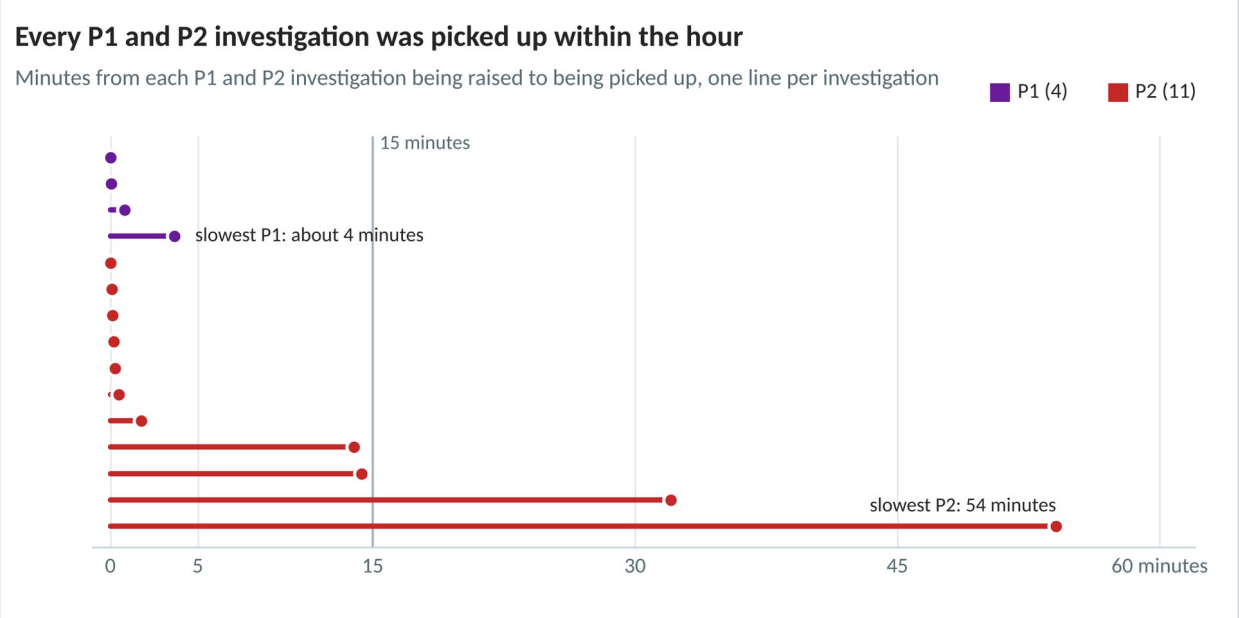


Figure 3. Time from each priority 1 and priority 2 investigation being raised to being picked up by the SOC.

UK Cyber Defence
soc@cyber-defence.io
https://www.cyber-defence.io

The Officers Mess, Royston Road, Duxford, Cambridge, CB22 4QH

What the alarms were. The quarter's alarms covered:

- changes to privileged accounts in Microsoft 365 and Entra ID;
- suspected credential theft from a domain controller;
- password spraying against a VPN;
- malware and hacking tools caught by Microsoft Defender;
- a stolen laptop;
- unexpected new accounts;
- penetration testers probing a decoy system.

Most alarms are not attacks. By our reading of the SOC's closing notes, around three in four investigations ended with a confirmed, legitimate explanation: an administrator's change, a policy update, a scheduled maintenance task, or a penetration test the client had commissioned. In each case the client got that answer with the evidence. The real threats included a password spray, a stolen laptop, hacking tools and an unexpected account. Each one was contained, was shown to have failed, or went to the client with the evidence needed to act.

Around the clock

25 of the 63 investigations (40%) began outside UK office hours, seven of them at weekends. Fifteen were raised between 6am and 8am, as Emily's early sweeps and morning threat hunt reported what had happened overnight, so the client's working day started with an answer rather than a question.

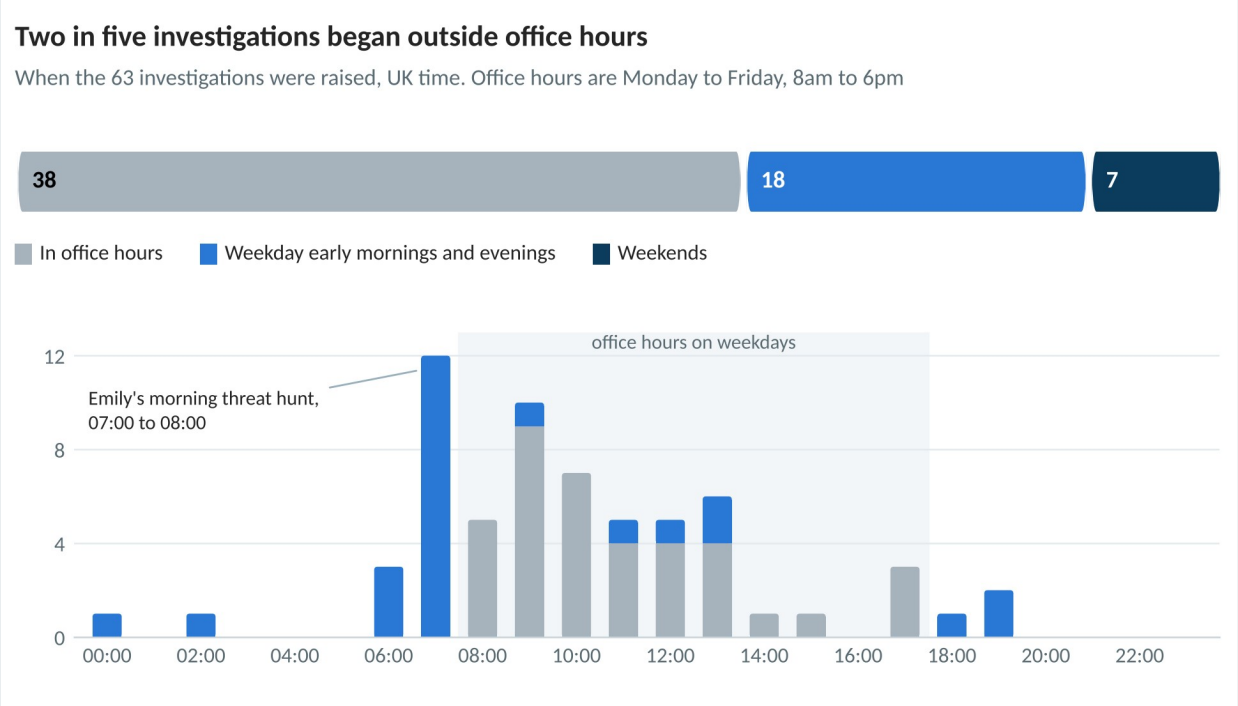


Figure 4. When the 63 investigations were raised, in UK time. The upper bar splits them into office hours, weekday early mornings and evenings, and weekends; the columns show the hour of day.

Overnight, urgent findings page an analyst. Lower-priority findings wait as tickets for the morning, so nobody is woken for something that can wait.

Month by month

October was the busiest month, with 22 security investigations against 13 in August and 11 in September, and 36 client requests, which include maintenance, scans and certification work. Threat advisories ran at nine in August, six in September and two in October.

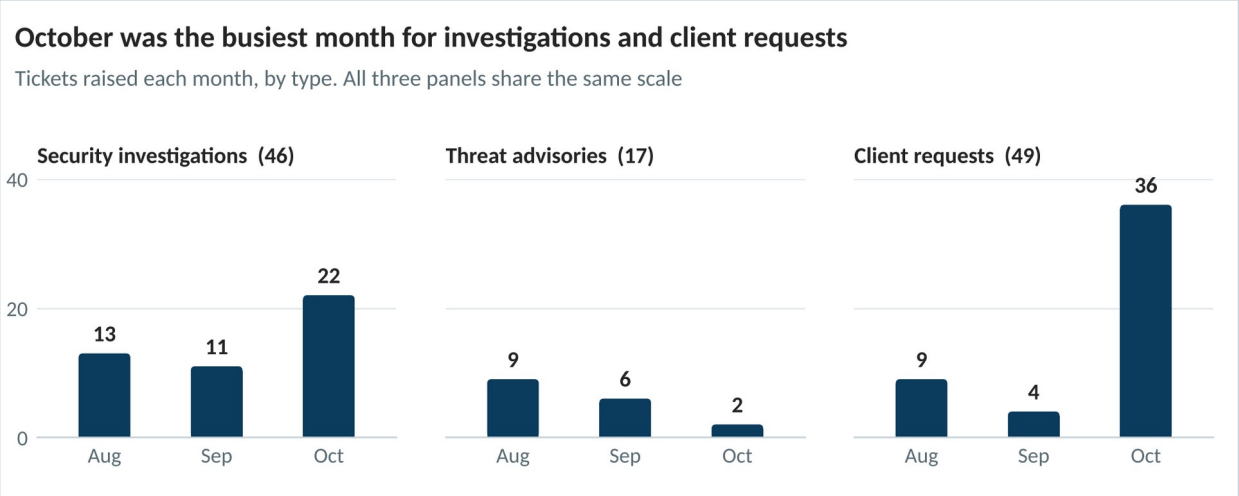


Figure 5. Security investigations, threat advisories and client requests raised each month. The three panels share one scale.

UK Cyber Defence
soc@cyber-defence.io
https://www.cyber-defence.io

The Officers Mess, Royston Road, Duxford, Cambridge, CB22 4QH

Defend and disrupt: EmilyAI's automated defences

Not every attack needs a person to decide what to do. When an attack is clear-cut, EmilyAI's automated defences block it at the firewall and on dynamic blocklists, and report the attacking machine to the ISP or hosting provider responsible for it. People stay in charge of everything that needs judgement.

An attack generated by AI, defended by EmilyAI

In September, one client came under an attack generated by AI. It ran at 271 attempts a second and kept up that rate for six hours: about 5.9 million attempts in all. EmilyAI made 11 automated responses, each one updating the firewall to block the attack. The attack was successfully defended.

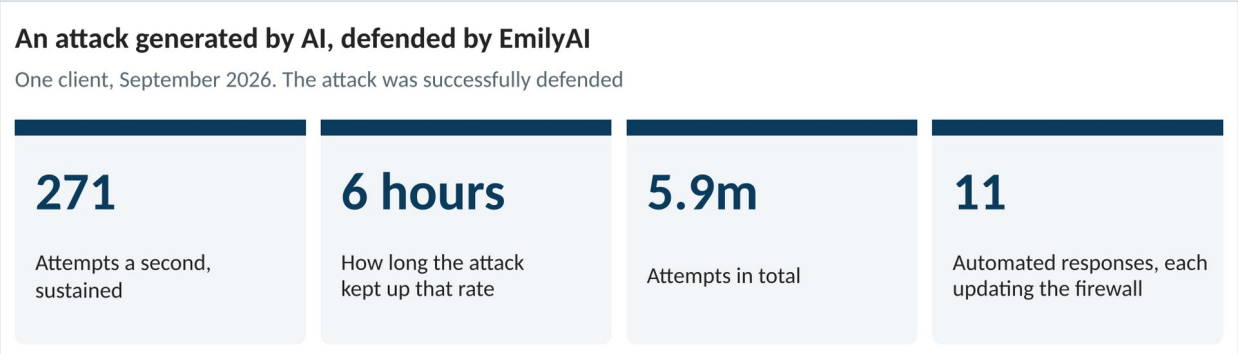


Figure 6. The AI-generated attack on one client in September 2026, and EmilyAI's automated response.

An attack written by a machine moves at machine speed, so the defence has to move at machine speed too, with people watching over it.

Every day, automatically

Most of EmilyAI's defensive work is quieter, and it happens every day. Across the quarter its automated defences updated firewall rules 95 times, about once a day, and updated dynamic blocklists 5,771 times, more than 60 a day.

Blocking protects our clients. Reporting goes further: EmilyAI sent 1,390 abuse reports to the ISPs and hosting providers behind attacking machines, about 15 a day, giving each provider the evidence it needs to take the machine off the internet for everyone. September, the month of the AI-generated attack, was the busiest month for all three. During this same period, EmilyAI, via The Hive, updated 76 central blocklists which cascaded over 10,000 malicious IP and domain updates.

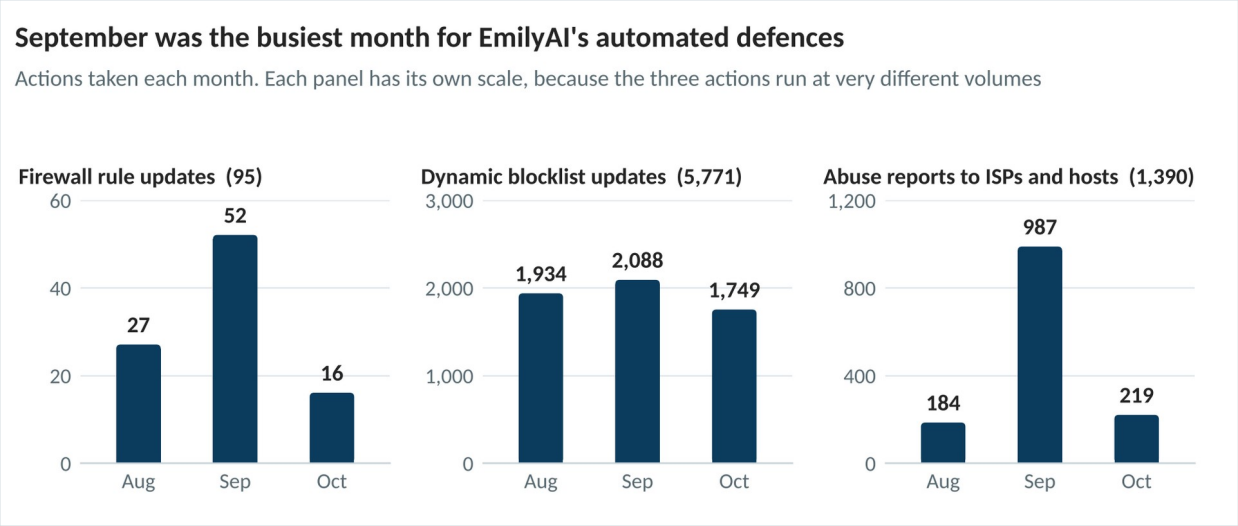


Figure 7. Firewall rule updates, dynamic blocklist updates and abuse reports sent to ISPs and hosting providers by EmilyAI's automated defences, by month. Each panel has its own scale.

Cyber Defence

Stories from the quarter

These eight short stories are anonymised: they name no clients, people or systems. Each one ended the way a good SOC engagement should, with a calm morning and a clear answer.

The penetration test that met the SOC

A UK Financial Services Firm, October. The firm commissioned a two-week penetration test, and the SOC picked up the testers at every stage:

- a machine nobody had seen before, scanning the network;
- EmilyAI creates a dynamic honeypot, the testers wandering into it;
- new administrator accounts and changes to multi-factor sign-in;
- an attempt to copy every password hash from a domain controller.

Each alarm was checked with the client by phone, two of them within half an hour, and the testers were left to finish undisturbed. A penetration test tells you whether an attacker could get in. A SOC tells you whether you would know.

64,000 failed logins, no way in

A Global engineering organisation, September. Overnight, the SOC spotted a password-spraying campaign against the remote-access VPN: 64,624 failed attempts in 24 hours, against 110 usernames, from 69 rotating addresses, with forged device details. The analysis showed the client's own VPN controls were quietly turning away unknown users, and no login succeeded. By the next morning the client had the full picture, and advice on a related vulnerability in the same equipment.

A ransomware alarm at 7am, answered by breakfast

A UK healthcare provider, October. A rule linked to Blackbit ransomware fired 20 times on one workstation just after 7am. Within about 60 seconds Emily had traced it to a single Defender policy update pushed by the client's own IT team. The client confirmed it, and the ticket was closed before the working day began.

A stolen laptop, watched until it was safe

A UK pension fund, October. After a staff laptop was stolen overnight, Emily watched for the device and its user's account to reappear. The audit logs showed the password had been reset and old sign-in tokens revoked, and the SOC followed the replacement laptop as it joined the network.

A hacking tool on one desktop, and only one

A financial services firm, August. Late on a Saturday afternoon, Defender caught a Windows licence-cracking tool on a single workstation. Within the hour Emily completed an automomous Threat Hunt and had shown it was on no other machine, with no sign of an intrusion. The client was told what to do next: confirm the removal, then rebuild the machine.

The Tor alarm that wasn't

A private bank, September. On a Sunday morning, a rule built to spot the Tor anonymity browser fired on the bank's laptops. By late morning the SOC had proved the rule was catching two Microsoft programs whose names happen to contain "tor". The SOC told the bank, then Emily rewrote the rule so it would not fire again.

UK Cyber Defence
soc@cyber-defence.io
https://www.cyber-defence.io

The Officers Mess, Royston Road, Duxford, Cambridge, CB22 4QH

An account nobody asked for

A construction and property consultancy, August. The morning threat hunt found a new local account created on a laptop by a remote-management script. By the evening the same account had appeared on 67 machines and had never been used to sign in. The client did not recognise it, and had the evidence the same day to take up with its IT provider.

Admin tool or attacker?

An insurance services firm, October. At 10am on a Monday, a remote-administration tool used by IT teams and attackers alike installed itself on one of the firm's machines. The SOC asked the client rather than guessing. It was planned maintenance, and the ticket was closed by early afternoon.

UK Cyber Defence
soc@cyber-defence.io
https://www.cyber-defence.io

The Officers Mess, Royston Road, Duxford, Cambridge, CB22 4QH

Supplier due diligence

Clients asked us to review 182 suppliers in September and October, 175 of them different companies. The service grew from 15 reviews in September to 167 in October.

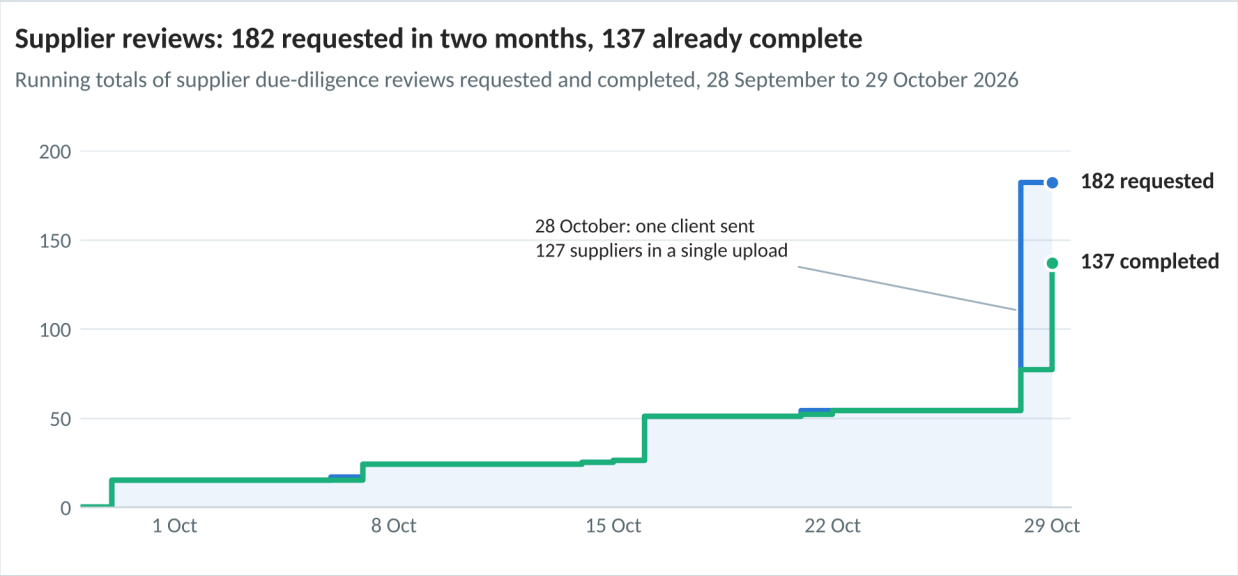


Figure 8. Running totals of supplier due-diligence reviews requested and completed, 28 September to 29 October 2026.

- **Speed.** By 29 October, 137 reviews were complete and 43 were in progress. A quarter of the finished reviews took about half an hour, and the median was about five hours.
- **Scale.** One engineering organisation sent 127 suppliers in a single upload on 28 October. 82 of those reviews were finished within two days.
- **The supply chain is changing.** The list ran from banks, telecoms carriers and cloud platforms to password managers, IT-disposal firms and air-conditioning contractors. It included three AI tools: note-taking, voice generation and AI-content detection. One logistics group asked about a consumer messaging app three times in two days.

Vulnerability and exposure management

We scan our clients' systems for vulnerabilities, then scan again to prove that each fix worked. In the quarter, follow-up scans proved 310 critical and high findings fixed: 111 critical and 199 high, alongside 269 medium. In all, 11,360 findings were confirmed fixed, most of them low-risk or informational.

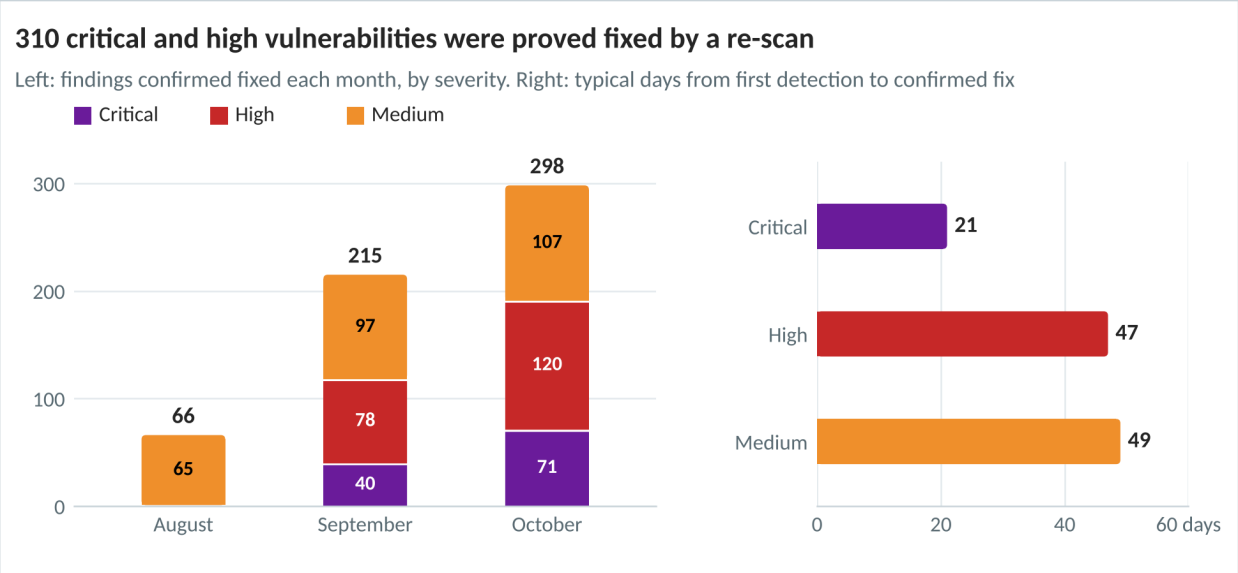


Figure 9. Critical, high and medium findings confirmed fixed by a follow-up scan each month (left), and the typical number of days from first detection to confirmed fix (right).

Critical findings are fixed first. Critical findings were typically fixed within about three weeks of first detection, in less than half the time taken for high and medium findings. That is what prioritisation should look like.

Threat advisories matched to each client. When a serious new vulnerability is published, the SOC checks whether the client actually runs the affected product, and tells them if so. This produced 17 advisories in the quarter. Among them:

- a print-management server exploit on the US government's list of actively exploited vulnerabilities, at two clients;
- a critical flaw in Windows certificate services, scheduled into the client's next patching run;
- serious flaws in network switches, a website content system and firewall management;
- 11 critical WordPress plugin flaws in one week, including a supply-chain compromise;
- a missing email-spoofing protection (DMARC) on a firm's domain.

Advisories typically went out within about a week of publication, through a weekly review. One was raised two days before the US government's own deadline for fixing the flaw.

Deception and honeypots

EmilyAI manages two permanent and the dynamic ability to bring up 30 more decoy systems, or honeypots, for one client: one on the internet and one inside its network. A decoy does no real work, so everything that touches it is unwanted by definition.

In the four weeks from 27 September to 24 October 2026, the internet-facing decoy recorded 10,782,613 attacks from 37,124 different addresses. That is about 385,000 a day, or more than four every second, day and night. The busiest day was 12 October, with 1,154,942.

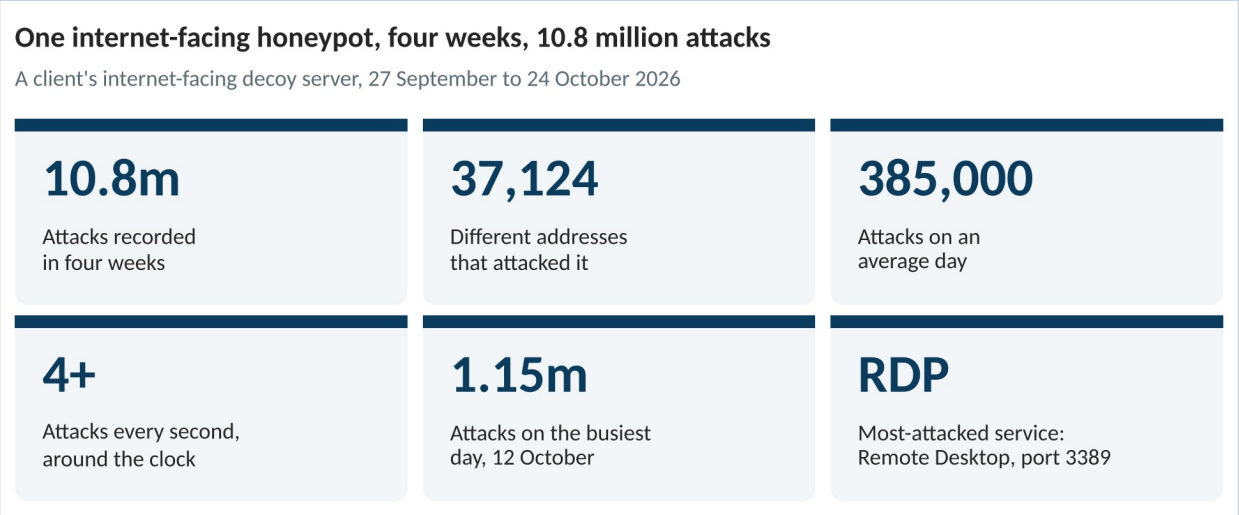


Figure 10. Attacks recorded by one client's internet-facing honeypot, 27 September to 24 October 2026.

The most-attacked services were Remote Desktop (RDP), internet telephony (SIP) and remote screen sharing (VNC): the services most often left open to the internet by accident. Most attacks came from machines hosted in the Netherlands, the United States, Ukraine, France and Bulgaria. That is where the attacking machine is hosted, often a rented server or a compromised home router, not where the attacker lives.

None of this is cause for alarm. It is the background weather of the internet, and it is why the basics matter: keep remote access off the open internet, put multi-factor sign-in in front of it, and have someone watching who knows the difference between weather and a storm. The SOC checks the most persistent addresses against the client's real systems. In this period only one of the top ten had touched them, and the client's firewall closed those connections.

The decoy inside the network did its job during the client's October penetration test: the testers found it, probed it and logged in. Nothing legitimate should ever connect to an internal decoy, so any connection to it is worth an immediate look. In October two clients asked for more decoy devices.

Cyber Defence

EmilyAI and the human analysts

Our SOC pairs EmilyAI, which never sleeps, with human analysts who make the decisions.

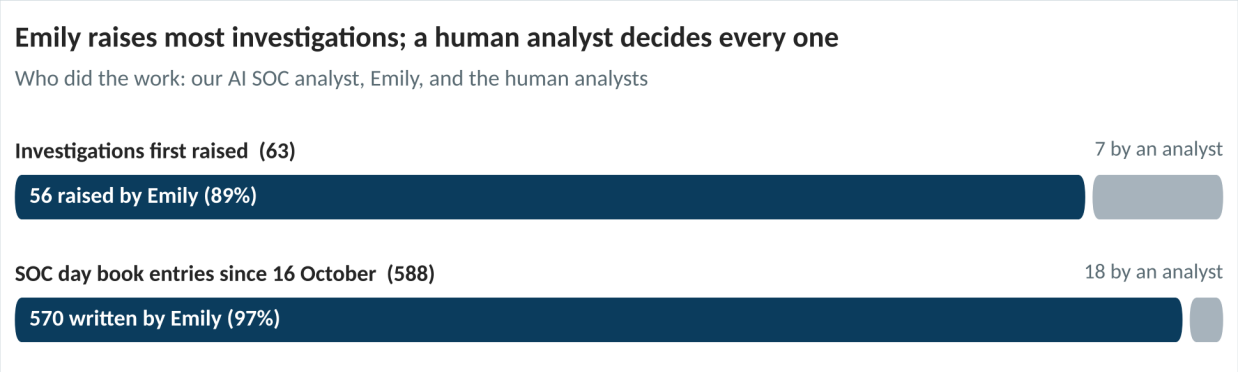


Figure 11. Who first raised the quarter's 63 investigations, and who wrote the SOC day book entries since it began on 16 October 2026.

- **Emily sweeps every client's data every hour** and runs a structured threat hunt each morning. She first raised 56 of the quarter's 63 investigations, and 136 of all 379 tickets.
- **She keeps the record.** Since the SOC day book began on 16 October she has written 570 of its 588 entries, about 40 a day.
- **Clear-cut attacks are blocked automatically; judgement calls go to people.** EmilyAI's automated defences block clear-cut attacks at the firewall and on blocklists, and report them to the providers that host them. In investigations, Emily raises, measures, explains and recommends, but she never contains a machine or locks an account herself. A human analyst decides, and calls the client when a decision needs their knowledge.
- **The human side.** When an alarm might have had an innocent cause, an analyst checked it with the client before closing it. The analysts also fixed the detection rules that produced false alarms, so the same false alarm does not recur.

UK Cyber Defence
soc@cyber-defence.io
https://www.cyber-defence.io

The Officers Mess, Royston Road, Duxford, Cambridge, CB22 4QH

Cyber Defence

How we measured

1. **Period and source.** 1 August to 29 October 2026, from the records in Pulse, read on 29 October 2026, unless stated otherwise below.
2. **What is left out.** Our demonstration and internal systems, one client account, test tickets, and the internal tickets raised when a client's data feed went quiet are not counted.
3. **Picked up.** The time from a ticket being raised to it being acknowledged in Pulse by an analyst or by Emily. It is not the time from an event to its detection.
4. **Office hours.** Monday to Friday, 8am to 6pm, UK time.
5. **Three in four.** This comes from reading the closing notes of each investigation, so it is approximate. Five alarms were triggered by our own vulnerability scanning: they are counted, because each had to be checked, but none is used as a story.
6. **Proved fixed.** A finding is proved fixed when a later scan of the same system no longer finds it. "Typical" means the median. Findings whose recorded dates were inconsistent are left out of the typical-days figures.
7. **Endpoints.** 47,619 is the total number of endpoints the SOC monitors, as at 30 October 2026. The 1,616 under deep inspection are those that reported to the SOC in the seven days to 29 October 2026.
8. **EmilyAI's automated defences.** The firewall rule updates, dynamic blocklist updates, abuse reports and the September attack come from EmilyAI's own records of the actions it took, by calendar month.
9. **Honeypot.** Counts come from the honeypot's own dashboard for 27 September to 24 October 2026; its records begin on 27 September. They count attacks on the decoy services and leave out the honeypot's network sensors (Suricata, P0f and Fatt), which record the same connections again.

UK Cyber Defence
soc@cyber-defence.io
https://www.cyber-defence.io

The Officers Mess, Royston Road, Duxford, Cambridge, CB22 4QH

Cyber Defence

About UK Cyber Defence

UK Cyber Defence runs a security operations centre for organisations in the UK and Gibraltar, from banks, pension funds and insurers to healthcare providers, logistics groups and gaming companies. Our analysts work alongside EmilyAI, the AI we have run in our SOC since April 2018, and use Pulse, our own SOC portal, to watch clients' systems around the clock, check every alarm, block and report attackers, manage vulnerabilities, review suppliers and run decoy systems.

To find out what our SOC would see in your organisation, email **soc@cyber-defence.io** or visit **www.cyber-defence.io**.

UK Cyber Defence
soc@cyber-defence.io
https://www.cyber-defence.io

The Officers Mess, Royston Road, Duxford, Cambridge, CB22 4QH