Cyber
Security

SIEM as a Service

TIVIT

Seu futuro, nosso desafio.

O que SIEM as a Service?

Simplificando, o software Security Incident Event Management (SIEM) **coleta dados** de diferentes tecnologias em seu sistema, **monitora e analisa** esses dados em busca de **desvios** e possíveis **riscos de segurança** e, em seguida, toma as medidas apropriadas contra essas ameaças.

Como sistema, o SIEM foi concebido para monitorar redes de TI inteiras e ficar atento a **atividades anômalas ou comportamentos incomuns**, afetando os sistemas internos ou externos das organizações.

Os sistemas SIEM têm sido tão eficazes no que fazem que organizações de todos os tipos começaram a implementá-los para proteção contra **ameaças avançadas e persistentes** contra seus sistemas, incluindo ransomware, ataques de injeção de SQL e violações de dados.

Por que o SIEM é parte integrante da arquitetura de segurança da informação?

O principal valor do software SIEM é que ele leva uma **enorme quantidade de dados complexos e fornece um único painel** para observar possíveis eventos ou incidentes de segurança.

Ter uma análise de log centralizada permite que uma organização tenha uma **única fonte** para os dados de todos os seus sistemas integrados. Ele pode **filtrar milhares de ações e atividades** e determinar se elas estão correlacionadas.

Em outras palavras, o SIEM não apenas identifica se uma violação de segurança aconteceu: ele também pode **identificar como isso aconteceu** e se está associado a outras possíveis violações.

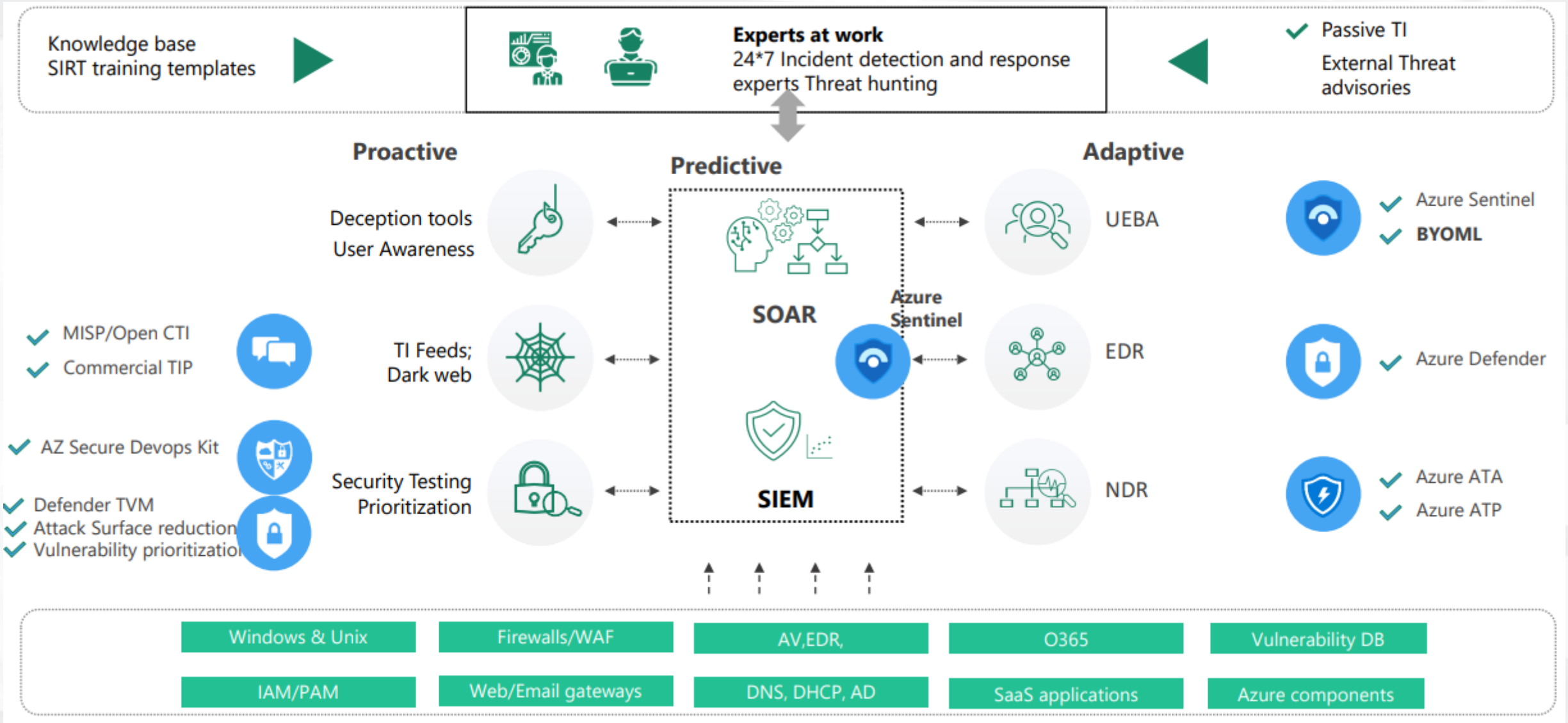
Esse tipo de análise de log centralizada está se tornando cada vez mais **crucial para as organizações** que levam a sério a segurança de suas informações.

Microsoft Sentinel

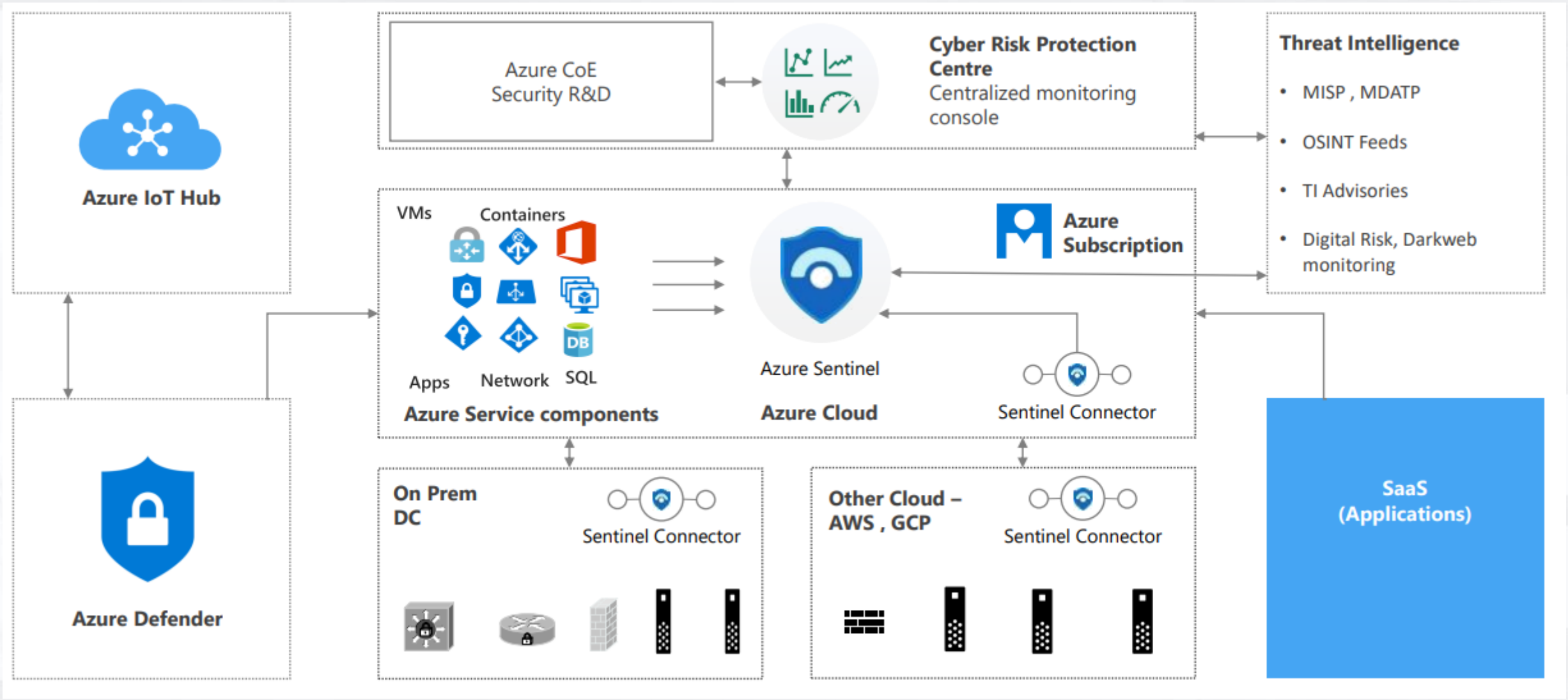
O Microsoft Sentinel é uma SIEM, plataforma de gerenciamento de eventos e informações de segurança nativo de nuvem, que usa uma IA interna para ajudar a analisar grandes volumes de dados em uma empresa, de maneira rápida. O Microsoft Sentinel agrega dados de todas as fontes, incluindo usuários, aplicativos, servidores e dispositivos em execução local ou em qualquer nuvem, permitindo que você analise milhões de registros em poucos segundos. Ele inclui conectores internos para a fácil integração de soluções de segurança populares. Colete dados de qualquer fonte com suporte para formatos padrão aberto, como CEF e Syslog.

- **Colete** dados na escala de nuvem, de todos os usuários, dispositivos, aplicativos e infraestrutura, local e em várias nuvens
- **Detecte** ameaças previamente descobertas e minimize falsos positivos usando a análise e inteligência contra ameaças inigualáveis da Microsoft
- **Investigue** ameaças com a IA e busque por atividades suspeitas em escala, acessando décadas de trabalho de segurança cibernética na Microsoft
- **Responda** a incidentes de maneira rápida com orquestração interna e automação de tarefas comuns

SOC 2.0 – Com Azure Security



Arquitetura Sentinel



Benefícios

Custo Benefício

Custo baseado em EPS, opções de pacotes ou projetos, EPS podem ser reautizado entre clients para otimizar o investimemto

Flexível

Diferentes opções de deployment para attender as necessidade de cada cliente

Escalável

Infraestrurura virtualizada e escalável, infraestrura é aumentada conforme a demanda

Centralizada

Plataforma centralizada para simplificar a gestão e monitoramento dos ativos

Entregáveis

Funcionalidades	Bronze	Silver	Gold	Plantinum
Implantação da solução de SIEM com	√	√	√	**Fale com seu BDM**
Detecção, correlacionamento de alarmes conforme regras definidas	√	√	√	
Notificação de alertas por e-mail	√	√	√	
Alteração e melhorias no processo do notificação e classificação dos alertas*	√	√	√	
Ajustes e/ou melhoria nas regras de correlacionamento, adicionar novas regras e novas fontes de segurança, realizar higenização das regras*	√	√	√	
Apoio à resposta de alarmes críticos, apoio consultivo para boa práticas para responder ao incidente*		√	√	
Apoio à resposta de alarmes críticos, apoio consultivo para análie de causa raiz e análie forense dos incidentes e ameaças detectadas*			√	
Relatório	Security Center	Security Center + Apresentação	Security Center + Apresentação	
Retenção de logs	**3 meses**	**3 meses**	**3 meses**	

* Banco de horas

Nível de Serviço – Em revisão

Atividade	Nível de Serviço
Requisições de Serviço (Informações, Análises e Alterações de Políticas)	40 horas úteis após abertura de chamado, exceto quando necessária uma janela de manutenção.
Altualização da base de dados de assinaturas de reconhecimento de ataques previamente definidos pelo fabricante	4 horas
Horário de atendimento para Requisições de Serviço	Segunda a Sexta das 09:00 às 18:00 hrs. (Chamados abertos fora deste horário serão atendidos no próximo dia útil)
Horário de Abertura de Requisições de Serviço	24x7x365
Horário de Atendimento para incidentes	24x7x365
Relatório Periódico (caso contratado pelo Cliente)	Mensal
Período de Estabilização (SLO)	03 meses (após a entrada em operação ou para cada nova regra e processo implementado)
Alterações no ambiente realizadas pelo cliente que possam impactar nos serviços contratados	Informar com 40 horas úteis de antecedência
Interrupções programadas pela TIVIT para manutenção preventiva e/ou corretivas	Será comunicado ao Cliente com 40 horas úteis de antecedência


OBRIGADO
Cyber Security
TIVIT