Cyber Defence

The Cyber Defence Eco-System

The SOC at the core, the modules that extend it, and EmilyAI on her own

Everything UK Cyber Defence sells is, in the end, one thing: a Security Operations Centre. The modules set out in this document are not separate products bolted to the side of it. Each one extends the reach of the same SOC into a part of an estate it could not otherwise see, and each returns its findings to the same analysts and the same reporting. The core gives good visibility on its own; every block added above it widens the field of view and sharpens what is already in it. The diagram that follows shows how they stack. Emily herself can also be bought on her own, without the subscription, and a later section sets out exactly what changes if you do.

What a client is actually buying is a quiet morning. Not the absence of threat, which nobody can sell, but the confidence that comes from knowing the night has already been looked at by someone whose only job was to look at it, and that anything which mattered has a name, a ticket and a next step waiting. The eco-system exists to make that morning reliable, and to keep it reliable as the estate grows.

It is worth saying plainly what this is not. It is not a collection of point products with a dashboard laid over the top. Every block in the diagram overleaf writes into the same store, is read by the same analyst, and appears in the same report. That is the whole of the design, and it is why adding a module makes the existing picture clearer rather than simply adding one more screen that somebody has to remember to check.

The core

At the centre sits the SOC itself, and the SOC is two things working as one.

The first is EmilyAI. Emily is an AI SOC analyst, begun in 2014 and in live service since April 2018. She reads all client data from Graylog, our SIEM environment, and she works the way a competent human analyst works: she forms a view of what an event is, and she writes that view down as a ticket.

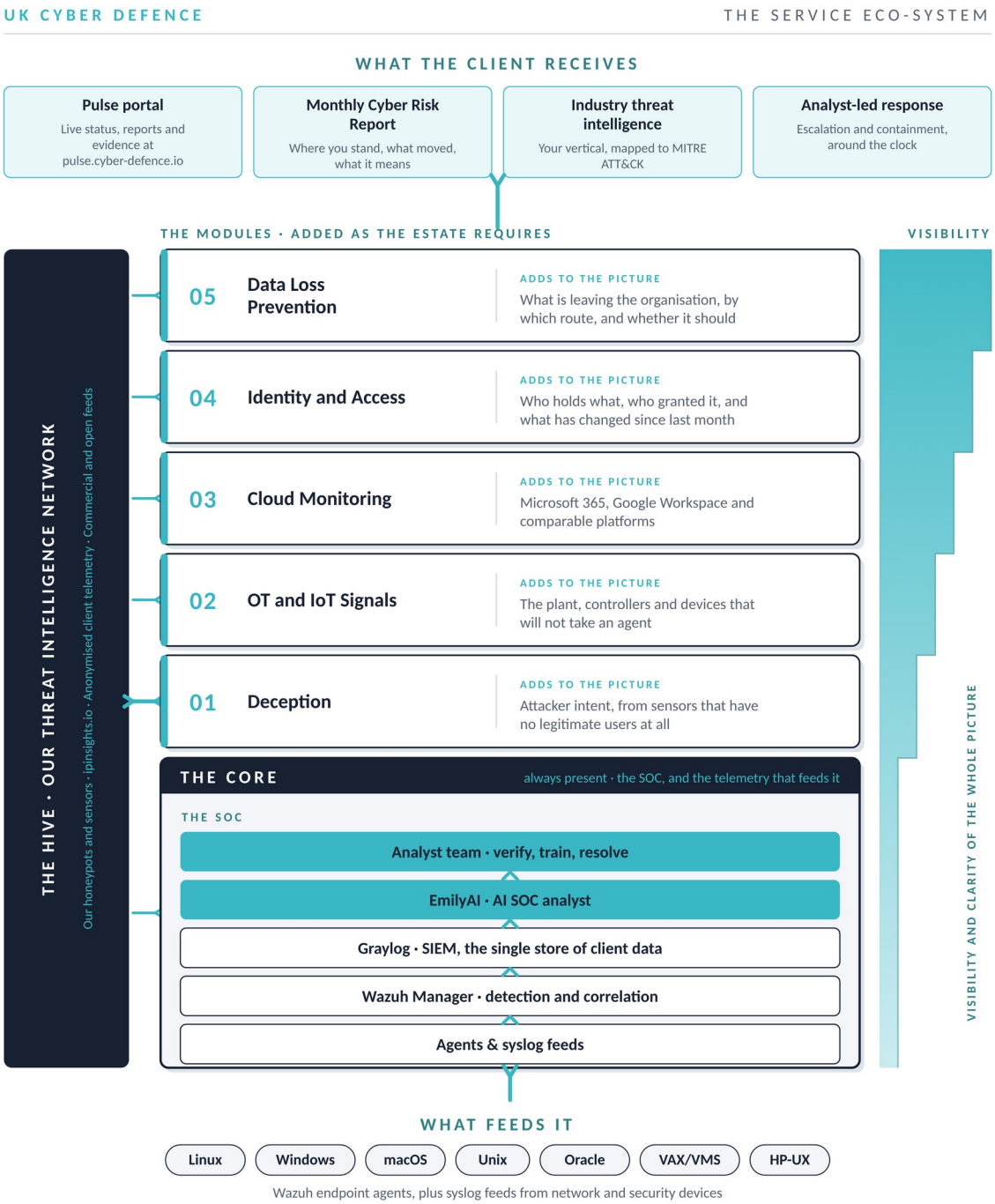
The second is a small team of genuinely talented engineers. They handle everything Emily cannot, and they do something more consequential than that — they watch her. They check her assertions, correct her where she is wrong, and keep her trained. An AI analyst nobody audits is a liability. An AI analyst audited continuously is leverage, and the team is what turns one into the other.

Beneath the SOC sits the telemetry that feeds it. Graylog is the single store of client data. Graylog is fed by the Wazuh Manager, which performs detection and correlation, and the Wazuh Manager is fed from two directions: syslog feeds from anything on the network that emits them, and Wazuh endpoint agents deployed across Linux, Windows, macOS, Unix, Oracle, VAX/VMS and HP-UX. That last list is not decoration. A great deal of what actually runs a business runs on platforms modern tooling has quietly stopped supporting, and we have not.

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

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

Cyber Defence



The eco-system as a stack. The core is the foundation and is always present. The five modules are added as the estate requires. The Hive runs the length of it, feeding every layer and fed in turn by the client's own deception devices, which is why that arrow runs both ways. The staircase on the right is the point of the whole diagram: visibility and clarity of the client's position grow with every block added.

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

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

Cyber Defence

The modules

Five modules extend the core. Each is a block laid on the same foundation, each is optional, and each adds a dimension of the picture that the layers beneath it cannot supply. They are numbered here in the order they are usually discussed, which is roughly the order in which they earn their keep.

01 Deception

The deception module is normally supplied as a pair of dynamic honeypots. One runs inside the client network and is purely dynamic: Emily spins honeypots up in response to activity she is already seeing, so the deception adapts to the attacker rather than waiting in a fixed position. The other runs externally, on an IP address we own, presented under a DNS record the client owns, so that to anyone probing the estate it appears to be part of it. The external device is always on, always listening, and runs thirty-seven different types of honeypot.

Deception is the cheapest high-fidelity signal in security. A honeypot has no legitimate users, so there is nothing to argue about: anything that touches it is, by definition, worth looking at. For most clients it is the module that changes the quality of the morning report fastest.

02 OT and IoT Signals

The second module is a dedicated appliance that sits inside the client network, gathers logs locally, processes them securely and returns signals intelligence to our environment. It exists because industrial control systems and connected devices rarely tolerate an agent, and frequently cannot have their data shipped off-site wholesale. The appliance does the work where the data lives and sends out only what is needed. It is the usual answer for IoT and ICS estates.

03 Cloud Monitoring

The third module extends monitoring into the cloud services where most work now happens — Microsoft 365, Google Workspace and comparable platforms. Sign-in activity, administrative change and data movement in those tenants become part of the same picture as everything else, rather than a separate console somebody has to remember to check.

04 Identity and Access

The fourth module is a dedicated identity and access capability, enabled for reporting. Identity has become the perimeter, and the useful questions about it are largely historical rather than instantaneous: who holds what, who granted it, what has changed since last month, and which accounts have quietly accumulated rights nobody intended them to have.

05 Data Loss Prevention

The fifth module covers data loss prevention: what is leaving, by which route, and whether it should be. It is reported in the same place and by the same analysts as everything else, which is the point.

The Hive

Running the length of the stack, feeding every layer of it, is the Hive, our threat intelligence network. It draws on four sources: the honeypots and sensors we run ourselves; ipinsights.io, our open threat intelligence project; anonymised telemetry from across the client base; and commercial and open

feeds. What it produces flows continuously back into the core, so that Emily and the analysts are never reasoning about one estate in isolation.

The part worth dwelling on is the loop. A client's own deception devices feed the Hive, and the Hive feeds every client. An attacker who probes one estate has, in the act of probing it, told us something we can use to defend all of them. The eco-system therefore improves as more of it is deployed — an unusual property for a security service, and the reason deception is the module we tend to recommend first.

What the client receives

Day to day, the output of the eco-system arrives in four ways. Pulse, our client portal at pulse.cyber-defence.io, carries live status, reports and supporting evidence. A monthly Cyber Risk Report sets out where the organisation stands, what has moved and what that means. Industry threat intelligence, specific to the client's vertical and mapped to MITRE ATT&CK, puts that position in context. And when something needs a person rather than a report, an analyst escalates it with containment guidance, around the clock.

EmilyAI on her own

EmilyAI can be bought without the subscription, and for some organisations that is the right answer. If you already run a SOC — if you have a SIEM you are happy with, a SOAR, and analysts on shift — then what you are short of is capacity, and capacity is precisely what Emily is. She is licensed to you, runs on your own infrastructure, reads from your SIEM, and writes her tickets into your own case management. We keep her tuned and we keep her current. You keep the rest.

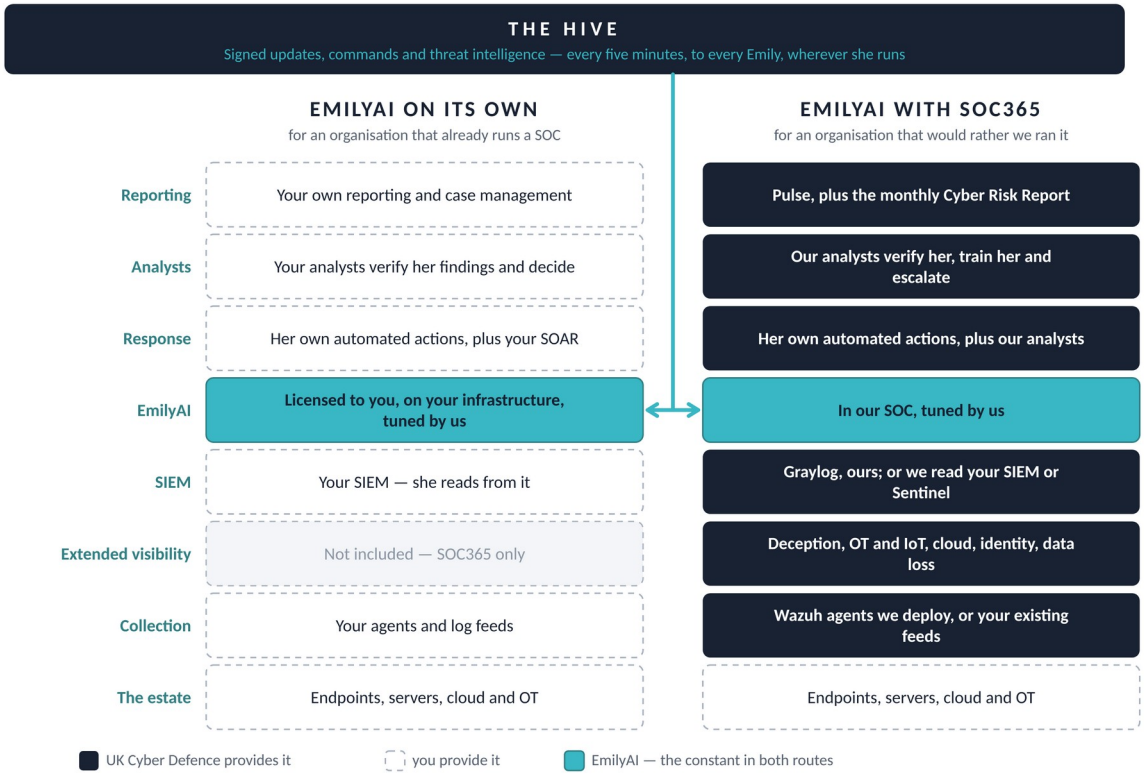
What does not change between the two routes is the Hive. Every Emily, wherever she runs, calls the Hive every five minutes and takes down cryptographically signed updates, commands and threat intelligence. She does not sit on a shelf going stale. A standalone Emily is as current as the one working inside our own SOC, and that is the single most important thing to understand about buying her on her own.

What does change is everything around her. The diagram overleaf sets the boundary out plainly. On the standalone route you supply the collection, the SIEM, the wider response orchestration, the analysts who check her findings, and the reporting. On the subscription route we supply all of it, and the five modules become available, because each of them depends on infrastructure we run.

Neither route is a lesser version of the other. The question is only whether you already own a SOC, or would rather not have to.

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

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



The same Emily on both routes. What differs is who supplies everything around her. The Hive sits above both because it serves both.

Where it usually starts

Which route to take is usually settled within a conversation. An organisation with a staffed SOC and a SIEM it trusts takes Emily on her own. An organisation without one, or with one it has tired of running, takes the subscription. A third group starts with Emily on their own infrastructure and moves to the subscription later, once the cost of keeping analysts on shift has made its own argument. Nothing is wasted in that move: it is the same Emily and the same Hive throughout.

On the subscription route, most clients begin with the core alone, because the core is the service and everything else is an extension of it. Once telemetry is flowing and the first month's report has landed, the sensible next step is deception, for the reason given above: it produces the highest-quality signal for the lowest effort, and it is the module that contributes back to the Hive as well as drawing from it.

After that, the estate dictates the order rather than we do. OT and IoT signals where there is plant, or plant-like equipment, that will not take an agent. Cloud monitoring where the work has moved to Microsoft 365 or Google Workspace. Identity and access where the organisation has grown faster than its joiners and leavers process. Data loss prevention where what leaves matters as much as what arrives. There is no obligation to take any of them, and no penalty for adding one later.

Taken together the proposition is modest to state and difficult to deliver: that someone competent has already looked, that whatever mattered has a name and a next step, and that the morning belongs to the client rather than to the estate.

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

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