Datasheet

Trend Micro™

Incident Response Service

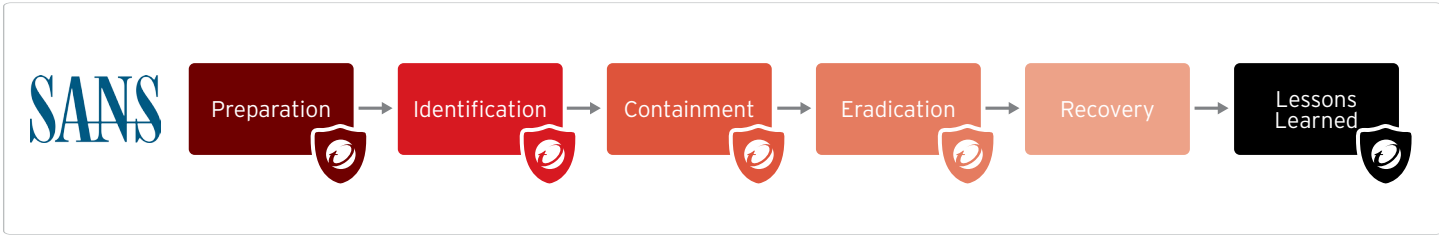
Resume operations quickly and safely

Mitigating the damage of an incident requires a rapid and strategic response from a highly skilled global team. From identifying the source of the breach to advising how to restore operations and minimizing impact, our Incident Response Service work around the clock to ensure the security and resiliency of your organization.

How it works

At its core, our Incident Response Service is based on the SANS model, a proven and effective methodology for responding to your cyber incidents. When an incident occurs, our team quickly assesses your situation, determines the scope and impact of the incident, then develops and executes a comprehensive response plan tailored to your specific needs. Throughout the process, we'll consistently keep you involved via secure channels, so you can make informed decisions about your organization's security.

Cyber incidents have been on the rise in terms of frequency and sophistication. Cybercriminals are continuously developing new techniques and tools to exploit vulnerabilities. According to research conducted by Ponemon, insider threat incidents have risen 44% over 2021 and 2022, with costs per incident up more than a third to $15.38 million.



SANS Incident Response model

Digital forensics

Through a preliminary triage call, we identify your key research questions. Examples include, "what is the root cause of the incident?," "what is the kill chain of the attack?," or "is there evidence of data exfiltration?."

Our Incident Response team then conducts a digital forensic investigation to uncover the evidence required to answer your investigation objectives. An investigation report is delivered, answering your research questions and a detailed list of high-priority recommendations is delivered. These strategic qualifiers help you prevent future incidents and safeguard your organization's assets.

How we work with you

Communication

When responding to a cyber incident, communication is critical. In some cases, the attacker may have compromised your Active Directory (AD) domain. By using out-of-band communication channels, we can ensure our communication is secure and that our efforts are coordinated efficiently.

Task management

Streamlining the incident response process allows us to facilitate incident coordination for your organization. By employing task management tooling, it's possible to assign tasks, track progress, and collaborate effectively with our crisis engineering team. This includes all tech stakeholders and our crisis management team—which comprises of management stakeholders.

By having two teams with complimentary focuses, we can ensure the technical aspects of your incident have been addressed, while managing the crisis from a higher-level perspective.

This approach promotes seamless collaboration and ensures we're taking the necessary steps to respond to the incident.

What can you expect?

Collaboration

- Out-of-band communication channels ensure easy and secure communication in the event that your domain may be compromised (i.e. through email and Microsoft Teams).
- Task management tooling makes certain each party is completely up to date.

Insight

- Digital forensics (on endpoints and servers) and network forensics (on network traffic) monitor threat actor behavior.
- Trend Micro™ Deep Discovery™ Inspector delivers a second layer of network forensics.

Engagement

- Incident Response are tailored specifically to your needs and typically requires between 5 to 10 days of engagement.
- Organizational activities are able to operate 24/7 during this period.

AVAILABILITY

Trend Micro Incident Response Service
is available for all existing and future Trend Micro customers.

Questions or requests? Reach out to us at incident_response@trendmicro.com or share your attack situation here.

Trend Service One™ Complete customers automatically have access to 40 hours of free Incident Response Service.