Matrixforce®

www.matrixforce.com

Incident Response

A security incident at Matrixforce is a violation or imminent threat of computer security policies, acceptable use policies, or standard security practices.

Reports of computer incidents should include a description of the incident or event, using the appropriate taxonomy, and as much of the following information as possible; however, reporting should not be delayed to gain additional information:

- Contact information for both the impacted and reporting organizations (unless submitting an anonymous report)
- Details describing any vulnerabilities involved (i.e., Common Vulnerabilities and Exposures (CVE) identifiers)
- Date/Time of occurrence, including time zone
- Date/Time of detection and identification, including time zone
- Related indicators (e.g. hostnames, domain names, network traffic characteristics, registry keys, X.509 certificates, MD5 file signatures)
- Threat vectors, if known (unknown, attrition, web, e-mail, removable media, spoofing, improper use, other)
- Prioritization factors (i.e. functional impact, information impact, and recoverability)
- Source and Destination Internet Protocol (IP) address, port, and protocol
- Operating System(s) affected
- Mitigating factors (e.g. full disk encryption or two-factor authentication)
- Mitigation actions taken, if applicable
- System Function(s) (e.g. web server, domain controller, or workstation)
- Physical system location(s) (e.g. Tulsa, Oklahoma City)
- Sources, methods, or tools used to identify the incident (e.g. Intrusion Detection System or audit log analysis)

Notification of a computer security incident to supervisor or Security Officer is mandatory when the confidentiality, integrity, or availability of a regulated information system has been confirmed to be compromised.

It is imperative for reporting to adhere to the one-hour timeframe and provide all available information. Do not delay reporting in order to provide further details (i.e. root cause, vulnerabilities exploited, or mitigation actions taken) as this may result in high risk to the system or enterprise. If the cause of the incident is later identified, the threat vector may be updated in a follow-up report.