Datasheet

Managed Services Component: Endpoint Detection and Response – Crowdstrike

It's not just malware anymore. Determined threat actors and APTs are sophisticated and resourceful in their efforts to evade and breach your cyber security defences – and then stay there.

Credential theft, system, software and hardware exploits, all combined into malicious toolsets that leverage the shells, command lines, and applications that are fundamental parts of the operating systems of your assets. Malware, ransomware, on disk, on memory...the list goes on.

The proliferation of endpoint threats across your security landscape only increases the risks to which your infrastructure is exposed.

Risks that you need to control in a way that's reliable and effective, driven by intelligence and expertise – and without the burden of managing the
complex systems needed to deliver that control.

Adarma can help.

Adarma's Endpoint Detection and Response Managed Service

Adarma was founded to make the world a safer place to do business, and our managed service products are designed to assure our customers of the best possible cyber defence.   We offer an unprecedented level of partnership and transparency.

Our analysts are cyber security professionals with combined decades of experience in SOC management and operations. Our SOAR capabilities make us fast and efficient in incident correlation and triage, IOC enrichment, and reporting.

Our VM and threat intelligence platform keeps customers informed of threats to their assets and security landscape as they emerge - and our analysts alert to detect them.

Adarma and Falcon Crowdstrike

Our Endpoint Detection and Response (EDR) service is supported by these capabilities.

Adarma uses Falcon Crowdstrike, a cloud-based, EDR platform to assist in rapidly and accurately identifying threats such as malware or APTs that infest your endpoints.

We chose it because of its lightweight client, speed of operation, and unique modelling of adversarial activity that's closely aligned with our own methodologies. Rather than relying on artefacts found in the wake of a breach or breach phase, Falcon Crowdstrike can detect Indicators of Attack in real time.

Combining our analysts' expertise with Falcon Crowdstrike's best features, we provide you a rapid and accurate alerting of endpoint threats. Our service
identifies, contextualises, and tracks vulnerabilities across the endpoints in your estate to give you the confidence to make the decisions that keep your risks under control.

Beginning with a physical or virtual interactive workshop, we'll develop our understanding of your business and your needs, ensuring we translate them effectively into outcomes. Then we get down to delivery – installing, onboarding and configuring Crowdstrike Falcon in your environment as determined by best practice.

And when you're ready delve deeper into other Crowdstrike Falcon – whether that's tighter integration with your existing SIEM and SOC solutions, more complex intelligence analysis, or extending your current solution's capabilities via Falcon's API - our team is ready to help.

Datasheet

Managed Services Component: Endpoint Detection and Response – Crowdstrike

Crowdstrike Falcon Key Features

Cloud-based architecture, daily aggregation of endpoint events from millions of sensors deployed globally (analysed by powerful ML techniques), all deployed via a lightweight endpoint client allow you to prioritise, respond, and remediate with confidence. Integrations with other services via easy to use API are possible.

Intelligence Visibility: Crowdstrike.io continuously captures activity on endpoints, giving a clear view of threats in a range from single endpoint to organisational-wide threat level, enhancing your situational awareness.

Facing the Unknown: Threat information is shared and updates the intelligence and detection capabilities. Unknown threats are detected through a series of methods including IOA, Machine Learning, white lists and blacklists.

Speed/Footprint: The client is lightweight and low impact, and functional without an internet connection. The quick search function returns results in five seconds or less.

Adarma's Delivery Team

- **Qualified, experienced engineers** with a background in cyber security and a specialisation in Crowdstrike Falcon.
- **Experienced in all aspects of** Crowdstrike Falcon installation, configuration, and development. We understand its context and capabilities as a tool in your security arsenal.
- **Immersed in the wider threat landscape** - we know threats proliferate rapidly and unpredictably. Staying aware of the big picture helps us help you target and prioritise the most critical vulnerabilities.
- **Multi-tiered team** with established escalation paths and procedures for improved incident response
- **Eyes on glass 24/7** - supporting you around the clock.

Why Adarma?

- **We've got the expertise you need** to successfully build and integrate end-to-end solutions and deliver value to your organisation.
- **We understand the design and purpose** of the platforms Crowdstrike monitors and integrates with – we speak your SMEs language because we're natives.
- **We partner with best of breed solutions** to deliver world class services.
- **We deliver value through the service** we implement and deliver.

About Adarma

We're one of the largest independent security services companies in the UK. As a business formed and run by experienced senior security leaders, we know security and how to deliver real value in the real world. This is why our clients are successful FTSE 350 organisations from all industry sectors.

Adarma delivers innovative tailored solutions for some of the world's biggest companies. Our teams are a diverse group of technical experts and consultants, all with the same objective and united by the same goal: to help our clients prepare for attack and stand side-by-side with them when it happens.

Helping make the world a safer place.

Contact us to discuss your Managed Service or EDR requirements enquiries@adarma.com

www.adarma.com

ADARMA