**Security Incident Detection and Response in Cloud**

A security incident indicates that systems and data in a network have been compromised or misused. A single security incident can be part of a bigger targeted attack such as a distributed denial-of-service (DDoS), ransomware, or advanced persistent attack. Security attacks can affect not only your organization's finances, but also its reputation. This is why it's critical to detect a security incident as soon as it occurs, mitigate the threat immediately, and contain or reduce the impact of the attack.

When it comes to solving a cybersecurity issue, reducing the mean time to detect (MTTD) a security incident is a priority. Did you know that the average amount of time to detect an attacker is [95 days](https://www.entrepreneur.com/article/345553)? With 95 days of dwell time—the amount of time between the attack and detection of the attack—in the network, attackers have plenty of time to carry out their malicious objectives. Every organization strives to reduce the MTTD and dwell time of attacks to minimize the damage. To reduce these parameters, security incident detection needs to be swift and effective.

## The challenge of detecting security incidents

Detecting security incidents or data breaches poses a challenge for organizations for various reasons. It often involves detecting indications of compromise from an overwhelming number of false alarms. Though, general preventive systems like firewalls and antivirus software give you alerts on deviant behavior, they don't provide the bigger picture. For every triggered alert, you need to investigate why it was triggered, which increases the resolution time.

General preventive systems provide limited data. For instance, if an employee's credentials are stolen and are being used to access critical resources, it's difficult to mark this as deviant behavior and flag it as an incident unless more contextual information is available. Security information and event management (SIEM) solutions correlate business contextual information with network activity to detect incidents in real time.

### [Log correlation](https://www.manageengine.com/log-management/siem/static-dynamic-event-correlation.html?cathaypacific)

Log correlation looks for significant patterns in activity by analyzing logs from various sources. Although an individual event may not look suspicious, correlating it with a related sequence of events can show indications of a threat.

Building a good correlation rule that defines what an attack pattern may look like helps uncover known attack patterns, and can be used to identify and stop suspicious activity. For example, you can build a rule for the following sequence:

**"A rule that detects multiple VPN logon failures followed by a successful VPN logon and an immediate remote login in a Windows device, after which suspicious software is installed."**

Alone, these events may seem unremarkable. But correlation rules help connect these incidents to highlight an attack pattern that the SIEM system can use to detect security incidents like these as soon as they happen.

### [Threat intelligence](https://www.manageengine.com/log-management/siem/threat-intelligence-solution.html?cathaypacific)

Threat intelligence helps in early incident detection by employing threat feeds to identify incidents. Threat intelligence modules in SIEM solutions leverage threat data from various sources from open source STIX/TAXII-based threat feeds to vendor-specific third-party threat feeds. These provide the latest and most reliable threat information available to help mitigate cyberthreats. With a regularly updated threat database, SIEM solutions can detect evolved security incidents in your network instantly.

### [Anomalous user behavior analytics](https://www.manageengine.com/log-management/siem/ueba-user-entity-behavior-analysis.html?cathaypacific)

To defend a network against threats and data breaches, it's important to study events taking place throughout the network system. The log data an organization stores contains deep insights into user behavior. This includes a user's login and logout times, their user privileges, accessible data, and much more.

Through machine learning, user and entity behavior analytics (UEBA) engines can monitor these logs constantly to recognize any deviation from the normal behavior pattern of a user. For example, if an employee's usual work hours are weekdays from 8am to 5pm, a login attempt at 11pm on a Saturday will be recognized as anomalous activity. With this self-learning mechanism, UEBA helps you more accurately detect insider threats, account compromise, data manipulation, and much more.

**AWS Incident Detection and Response**

AWS Incident Detection and Response offers AWS Enterprise Support customers proactive monitoring and incident management for their selected workloads. AWS Incident Detection and Response is designed to help you reduce potential for failures on your workloads and to accelerate your recovery from critical incidents.

AWS Incident Detection and Response begins with a review of your workloads for reliability and operational excellence. AWS experts work with you to define critical metrics and alarms that provide improved visibility into the application and infrastructure layers of your workloads, making it easy to find and prioritize issues during an incident. AWS Incident Management Engineers continuously monitor your workloads, detect critical incidents, and engage you on a call bridge with the right AWS experts to accelerate the recovery of your workloads. All incidents are managed with the highest level of severity and escalation, and AWS remains engaged until the incidents are resolved. Lessons learned from previous incidents inform improvements to response plans and workload architecture, driving a continuous improvement cycle to improve the resiliency of your workloads.

AWS Incident Detection and Response is available in English for workloads hosted in [eligible AWS regions.](https://aws.amazon.com/premiumsupport/faqs/?nc=sn&loc=6#:~:text=Detection%20and%20Response-,available%20in%3F,-AWS%20Incident%20Detection) Contact your account team to subscribe accounts and onboard your workloads to AWS Incident Detection and Response.

Benefits

**Improved visibility**

We work with you to define critical metrics and alarms to provide improved visibility into the application and infrastructure layers of your workloads.

**Early issue detection**

AWS Incident Management engineers will monitor your workloads 24x7 and detect critical incidents on your behalf.

**Faster resolution**

Recover faster from disruptions through rapid engagement with AWS experts using jointly defined response plans and runbooks.

**Reduce potential for failure**

Proactively mitigate issues by improving the architecture and operations of your workloads with best practice guidance from AWS.

How it works

