UnderDefense

We are First Responders in the cyber world

We help companies respond & recover from Security Incident.

Incident Response Services

You can get **back to normal business operations 4X faster.**

YOU WILL RECEIVE

Answers
What, When, How, Where, WHY

Treatment
Certified industry experts & Elite threat hunters

Damage evaluation and risk mitigation
Threat will be localized and contained

Reduced impact and dwell time
Involving IR team can save you more than 50% of cost

Recovery
Get back to normal operations fast

KEY ADVANTAGES

Elite threat hunters
Former National Security Services and Cyber Crimes Unit Officers will leave attackers with nowhere to hide.

24x7 incident response
Around the clock availability and support for you. Our Incident Response team is ready to start investigations within 4 hours from first contact onsite or remote.

Malware Analysis
Our reverse engineers analyze 10 000+ malware samples/month, write decoders that provide insight into the capabilities and TTPs used by attackers.

Technology
We have solid experience working with industry-leading software like Splunk, Azure Sentinel, or Radar, as well as any tools our clients are using.

Transparency and no hidden costs

Focus on answers and recovery

We'd make sure it will not repeat

KEY CAPABILITIES

1 **Fast IR of a high quality:**
The speed to remediation is critical, when a business needs to restore it’s normal operations.

Expertise, proven process and industry leading technology helps us resolve incidents faster and more efficiently.
As a result: less hours incurred and lower costs.

2 **Negotiation support:**
Our Incident Responders have years of experience and deep understanding on how malefactors work, so we can fully support or lead negotiations defending company’s business interest.

3 **Decrease ransom payoff:**
During downtime, business may be losing a lot of money every minute.

If paying a ransom provides a faster, more cost effective and complete restoration of data, often we can significantly decrease it from initial demand during negotiation and pay a ransom on a client’s behalf if needed.

4 **Experience and expertise:**
Our forensic experts have 10+ years of hands-on experience in DFIR.

UnderDefense IR team have sharpened their skills on cutting edge of cyber attacks as National Security Services and Cyber Crimes Unit Officers fighting nation-state APT groups.

5 **Crisis management:**
Often the cost of a breach and company reputation is highly correlated with crisis communication.

We help clients on incident-related communications -including executive communications, public relations and disclosure requirements.

6 **Result oriented:**
As a deliverables of our work company will get Executive summary, Investigative report and Remediation report.

Our goal is to help client improve overall security posture of the environment to prevent or significantly limit the damage from future attacks.

INCIDENT TYPES COVERED

1 **Intellectual Property Theft:**
This includes the theft of ideas, inventions, creative expressions, trade secrets or other sensitive information in attacks often conducted by sophisticated state-sponsored actors.

2 **Financially-Motivated Crime:**
Business email compromise, payment card theft, extortion / ransomware, cryptojacking and others are examples of this type of attack.

3 **Destructive Attacks:**
These can be anything from damaging, targeted malware deployed by sophisticated adversaries, to nuisance malware designed to cause business disruptions.

4 **Data Breaches:**
This includes the theft of personally identifiable information (PII) that could potentially expose an individual or a customer of your business.