

FORWARD DEPLOYED ANALYST

ON-SITE, CUSTOMIZED INTELLIGENCE, INSIGHTS AND ANALYTICS

OVERVIEW

Forward Deployed Analysts use FireEye intelligence sources, methods and data to provide our clients with a decision-making edge. Analysts contextualize cyber threats; correlate source data; and provide tactical, operational and strategic intelligence to provide insightful assessments. They work with intelligence collected from Mandiant incident response investigations, FireEye threat information gathered from millions of virtual machines and FireEye iSIGHT adversarial threat intelligence collection and analysis. Forward Deployed Analysts deliver visibility into the tactics, techniques and procedures (TTP) that attackers use against targeted organizations.

Industry-Leading Expertise

Each FireEye Forward Deployed Analyst comes with the threat intelligence and information security expertise to reveal meaningful insights. The analyst will leverage FireEye proprietary methodologies, approaches and tools to stay current on the latest research and TTPs to identify trends and anomalous activity, while forecasting threat actor activity. The analyst will provide insight into the latest threat activity targeting the customer's industry, company, personnel and data systems.

On-Site, Customized Insight

The Forward Deployed Analyst delivers customized intelligence and analysis for each organization's decision makers as well as front line network defenders. These custom products include a comprehensive set of dossiers, trends, news and analysis on advanced cyber threat groups. Decision makers can set priorities for intelligence collection and production to gain insights on very specific topics of interest that may be unique to the organization.

HIGHLIGHTS

- Develop or complement an in-house intelligence capability driven by FireEye's industry-leading threat intelligence
- Access FireEye's intelligence to understand the relevance and priority of threats to an organization's network
- Convey key intelligence findings and context about threat activity across an organization
- Identify potential threats and threat actors specific to each organization
- Identify and prepare for the tactics used by the most advanced threat actors

On site, the analyst will learn the priorities of the organization and guide production analysis to determine what will be most impactful for the client. These products will be based upon raw data generated by client security systems and fused with FireEye intelligence to provide greater context. While reporting will be customized, current customers frequently request deliverables such as:

- **Threat briefings:** Overviews of cyber threat landscape, evaluations of likely targets
- **News analysis:** Assessments of the most important, current and popular open source intelligence events in the media
- **Intelligence profiles:** Contextual and strategic analysis clarifying user understanding of threat groups, sponsors and industry activity
- **Threat insights:** Examination of new developments regarding threat group activity customized to the customer, industry and region
- **Trends:** Observed and identified threat actor tactics and targets across sources

Connection to FireEye iSIGHT Intelligence

While deployed to the client site, the analyst maintains integration with the core of FireEye intelligence. This means that the analyst will continue to have direct communication with the core intelligence researchers and incident responders to gain intelligence in real time as incidents are developing, even before products may be written. Additionally, a suite of proprietary tools used by the Forward Deployed Analysts brings a technological edge to speed analysis. The analyst provides a critical bridge to FireEye intelligence and tools.

Why FireEye?

Expertise. Technology. Intelligence.

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence and expertise — reinforced with the most aggressive incident response team — helps eliminate the impact of security breaches. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. The FireEye Global Defense Community includes more than 3,100 customers across 67 countries, including over 200 of the Fortune 500.

FireEye offers a comprehensive portfolio of services. For full details, contact us at services@FireEye.com or **+1 855.692.2052**.

FireEye, Inc.

1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

