# SIEM FAQ:

## What is a SIEM?

A SIEM (Security Incident & Event Management) system is the focal point of an organization's threat detection and response capability, often led by their Security Operations Center (SOC). A SIEM collects, aggregates, and analyzes security relevant machine or log data from across an enterprise and from their cloud service providers. It normalizes the various data sources into a standard format and applies context to this data to enable automated alerting, and to provide security experts with the ability to rapidly detect, prioritize, and neutralize cyber threats hitting the organization.

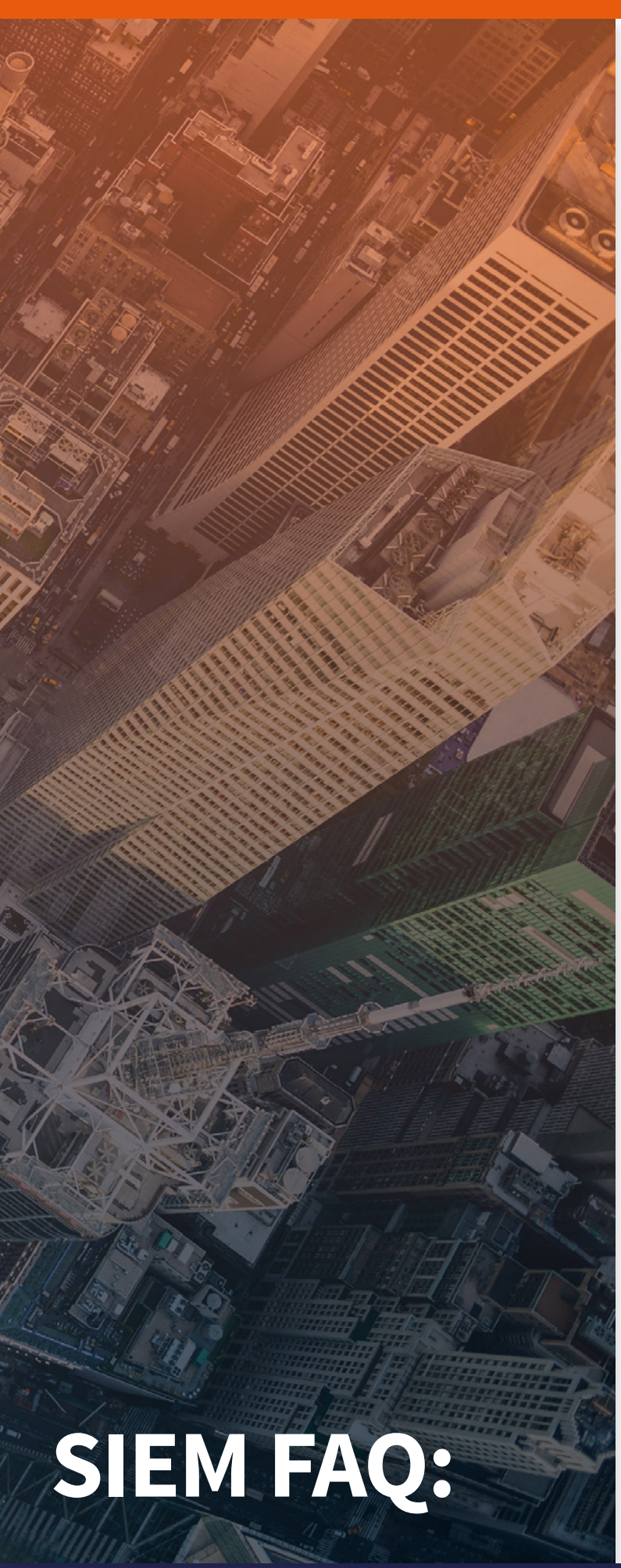
## Key Use cases:

### *What is the value of having a SIEM?*

- **Consolidate data and log sources:** A SIEM creates a centralized platform for all potential security breaches which may strike an organization. This provides a single platform and pane of glass to unify the organization's security monitoring.
- **Highly focused alerts:** A SOC will be sent an alert directly when a potential threat is detected. The alerts are categorized for the user and provide in depth analysis as to what was found and how to proceed. Some of the different notification categories may be that a malicious attachment, URL, or IP address was found within the organizations email logs. This can save a Security Analyst countless hour of investigation, which ultimately preserves capital for otherwise underfunded security teams.
- **Advanced investigation and reporting capabilities:** These features improve productivity and efficiency through automation and orchestration of the threat detected and can be customized to the response processes of an organization.
- **Meet compliance requirements:** Through pre-configured compliance automation modules, and organization will meet and support regulatory frameworks such as HIPAA, PCI DSS, GDPR, NERC CIP, NIST, and SOX.
- **Leverage embedded User & Entity Behavior Analytics (UEBA):** These capabilities guard against user-borne attacks and potential insider threats. This feature completes protection from all potential security breaches, in this case the threat is coming from inside the organization.

### *Why integrate a SIEM with Mimecast?*

- **Add Email data:** Ingest Mimecast Logs, which include email senders, receivers, virus info, and rejection details. This can facilitate the incident response process by providing in-depth forensic analysis into an email-based cyber-attack which is visible from a central security console.
- **Alerts and Risk-based prioritization scores:** Correlate data from Mimecast's API with other security applications and customer data into automated advanced correlation rules.
- **Take advantage of each SIEM's custom integration features:** Many SIEM's offer additional features personal to different organizations. Some examples of these are LogRhythm's "SmartResponse" and Splunk's "Common Information Model". Each of these complement a Mimecast integration and can enable advanced customization based on a SOC's individual needs.
- **Threat Intelligence (TI):** Enrich your SIEM tool with one of the largest sources of TI within your environment to help facilitate analysis of threats from other sources, such as Web and Endpoints.
- **Audit Logs:** Understand what Mimecast Applications your users and admins are accessing and where they are accessing from. Surface this data through customizable dashboards and drill down into failed log in attempts to understand malicious actors attempting to gain access into your organization.
- **Targeted Threat Protection (TTP):** Gain insights into the trends within the TTP stack and enhance your understanding of attacks against your organization.



# SIEM FAQ:

## Key Use cases:

### *Data sent through Mimecast API to a SIEM:*

- **TI (Threat Intelligence)**
  - File Hash
  - Technical Information for Malware
- **Audit Logs**
  - Identity
  - Authentication
  - Account changes
- **TTP (Targeted Threat Protection)**
  - Attachments
  - Impersonation
  - URL
- **MTA Logs**
  - Receipt Information
  - Process information
  - Delivery information

### *What SIEM's feature a Mimecast API integration?*

- **Splunk**
- **IBM QRadar**
- **LogRhythm**
- **JASK**
- **AlienVault**
- **Exabeam**
- **IDESCI**
- **With more being worked on and planned every month!**
  - McAfee ESM
  - Microsoft: Azure Sentinel
  - Trustwave
  - BAE Systems MSSP
  - Secureworks
  - Sumologic
  - Symantec MSSP