MANAGED DETECTION & **PARTNERED** RESPONSE

VIASAT CYBER SECURITY SERVICES

Why Managed Detection & Partnered Response (MDPR)?

Current cyber security services landscape

It’s no secret that accelerated digital innovation is a double-edged sword that heavily impacts the security industry. As data becomes the new currency of our digital lives, companies must ensure the privacy and security of their intellectual property and customer information.

Overwhelmed by the ever-growing cybersecurity tech stack of different tools and managed services? You are not alone. If you ask the majority or security professionals, at any level, whether they have enough knowledge to really discern the difference between providers and services, the answer is a resounding NO! The real issue is because of the mountain of security solutions, security professionals and teams feel that the only way to be successful is to outsource the security requirements to a vendor. They are supposed to know at least more than you do, right? The reality is often far different. Vendors are expert in their own products and potentially a few others that directly interact with their own. The impact is that this solution makes you an outsider to your own security and it becomes increasingly difficult to choose the right vendor or solution that meets your core mission when you need to change.

Current MSSP and MDR services are stand-alone capabilities and are not designed to accelerate the maturity of your security program. These services are external solutions only, and as a result, are not an extension of your own team. The current solutions are unable to truly partner with you, learn your security goals and current visibilities, train you to help augment your team, or customize the types of support you may need. In order to really take full advantage of MSSP and MDR solutions, it requires knowledge and expertise that most organizations lack. Who really wants to be an outsider to their own security, unable to truly impact the outcome of issues that impact your business?

What is Managed Detection & Partnered Response?

The solution at a glance

Managed Detection & Partnered Response is a concept of security operations that is designed to apply internally as well as externally to strengthen and accelerate your current security program. They key concept behind MDPR is that YOU are the hero of story, not the security service. When you choose Viasat as a partner, you now have a team of professionals who are highly invested in your success. As a trusted security partner, our team will work hand in hand with you to create a customized solution that helps you solve your security problems.

We believe that you should be able to get the very best from our team without having to be an expert across the breadth of capabilities that we provide. Whether you need a high level of interaction to gain velocity for your program, or a more nuanced application of our security capabilities, our guiding principle is to meet you where you are, identify where you want to go, and help you get there as fast as you want to move. We think you will be surprised at how fast you can move when you have a real partner and not just a vendor. Your security program will be better because our partnership isn’t just about a tool, or collection of tools we provide. Our partnership is all about seeing you and your team succeed. **We win when you win.**

What is included in MDPR?

Strengthen your security with the partnership model

World-class CSOC services (Cyber Security Operations Center)

Our team of dedicated analysts secure a diverse set of networks- from residental customers on our ISP network to to President of the United States. American Security Today award winner for "Best Cyber Security Program for Government or Military."

SIEM build and integration

Based on customer need, Viasat will add and manage custom correlation searches, dashboards and third-party tools in support of the customer SIEM and security requirements. The team will provide custom applications and support to help bolster monitoring and analysis.

Network and end point detection and response

We use network and endpoint telemetry data to enable real time interrogation of internal traffic (e.g., east/west and north/south) to perform threat detection and respond to security incidents regardless of where the adversary may be trying to gain a foothold.

Status reviews and white glove support

In conjunction with submitting a Monthly Reports, Viasat will hold actual meetings with your security team. On a daily basis, this service provides white glove hand-in-hand support - 24/7/365 managed detection and partnered response, live slack channels, and assigned analysts.

Immersive CSOC training

Viasat's immersion training for detection and response is an instructor lead experience where members of your security team have the opportunity to train with our security team in the environment developed as part of Viasat's MDPR. This means that you train with the actual information and SIEM that you use on a daily basis, giving you truly relevant training for your team that strengthens the partnership and increases the velocity and maturity of your security team.

Cyber Security Operations Center lines of operation

From resident to president

Cyber detection & response

The detectives. While the adversary must discover only one way in, the detection and response team must constantly defend and hunt across all internal systems and network entry points to prevent compromise. Any suspicious behavior identified will instantiate our Incident Response Process and an investigation will be conducted to gather and analyze evidence, determine impact, identify the root cause, and provide remediation instructions to the decision makers.

Cyber Threat Intelligence

The researchers. In order to be successfully proactive in an ever-changing landscape, advanced situational awareness and a deep understanding of emerging threats is necessary. The CTI team provides actionable and relevant intelligence on customer environments that comprehends, synthesizes, and prioritizes current vulnerabilities and critical systems, reducing risk and remaining ahead of the adversary.

Cyber infrastructure engineering

The architects. An optimized and secure network is the foundation that provides the structure and support for advancements made in the Security Operations Center. The network engineers are responsible for configuring and maintaining the security appliances and policies.

Development

Cyber Q branch (007). On the front lines of technological innovation and ingenuity, the Viasat SOC harnesses automation to capture and accelerate human intelligence, producing correlative machine-aided detection capabilities fueled by unstructured data warehousing. This engineering manifests as a bespoke toolset, accelerating operational velocity, accuracy and efficiency.

Cyber analytics

The scientists. In order to keep up with the ever-changing threat environment, our analytics team focuses on the use of data to proactively filter and identify notable events. This behavioral analysis allows the CSOC to improve response time, determine course of action and allows for more time to be spent on high severity investigations.

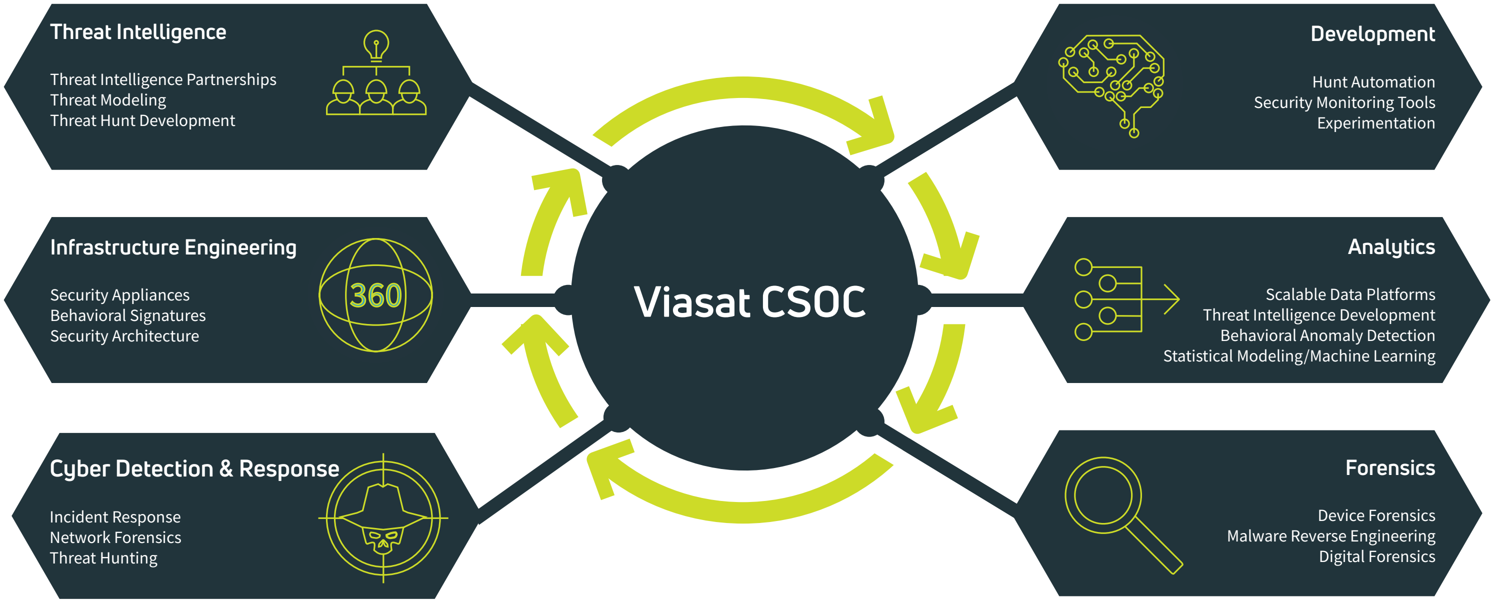
Cyber forensics

Crime scene investigators. During critical investigations when deeper analysis is required, a forensic investigation is conducted. The investigation includes a deep dive analysis of system artifacts in order to identify compromise, root cause, impact, generate threat intelligence, and provide remediation recommendations to customers.

How the lines of operation work together

Viasat Cyber Security Operations Center has six main focus areas; cyber detection and response, cyber threat intelligence, cyber infrastructure engineering, cyber analytics, forensics and development. Together, these cohesive efforts form a holistic cyber approach, providing advanced machine learning, novel threat intelligence, and accelerated detection times.

This integrated model gives the agility to scale and respond to emerging threats and surges as quickly as they evolve.



Viasat CSOC

Threat Intelligence

Threat Intelligence Partnerships
Threat Modeling
Threat Hunt Development

Infrastructure Engineering

Security Appliances
Behavioral Signatures
Security Architecture

Cyber Detection & Response

Incident Response
Network Forensics
Threat Hunting

Development

Hunt Automation
Security Monitoring Tools
Experimentation

Analytics

Scalable Data Platforms
Threat Intelligence Development
Behavioral Anomaly Detection
Statistical Modeling/Machine Learning

Forensics

Device Forensics
Malware Reverse Engineering
Digital Forensics

Our network

At the core of Viasat’s security experience is protecting live networks to deliver high quality, uninterrupted connectivity. The processing and analysis of all the data across our network gives us prime security intelligence across all industries.

This intelligence has not only given us the edge to adapt rapidly to adversaries and market needs, it has given us a broader view into what is next and what is needed for the industry as a whole.

EVERY DAY ON OUR NETWORK:

500TB of data **delivered**

30TB of user data ingested, **analyzed and archived**

5.5bn **security events** analyzed

5,000 seamless **beam handovers**

2,000,000+ passenger **personal electronic devices (PEDs)** connected worldwide

WHICH TRANSLATES TO BETTER INTELLIGENCE, FASTER RESPONSE AND MORE TIME SPENT WITH CUSTOMERS (ANALYTICS PROVIDED FROM VIASAT RESIDENTIAL NETWORK):

600,000+ customers are predictively protected from inbound malware using custom threat intelligence per quarter

94 observations analyzed per customer

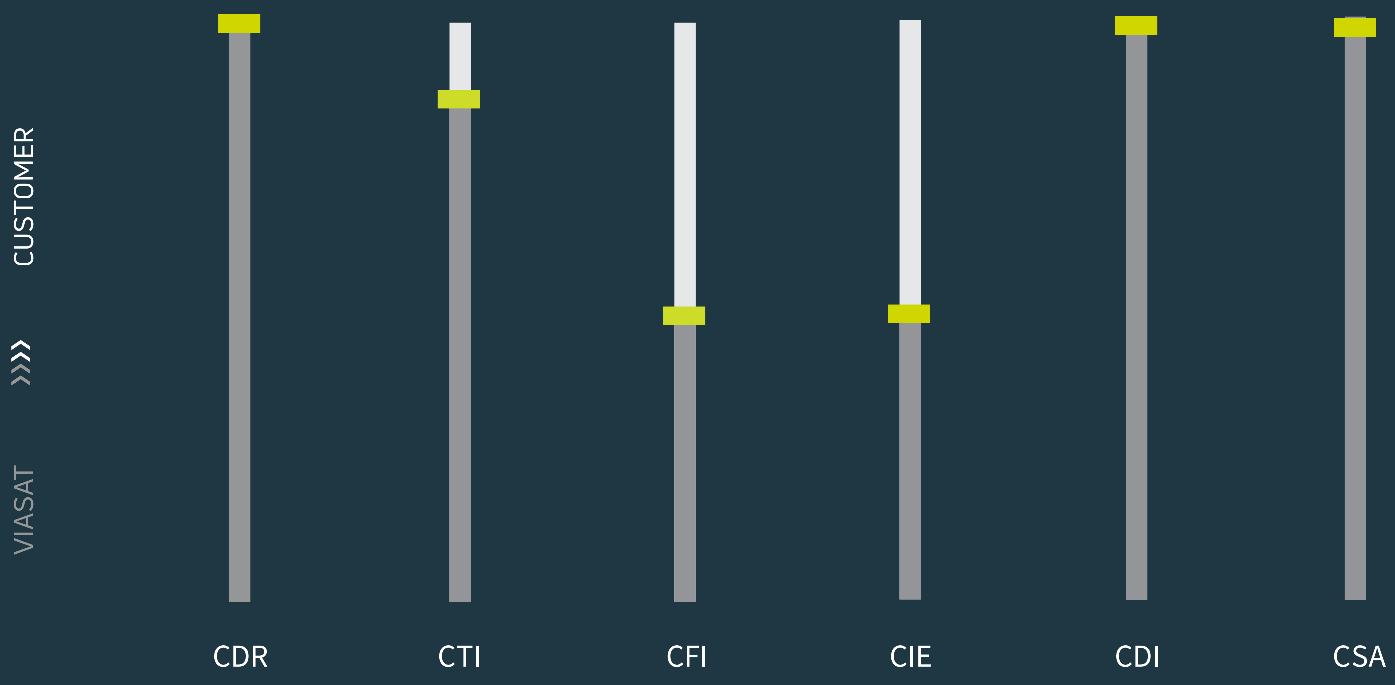
313 phishing URL’s detected and blocked/month

13Million ↑ Indicators of Compromise (IOCs) or threat indicators used on a daily basis to protect customers

Managed detection & partnered response work share slider sample

As your partner, it is important for us to work together and create a customized solution that will solve your security needs. Our work share slider is meant to evolve over time as the needs of your team may change or grow with the number one goal to see you and your team succeed.

Capability engagement:



Cyber detection and response

Incident response

Digital forensics

Threat hunting

Cyber threat intelligence

Threat intelligence partnerships

Threat modeling

Threat hunt development

Cyber forensic investigations

Device forensics

Malware reverse engineering

Network forensics

Cyber infrastructure engineering

Security appliances

Behavioral signatures

Security architecture

Cyber development and integration

Hunt automation

Security monitoring tools

Experiementation

Cyber security analytics

Scalable data platform

Statistical modeling and machine learning

Threat intelligence development

Behavioral analytic and anomaly detection

CONTACT

SOC DIRECTOR: PAUL KEENER
TEL 760.893.4031
EMAIL paul.keener@viasat.com