OP INNOVATE

DFIR SERVICES

Be prepared for the most advanced cyber attacks

Swift action within minutes by ANT, a world-class team of incident responders.

KEY BENEFITS

- ✓ **Guaranteed service level -** A swift response within minutes.
- ✓ **State level professionals -** A team of crisis managers and technical experts at your side.
- ✓ **Exceptional track record -** Effectively solving several cyber crises per week.
- ✓ **Vendor agnostic -** As your trusted advisor, our team will adjust to your business line and deployed technologies.
- ✓ **Efficient response -** Our team will resolve the attack and minimize the impact and risk allowing you to focus on your business and customers.
- ✓ **Maximize your readiness -** Engaging a long term agreement improve your business readiness by laying the methodologies and infrastructure.
- ✓ **Swiss army knife -** Our professionals are equipped with our own custom tools along with the best-of-breed technologies available.

OP Innovate's ANT team are international leaders in the fields of cyber research and incident response services, leveraging a suite of disruptive products, born out of our extensive experience in the trenches of cybersecurity.

Team members are all accredited professionals, certified on a variety of sought-after qualifications. Each brings unrivaled cyber expertise to the table, combining a thorough depth of technological knowledge with a drive to deliver high quality findings in all areas examined.

ANT uses an innovative rapid response tool, which is at the cornerstone of incident handling. This tool grants the team a critical head start by beginning our DFIR activities from the earliest moments of the team's engagement.

ANT

DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR) SERVICES

Ransomware

Respond to and recover from a ransomware attack. Contain the threat, determine root cause, window of compromise, attacker activity, and quantify sensitive information exposed. Where required, negotiate with threat actors, acquire and validate decryption keys, and develop and implement a recovery plan.

Web Application Compromise

Respond to and recover from a web application attack. Contain the threat, analyze logs, review code, quantify exposure or loss of sensitive information, and get recommendations for design hardening countermeasures.

BEC

Respond and recover from unauthorized access to your enterprise email environment. Contain the incident, determine root cause, window of compromise, attacker activity, and quantify sensitive information exposed.

Insider Threat

Investigate abuse of privileged access afforded to otherwise trusted employees, including identification of data accessed or misappropriated and/or unwanted actions taken by insiders.

Unauthorized Access

Hunt for historical or ongoing indicators of compromise to identify evidence of unauthorized access or activity (across cloud, email, endpoints).

Malware

Analyze malware samples using open source intel, sandboxing, reverse engineering, and deliver a report, including the behavior and functionality of the malware.

AFFECTED DOMAINS

Area	Potential Damage	How ANT helps
Legal	Legal culpability and requirement to disclose.	Legal counsel to advise on handling legal aspects of response, disclosure & transparency, and documentation.
Financial	Costs of downtime including lost business, salaries and costs associated with returning to "business as usual".	Facilitation of swift return to "business as usual", recovery of stolen funds, and expert advice on negotiation and ransom payment. The team can work with your cyber insurer where relevant.
Reputational & customer retention	Damage to reputation inflicted by disgruntled customers and competitors alike.	Proven reputation management strategy that includes advice on disclosure of the incident to relevant stakeholders including broader employee base, board of directors, customers, media etc to retain their trust.
Regulatory	Costs associated with regulatory fines and the need to provide data regulators with breach related information within short time frames.	Compilation of compliant, tailored ICO reports on details of the incident and the response steps being taken, as required by regulators.

Maximize readiness and resilience with ANT

When your organization faces a crippling cyber incident, will you be ready? The speed of your response, as well as the effectiveness of your tools and playbooks, will determine how quickly you can recover and return to business as usual. Extend the existing boundaries and capabilities of your team by putting our world-class incident response and cyber risk management ANT Team on speed dial.

Our portfolio includes cases involving rogue insiders to organized crime syndicates and nation-state threats. ANT Team deals with numerous high profile incident response investigations each year. The ANT Team retainer gives you forensics and response expertise when you need it most, with a pre-determined service-level agreement (SLA). At a time when the skill gap in cybersecurity is growing and skilled teams are overwhelmed with work, it pays to prepare for a rainy day.

PROPRIETARY TECHNOLOGY

ANT automates the critical early response phases by shortening the incident lifecycle. It fastidiously gathers log and system data, triages and analyzes it, in search of the attack vector. ANT gives you a fighting chance to get your business back up and running by supporting our Extended Detection and Response (XDR) capabilities.

- ✓ ANT slashes time spent on incident response, and boosts mean time to recover (MTTR).
- ✓ ANT is portable, lightweight, agentless and quick. It supports both Windows and Linux OS.
- ✓ ANT correlates operating system and application log data to give responders that much needed head start.
- ✓ ANT utilizes an enterprise-level data analysis engine to acquire workable intel on the ongoing attack

A STELLAR TRACK RECORD

A small selection of the team's wins

Iranian Pay2Key vs the Israeli logistics supply chain

OP Innovate served as the Israel National Cyber Directorate's (INCD) main incident response partner during the Iranian Pay2Key cyber campaign which targeted at least 80 Israeli firms in Dec 2020.

Bank Sniffing

A bank in South America was tipped off that active surveillance was being conducted from their offices and IT environment. The team discovered covert hardware physically deployed in their headquarters and took it down.

DDoS the Provider

A leading provider of video streaming services was hit by a brief yet potentially fatal distributed denial of service (DDoS) attack. More destructive attacks were threatened. The team's intervention ensured that the threats were not realized.

Hospital Takedown

A major Israeli hospital was hit with a destructive ransomware attack that sent hospital staff back to using pen and paper. The team worked tirelessly to recover operations and restore lost information.

Investment Fund BEC

A private equity family office woke up to a disturbing update from one of its portfolio companies - a wire transfer failed to land in the correct bank account. Armed with the team's IR report and a detailed attacker profile, the US Secret Service was able to recover the stolen funds.

Cryptocurrency Breached

A cryptocurrency exchange was hacked. Assets worth tens of millions of US dollars were stolen. The team identified the attack vector, contained the attack and recovered more than half of the stolen assets.

ABOUT OP INNOVATE'S ANT TEAM

OP Innovate is a leader in cyber exposure management with its groundbreaking WASP web application EM platform.
The OP Innovate's research team holds extensive expertise in cyber research, penetration testing, incident response, training and forensics. As veterans of prestigious military intelligence units, these accredited professionals are certified on a variety of sought-after qualifications, delivering unparalleled cyber expertise and dedication to deliver high quality findings in all areas examined.

UNDER CYBER ATTACK?

Scan the QR Code
Fill Out The Online Form

And We Will Contact You Immediately.