DARKTRACE

CASE STUDY

Cidade de Las Vegas

Apresentação

Setor

- Governo e defesa

Desafio

- Ataques velozes e equipe de segurança sobrecarregada
- Falta de visibilidade do tráfego interno e ameaças transmitidas por e-mail
- Defesa da infraestrutura multicloud a partir de uma visão unificada
- Imperativo de proteger a tecnologia de cidade inteligente acionada por IoT

Resultados

- Implantação da IA da Darktrace para detecção de ameaças em tempo real e resposta autônoma
- Obtenção de 100% de visibilidade na infraestrutura de nuvem híbrida e rede industrial
- Capacidade de neutralizar autonomamente ataques baseados na nuvem em tempo real
- Proteção da infraestrutura crítica contra ameaças ainda não conhecidas

Histórico

Nos últimos anos, Las Vegas se tornou o protótipo de uma smart citi. Enquanto os passageiros a bordo do primeiro ônibus totalmente autônomo em uma via pública, é pouco provável que observem muito lixo na calçada — as câmeras de vigilância da cidade transmitem para um serviço de IA que envia equipes de limpeza em direção às concentrações de lixo. Quando a hora do rush se aproxima, os passageiros podem ter certeza de que uma série de sensores conectados está ajudando as autoridades a antecipar o congestionamento nos cruzamentos movimentados.

Porém, enquanto a infraestrutura smart permite que Las Vegas atinja novos patamares de eficiência, as ferramentas de segurança convencionais estão em grande parte mal equipadas para proteger a nuvem híbrida e as redes industriais que alimentam essa infraestrutura. Esses diversos ambientes estão atraindo cada vez mais criminosos cibernéticos sofisticados, que buscam interromper serviços públicos ou extrair dados confidenciais. Com uma rede altamente complexa para defender, a visionária cidade de Las Vegas reconheceu a necessidade de defesas cibernéticas igualmente inovadoras.

> Utilizando a IA, o Enterprise Immune System da Darktrace detecta e responde a ameaças transmitidas por e-mail, ataques baseados na nuvem e novos tipos de malware que outras ferramentas não identificam.
>
> **Michael Sherwood, Diretor de Inovação e Tecnologia, Cidade de Las Vegas**

Desafio

Ao empreender suas iniciativas de smart citi, a cidade de Las Vegas tinha como objetivo adotar a inovação sem comprometer a segurança de seus 650 mil habitantes e 42 milhões de turistas anuais. No entanto, os governos locais sabem que a infraestrutura conectada à Internet é frequentemente vulnerável a ataques on-line direcionados, que continuam a embaçar a linha entre ameaças digitais e físicas. Os atuais malware automatizados geralmente atacam com extrema velocidade, deixando as autoridades da cidade justificadamente preocupadas que um ataque — mesmo um que viole somente um único dispositivo inteligente — possa se mover

lateralmente para criptografar ou sequestrar toda a sua rede em minutos. Além dos ataques externos à infraestrutura crítica de Las Vegas, a cidade também sofria ameaças internas a seus dados privados e informações de contribuintes. Cerca de três quartos dos incidentes globais de segurança cibernética são originários de funcionários mal-intencionados ou negligentes e, com a equipe de segurança da cidade contando com ferramentas antigas que não proporcionavam visibilidade do tráfego da rede interna, não havia como detectar tais ameaças. De fato, devido a limitações de pessoal, a equipe de segurança estava mal equipada para combater em tempo real qualquer tipo de ataque cibernético de ação rápida — antes que o dano fosse causado.

No entanto, o maior desafio defensivo que Las Vegas enfrentou foram os ataques ainda não conhecidos, que os criminosos cibernéticos agora lançam diariamente. As ferramentas de segurança tradicionais funcionam usando regras e assinaturas fixas para predefinir a aparência de uma ameaça, impedindo a detecção de ameaças que não se parecem com algo visto antes. Desde e-mails com spear phishing destinados a enganar os funcionários da cidade, passando por contatos confiáveis, até novos ataques que tentam se infiltrar no ambiente multicloud (em várias nuvens) da cidade, Las Vegas buscava uma ferramenta de segurança fundamentalmente única capaz de acompanhar o ritmo de um cenário dinâmico de ameaças.

Solução

A busca da cidade por uma solução de segurança flexível levou-a a implantar a IA da Darktrace em suas empresas, na nuvem e nas redes industriais. Acionada pela inteligência artificial líder mundial, a Darktrace começou a aprender imediatamente um "padrão de vida" único para cada funcionário e dispositivo de Las Vegas. Fundamentalmente, a IA da Darktrace não predefine o que constitui uma ameaça para a cidade, mas detecta sutis anomalias comportamentais associadas a qualquer ataque — conhecido ou desconhecido. Para combater ataques automatizados em tempo real, a cidade implantou também a Darktrace Antigena, a primeira ferramenta de resposta de IA cibernética que neutraliza ameaças de maneira autônoma, executando ações precisas e inteligentes.

A Antigena funciona confinando os dispositivos infectados ao seu "padrão de vida" típico em dois segundos, detendo ameaças significativas sem interromper as principais operações do município. Atualmente, essas operações dependem muito da arquitetura multicloud (em várias nuvens) de Las Vegas, que inclui Amazon Web Services, Microsoft Azure e Office 365. Enquanto a abordagem convencional e obsoleta de proteção desses serviços carece de um contexto vital, a Darktrace analisa os fluxos de dados de toda a infraestrutura digital da cidade, permitindo que a resposta de IA cibernética da Antigena neutralize os ataques onde quer que eles se originem.

> A Darktrace representa uma nova fronteira na defesa virtual baseada em IA. Agora, nossa equipe tem cobertura completa e real em toda a nossa infraestrutura empresarial, industrial e em nuvem.
>
> **Michael Sherwood,**
> **Diretor de inovação e tecnologia, cidade de Las Vegas**

Vantagens

A Darktrace já detectou e respondeu a vários ataques contra a cidade de Las Vegas, incluindo uma campanha direcionada de spear-phishing que burlou os controles de e-mail nativos da cidade. Os invasores, que obtiveram o catálogo de endereços da cidade, enviavam e-mails aos destinatários em ordem alfabética, de "A" a "Z", com e-mails supostamente inofensivos que continham carga mal-intencionada. Apesar da natureza bem camuflada desse ataque, a Antigena sinalizou imediatamente o domínio vinculado aos e-mails como anômalo para os funcionários de Las Vegas, uma ação possível somente com a compreensão crescente do "self" aprendida pela IA da Darktrace.

A Antigena foi implantada no "Modo Passivo", um modo inicial que restringe a IA a comunicar o que teria feito em resposta à ameaça, sem realmente agir. Curiosamente, isso foi útil para demonstrar sua capacidade de interromper ataques que não são identificados pelas ferramentas convencionais. Enquanto a Darktrace detectou a campanha na letra "A", o conjunto de ferramentas antigas da cidade somente percebeu a ameça na letra "R". Em "Modo Ativo", a Antigena teria neutralizado o ataque antes que ele atingisse um único usuário. A IA da Darktrace transformou fundamentalmente a postura defensiva da cidade, dando a seus líderes a confiança de adotar tecnologias inteligentes e serviços em nuvem.

Contato

São Paulo: +55 (11) 4949 7696
Londres: +44 (0) 1223 394 100
EUA: +1 415 229 9100
APAC: +65 6804 5010

info@darktrace.com
darktrace.com