Precursor

Innovative cyber risk management

MDR Service Definition v0.2

20242025

Assured Service Provider
in association with
National Cyber Security Centre

CREST

www.precursorsecurity.com

Introduction

Company Overview

Precursor Security is a UK based cyber-risk management services provider. We deliver a blended approach to security services integrating both defensive and offensive capability giving us a unique edge in full-suite security. We deliver managed SOC services, incident response services and consultancy to a diverse customer base while also operating with our sister company to deliver CREST acreddited penetration testing and offensive capability. This partnership gives our analysts and penetration testers an itterative and competative environment which drives inovation on both fronts.

Our mission is to reduce cyber-risk exposure for our customers by delivering innovative services and products which combine best in class tooling with years of operational experience.

We have a diverse customer base across the UK including SME's, Insurance Partners and Enterprise customers who place their trust in us to protect their buissnesses and livelihoods.

Our UK-Based Precursor Security Operations Center (SOC) delivers our Precursor Managed Detection & Response (MDR) service, around the clock, every day of the year. This service resides entirely on UK shores and ensures that organisations are protected .

Solution overview

MDR is Precursors leading managed SOC service, consisting of Three service tiers each tailored towards specific phases of an organisations lifetime. MDR is vendor-agnostic, allowing organisations to bring their own security controls for our elite 24x7 team to monitor. This lets organisations unlock unrealised value from their existing suite of security controls. For organisations without any existing security tooling, Precursor can offer security solutions via our carefully selected existing technology partners, each chosen purely for their best-in-class capability such as CrowdStrike Endpoint Protection.

MDR is tailored to your organisation and offers the following key components:

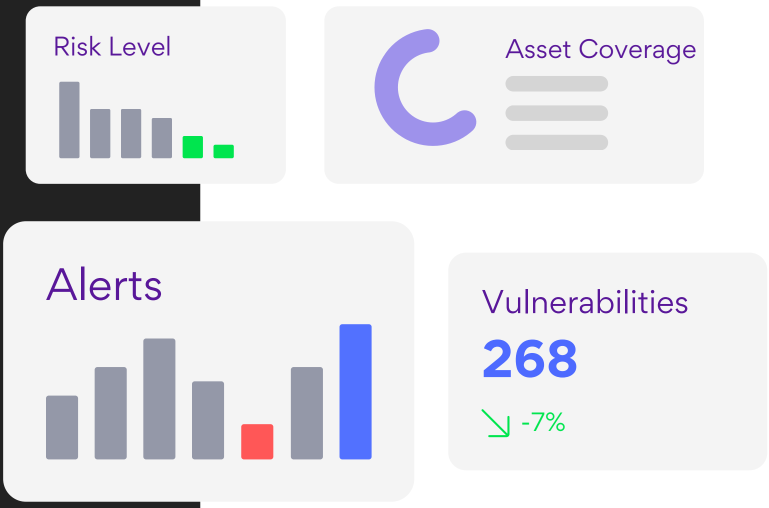
- Endpoint Detection & Response (EDR)
- Security Information & Event Management (SIEM)
- Managed Vulnerability Scanning Service
- Attack Surface Management
- Cloud Security Posture Management
- CREST Certified Penetration Testing

Utilising your technology, MDR monitors your IT estate for anomalies and threats utilising EDR and SIEM. We provide full visibility into each layer of your technology, across Identity, Network, Cloud, Endpoint and Data

Unlike traditional detection and response capability, Precursor takes a proactive approach to security. Our focus on active threat hunting means that our team can detect attackers early in the attack lifecycle, long before they cause an impact or trigger alerts. By performing continual monitoring of your assets from both a defensive and offensive perspective we are able to gain a complete picture of your environment through an attackers eyes. This allows us to maintain control of highly dynamic environments and provide focus to areas with high probability of attack while remediation takes place.

Features

Security Operations Centre (SOC) 24x7 – 365 days per year



Customer Portal

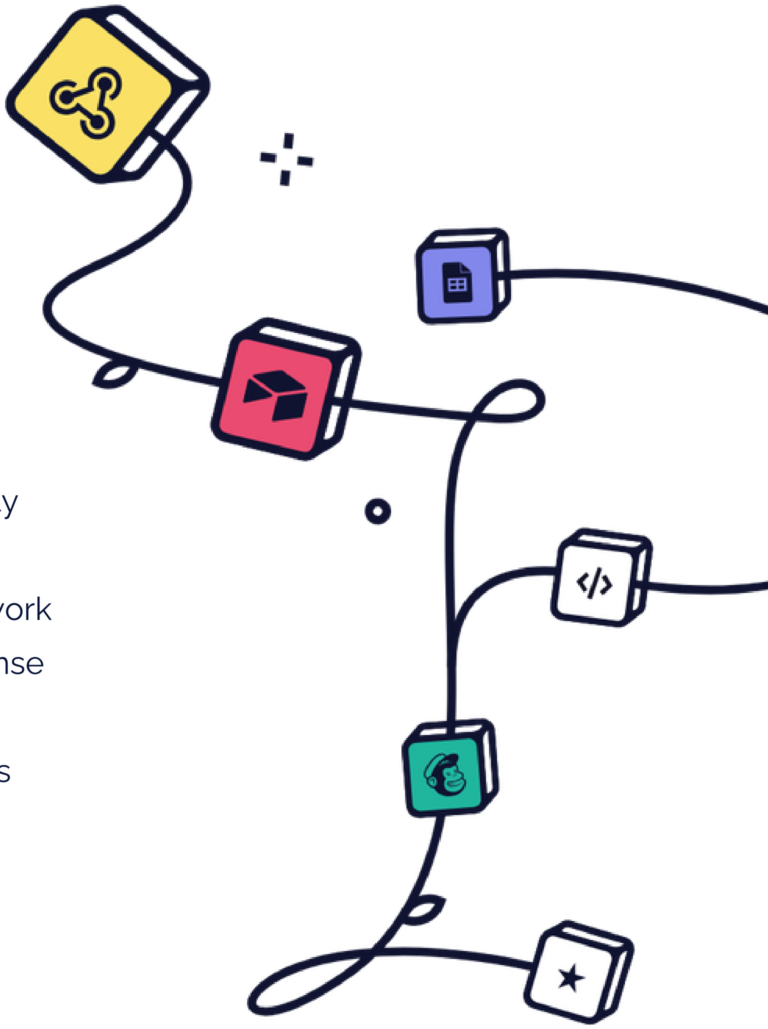
Providing customers with a tangiable and transparent view of the service gives real-time insights into SOC performance. Our custom real-time dashboards allow visibility of core SOC metrics, including but not limited to:

- Alerts across your estate
- Investigation insights
- Incidents triggered
- Monitoring coverage
- Project tracking

Features

Integrations for any EDR/XDR

We are one of the only providers who are 100% vendor agnostic. Our MDR platform can easily integrate your existing EDR, XDR, or any other technologies that require security monitoring.



Automation & Orchestration

Our MDR platform offers full Security Orchestration, Automation and Response (SOAR) capabilities. We work with you to refine automated response playbooks, driving down the time to respond and the impact of malicious activity.

Features

On Average

Assets Coverage

99%

Time to Investigate

10 minutes

Cutting-Edge Threat Intelligence

Our MDR service is integrated with strategic intelligence partners such as NCSC CiSP and other commercial partners, providing rapid and discrete intelligence about the threats likely to target your organisation. This tailored intelligence is integrated directly in your tenant.

Full Incident Response

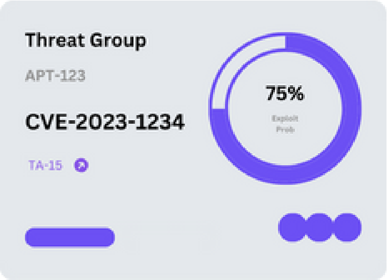
We recognise the need to quickly mobilise a team of specialists during a major security incident. MDR provides full incident response capabilities across the board including:

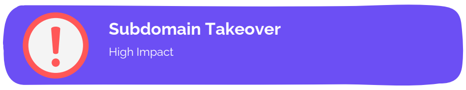
- Digital Forensics Investigation
- Threat Actor Negotiation
- Recovery

Features

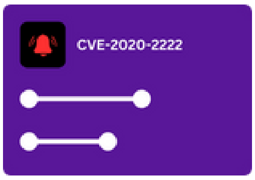
Proactive Threat Hunting

Our ability to activley hunt for threats and advanced attackers that exist outside of the visibility provided by normal tooling is what gives our service the edge. This capability allows us to identify and remove attackers early in the attack lifecycle well before any material impact has occurred.



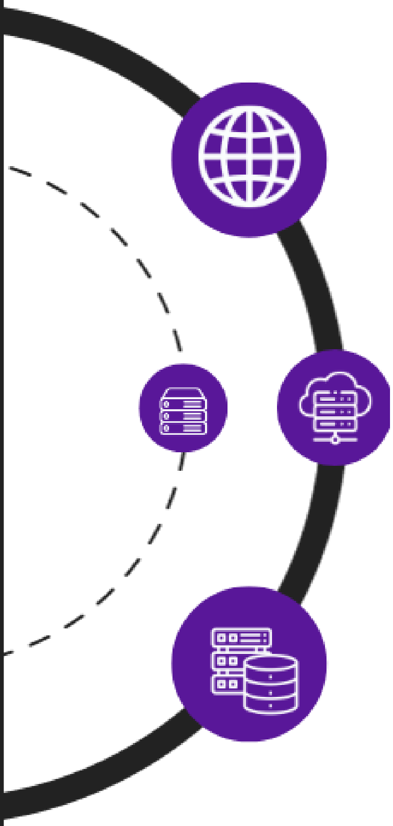


Attack Surface Management



Modern organisations have a fluid attack surface. Attack surface management offers oversight by providing continuous visibility into public facing assets, from discovery to vulnerability identification. It aids in identifying shadow IT, detecting domain configuration errors, highlighting public facing services, pinpointing technical vulnerabilities, and monitoring for potentially leaked user credentials.

Features



M365 & AD Monitoring

In modern networks the network-boarder is blured between on premise, SaaS and Cloud. Our team will monitor across your entire organisational footprint to ensure attackers are detected and stopped across any vector.

Cloud Posture Management (CSPM)

Although cloud adoption has grown rapidly in recent years many cloud environments enter production with insecure default settings and without adequate security hardening. We assess and monitor your cloud environment against industry recognised CIS security benchmarks to ensure that your environment does not present attackers with oppertunity.

Features

Cyber Essentials Certification

Precursor Security is an IASME approved cyber essentials certification body and will help guide your organisation to achieve compliance. This not only allows your organisation to work with UK Government business, but by taking a proactive approach to security we can prevent attacks from succeeding rather than responding when they do.

Annual CREST Penetration Test

Penetration testing is the gold standard of identifying vulnerabilities in an organisation that attackers will use to cause you harm. Our sister company is a leading CREST Certified Penetration Testing provider that will use CREST certified staff to proactivly identify vulnerabilites across your assets and help remediate them before they are used by attackers.

Service Level Packages

Our core service is spread across 3 distinct levels each tailored towards a specific point in an organisations lifetime.

ENDPOINT DEFEND

Ideal for small businesses in need of protection.

- ✓ 24x7 UK SOC Team
- ✓ Full Incident Response
- ✓ Custom Real Time Dashboards
- ✓ Rapid Response SLA
- ✓ Proactive Threat Hunting
- × M365 & AD Monitoring
- × Cyber Essentials Certification
- × Digital Risk Protection
- × Attack Surface Management
- × Dedicated Client Analyst
- × Annual CREST Penetration Test
- × Cloud Posture Management

Most Popular

BUSINESS DEFEND

Complete Protection for Small and Medium-sized Enterprises (SMEs)

- ✓ 24x7 UK SOC Team
- ✓ Full Incident Response
- ✓ Custom Real Time Dashboards
- ✓ Rapid Response SLA
- ✓ Proactive Threat Hunting
- ✓ M365 & AD Monitoring
- ✓ Cyber Essentials Certification
- ✓ Digital Risk Protection
- ✓ Attack Surface Management
- × Dedicated Client Analyst
- × Annual CREST Penetration Test
- × Cloud Posture Management

ENTERPRISE DEFEND

Comprehensive Proactive Detection and Penetration Testing for Enterprises.

- ✓ 24x7 UK SOC Team
- ✓ Full Incident Response
- ✓ Custom Real Time Dashboards
- ✓ Rapid Response SLA
- ✓ Proactive Threat Hunting
- ✓ M365 & AD Monitoring
- ✓ Cyber Essentials Certification
- ✓ Digital Risk Protection
- ✓ Attack Surface Management
- ✓ Dedicated Client Analyst
- ✓ Annual CREST Penetration Test
- ✓ Cloud Posture Management

In addition to the included features on each tier, optional features are available to bolt-0n.

Service Description

MDR - Endpoint Defend

MDR Endpoint Defend is a comprehensive solution that caters to small businesses requiring protection against malicious attacks. It offers 24x7x365 monitored Endpoint Detection & Response coverage to all workstations and servers within an organisation.

Powered by Crowdstrike Falcon, a leader in Endpoint Detection & Response, each organisation is granted direct-access to their Crowdstrike tenant. Alternatively, organisations with existing tooling and licenses can integrate with any EDR vendor to optimise their investments. Supported products include, but are not limited to, SentinelOne, Microsoft Defender, and Sophos XDR.

Our team of experts is available round-the-clock to address every alert generated by either our Crowdstrike EDR or your existing EDR solution. Each alert undergoes a rigorous investigation, employing the latest industry practices to identify any signs of compromise.

In case of malicious activity, our analysts implement containment measures either by directly connecting to the affected hosts or by automatically orchestrating actions through our ITSM into your EDR's API, thus reducing average threat dwell time and mitigating impact.

Service Commitments

MDR - Endpoint Defend

As part of this service, **Precursor** will provide the following:

- Implementation and deployment of sensors (If not already existing).
- Maintenance of policies, rules and updates for the EDR tooling.
- Regular Threat Hunting activities to identify threats dwelling in your environment that standard tooling can't detect.
- Threat Intelligence integrations for specific indicators of compromise.
- Multiple direct contact links into the vSOC, including a 24x7 open-line telephony system (Password required to dial in).
- Extensive incident reporting and alert investigation details via our Customer Portal.

As part of this service, the **customer** will provide the following:

- Information of their environment to assure suitable deployment.
- Sufficient access and permissions to the IT estate.
- Inform Precursor of any upcoming or future changes to the IT estate or business that may impact the delivery of the MDR service.
- Maintain sufficient contacts for incidents and alert investigation procedures.

Service Description

MDR - Business Defend

MDR Business Defend goes beyond the endpoint, extending detection & response capabilities to common business technologies, such as:

- Microsoft Office 365
- Active Directory
- E-mail
- Firewall

In addition to the extended monitoring, this service also provides features designed to enhance proactive reduction of cyber risk:

- Cyber Essentials Certification
- Digital Risk Protection by EdgeProtect

Utilising the extended data sources, the elite vSOC team monitor for dangerous threats such as:

- Phishing & Social Engineering
- Network-based malware
- Insider Threat and Data Loss Risk
- Identity Compromise & Leaked/Stolen Credentials

Service Commitments

MDR - Business Defend

As part of this service, **Precursor** will provide the following:

- Implementation and deployment of the solution.
- Ingestion from the below sources:
    - Microsoft Office 365/Google Workspace
    - Microsoft Defender (Any of the Defender family)
    - Firewalls/NIDS
    - Active Directory/Okta
    - E-mail flow and E-mail filtering logs
- Maintenance of EDR and SIEM related elements i.e. Data source health, detection rules and platform health.
- Threat Hunting activities performed regularly to identify threats dwelling in your environment that tools can't find.
- Threat Intelligence integrations for specific indicators of compromise.
- Provide immediate notifications on any compromised accounts, leaked credentials, malicious domains, delivered phishing emails.
- Multiple direct contact links into the vSOC, including a 24x7 open-line telephony system (Password required to dial in).
- Extensive incident reporting and alert investigation details via our Customer Portal.
- Monthly Attack Surface Management

As part of this service, the **customer** will provide the following:

- Information of their environment to assure suitable deployment.
- Sufficient access and permissions to the IT estate.
- Inform Precursor of any upcoming or future changes to the IT estate or business that may impact the delivery of the MDR service.
- Maintain sufficient contacts for incidents and alert investigation procedures.

Service Description

MDR - Enterprise Defend

MDR Enterprise Defend is Precursors most-holistic offering in the Managed SOC space. Precursor recognises that at the enterprise level, security goes beyond traditional monitoring services,

MDR Enterprise Defend provides you with a blend of defensive and offensive services, along with a dedicated client analyst whose primary objective is to understand your organisation and ensure maximum value is being realised from the service you consume.

Precursor offer the following additional features, on top of MDR Business Defend:

- Attack Surface Management
- Vulnerability Scanning
- CIS Benchmarking
- Dedicated Client Analyst
- CREST Penetration Test
- Unlimited SIEM data ingestion

Service Commitments

MDR - Enterprise Defend

As part of this service, **Precursor** will provide the following:

- Implementation and deployment of the solution.
- Ingestion of data from any desired source (Unlimited data ingestion).
- Maintenance of EDR and SIEM related elements i.e. Data source health, detection rules and platform health.
- Threat Hunting activities performed regularly to identify threats dwelling in your environment that tools can't find.
- Threat Intelligence integrations for specific indicators of compromise.
- Provide immediate notifications on any compromised accounts, leaked credentials, malicious domains, delivered phishing emails.
- Multiple direct contact links into the vSOC, including a 24x7 open-line telephony system (Password required to dial in).
- Extensive incident reporting and alert investigation details via our Customer Portal.
- Dedicated client analyst who will be your business partner throughout the relationship.

As part of this service, the **customer** will provide the following:

- Information of their environment to assure suitable deployment.
- Sufficient access and permissions to the IT estate.
- Inform Precursor of any upcoming or future changes to the IT estate or business that may impact the delivery of the MDR service.
- Maintain sufficient contacts for incidents and alert investigation procedures.

Service Levels

Industry leading responses

At Precursor, our elite team are experienced professionals in detecting and responding to advanced cyber threats, in addition to delivering an outstanding customer service. Below, you will find all of our service levels for the MDR product.

Ticket Definitions

All of our elite MDR teams work is logged in ‘tickets’, all tracked by you in real-time via our Customer Portal. To help you understand the types of tickets you’ll see, please see below our definitions:

Ticket Type	Description
Cyber Incident	If our team identify malicious activity, present or current, they will invoke a ‘Cyber Incident’. We align our definition of a cyber incident to exactly how NIST define one: “A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.”
EDR Alert	These tickets are alerts generated via your Endpoint Detection & Response (EDR) solution, we send these alerts to our ticket system via the vendors API. You will find comments on those tickets summarising any investigation steps and findings.
SIEM Alert	These tickets are alerts generated via our Security Information & Event Management (SIEM) platform. These alerts can be from any other data source such as Microsoft 365, Active Directory, Firewall, Public Cloud etc.
Tuning	Unlike other providers, we openly share the amount of tuning we provide to our platform to demonstrate the sheer volume of “Housekeeping”. Tuning tickets are raised by our elite analysts if they find a method to improve the accuracy of a detection rule/method.

Service Levels

Industry leading responses

SLA's and Response Times

Priority Level	Definition	Wait Time	Response Time	Investigation Time
P1 - Critical	An alert/event directly attributable to malicious activity.	5 Minutes	15 Minutes	30 Minutes
P2 - High	An alert/event that is highly likely to be a precursor/indicator to malicious activity.	5 Minutes	30 Minutes	60 Minutes
P3 - Medium	An alert/event that is commonly associated with malicious behaviour.	5 Minutes	60 Minutes	120 Minutes
P4 - Low	An alert/event where the activity is a potential security risk.	5 Minutes	120 Minutes	240 Minutes

Response Time Definitions

Wait Time - How long an alert/request should wait in our queue(s) before it is assigned to an owner for next steps.

Response Time - This is how long the owner has to provide a first response i.e. comment demonstrating/summarising what's been done within the Response Time SLA.

Investigation Time - This is how long our team have to fully investigate an alert/request prior to closure/escalation.

Service Provision

Onboarding Overview

Upon becoming a customer of Precursor, we immediately act upon our commitment to deliver an outstanding customer experience by initiating a project to begin onboarding.

Our projects are managed by a qualified Project Manager (PM) who will ensure all requirements and deadlines are met. You will also be assigned a SOC engineer who will be responsible for the technical delivery of onboarding.

Onboarding items can include:

- Sensor deployment (via GPO, SCCM or an RMM of your choice).
- EDR tenant provision and configuration (If you're bringing your own EDR, we will review the tenant configuration).
- SIEM data ingestion.
- Customer user access to EDR/SIEM/Customer Portal.
- Vulnerability Scanning, Attack Surface Management and Digital Risk Protection deployment.

Our provisioning team are experts in supporting organisations of any size, including attending Change Approval Board (CAB) and Architecture Review Boards (ARB), if required.

Our SOC Engineers ensure a minimum of 80% sensor coverage is achieved during project stage and all minimum data sources are ingested. We follow NCSCs guide on "Must Have Data Sources" for SIEM.

Service Provision

Onboarding Process

At a high-level, our onboarding process can be viewed as 3 key phases.

1. Project kick off

Our Project Manager conducts a project kick off meeting, detailing the deliverables, solution overview, involved parties and overall timeline.

2. Project Delivery

You will be assigned a SOC engineer who will be responsible for the technical provision of the solution.

3. Go-Live

Upon delivery of the pre-agreed key milestones, the project will transition to live-service, where a handover meeting will take place to confirm the service into live.

Precursor

Service Methodology

Setting the bar in delivery.

MITRE ATT&CK Framework

Our vSOC team align detections and understanding of threat actor activity to a framework known as MITRE ATT&CK Framework. This is an industry leading standard for communicating and understanding threat actor Tactics, Techniques and Procedures (TTP's).

Following this framework maintains full and up to date visibility into how threats evolve. We hold certifications in MITRE ATT&CK.

Cyber Threat Intelligence

The MDR platform integrates with Cyber Threat Intelligence (CTI) sources such as VirusTotal, Abuse.CH, SOCRadar and NCSC CiSP.

This ensures that the vSOC team have access to known-malicious IP addresses, domains, URLs and files that can be found in your environment, used as tip offs.

Training

At Precursor Security, we take training of our staff very seriously. As a human-operated service, we recognise the importance of ensuring our analysts and engineers have the latest understanding of threats and tooling.

We hold and maintain multiple certifications and provide budgets for annual training. We're also a strategic partner of HackTheBox who provide our team with regular live-fire exercises and labs.

Service Methodology

Setting the bar in delivery.

Continuous Improvement (ITIL)

The vSOC is committed to continual improvement. Pralign to ITIL Continual Service Improvement (CSI), which is a 7-step improvement process. We hold regular service reviews internally to ensure our processes are up to specification for delivering an outstanding service that protects our customers around the clock.

Our vSOC Management are also GIAC GSOM certified, covering process improvement as a key area of certification.

Automation

We recognise that threats are breaking into networks faster year on year. As a result, SOC teams must action their responses faster. To combat this, We have partnered up with N8N as our automation technology partner.

We have automation playbooks for phishing, ransomware, data exfiltration, identity compromise and more. This further speeds up response times whilst eliminating human error.

Partner Selection

As a technology-centric service, we select our partners very carefully by assessing them against multiple pillars of requirements. We are transparent in our selections and remain vendor agnostic to support customers of all ranges.

Service Methodology

Reporting & Communications

Customer Portal

At the beginning of onboarding and throughout the lifecycle of the service, the majority of your requests can be met through the customer portal. Additionally, your service performance can be monitored in real-time through dashboards in this portal.

We want to ensure you get the most from your reporting, we will work with you to create custom dashboards bespoke to your insight requirements.

SOC Communications

When our elite vSOC team perform investigations, they may reach out to notify you of findings, incidents or request further information. To accomplish this efficiently, we capture from you who your preferred contacts are for each of these streams of communications.

1 Cyber Incident Declared

If the team identify malicious activity, a cyber incident will be invoked and you will receive regular communications which can be tracked via e-mail and/or the portal.

2 Request for Information (RFI)

MDR SOC Analysts generate these notifications when investigating activity and need more information. The frequency of these notifications varies based on your environment.

Action is required. Please review the activity in these alerts and let the vSOC team know whether or not you expect this activity.

Quality, Compliance and Security

ISO27001

As a security-centric organisation, Precursor maintain an ISMS in accordance with ISO27001/2. Precursor are also ISO27001 accredited.

Cyber Essentials Plus

In addition to our commitments and investment to ISO standards, we recognise IASME Cyber Essentials Plus as a “must-have” for any security conscious organisation. As a result, we also maintain our compliance for CE plus.

Annual Penetration Testing & Security Assurance

Continuous Self-Testing is a crucial component in a proactive approach towards safeguarding our networks. One way to achieve this is by employing the same Tactics, Techniques and Procedures (TTPs) utilized by our adversaries. By conducting controlled tests on our network, core systems, and applications, we can detect vulnerabilities before they're exploited. It's also essential to ensure that our systems adhere to best security practices, offering a strong layer of defense. Combining this with adversary emulation attacks against ourselves validates our detection and response capabilities. Together, these measures increase operational resilience and instill confidence in our ability to protect against fast-evolving cyber threats.

ISO9001

Quality is a reason Precursor exists today, when the brand started, our vision was to deliver high-quality, high-performing security services. For those reasons, we make an ambitious effort to maintain compliance and achieve ISO9001.

www.precursorsecurity.com