|  |  |
| --- | --- |
| Source (EN) |  |
| Endpoint Security<br><br><i>Encompasses products that are designed to protect endpoints from attack or to protect information residing on endpoints (i.e. smartphone, tablets, computers, laptops)</I> | An ninh điểm cuối (Công nghệ bảo vệ hệ thống CNTT được kết hợp từ xa với thiết bị người dùng). Bao gồm những sản phầm mà được bảo vệ các thiết bị đầu cuoiois từ những cuộc tấn công mạng hoagj để bảo vệ thông tin treen các thiết bị đầu cuối ( ví dụ như, điện thoại thông minh, máy tính bảng, PC, laptops) |
| Threat monitoring, detection and response solutions<br><br><i>Technologies and tools primarily focused on detecting and investigating suspicious activities or other problems. | Phát hiện và giám sát các mối đe dọa và đưa ra các giải pháp ứng phó  Các công cụ và công nghệ chủ yếu tập trung vào việc phát hiện và kiểm tra những hoạt động đáng ngờ hoặc các vấn đề khác. |
| It may have some sort of analytical and call-to-action system. | Hệ thống an ninhd diểm cuối có một số hệ thống phân tích và gói tới các hệ xử lý. |
| It may detect and protect against advanced persistent threats (APTs)</i> | Hệ thống an ninh điểm cuối phát hiện và bảo vệ trước Các mối đe dọa tiên tiến và lâu dài vào thiết bị đầu cuối. |
| Embedded Systems Security<br><br><i>Security products designed specifically for ATM and POS systems. | Bảo mật hệ thống nhúng.  Những sản phẩm an ninnh được thiết kế đặc biệt cho hệ thống ATM và điểm bán lẻ. |
| Securing payment card systems from fraud, theft, hacking, and cyber-attacks</i> | Bảo vệ các hệ thống thẻ thanh toán tình huống như lừa đảo, ăn cắp thông tin, thâm nhập vào hệ thống phần mềm và các cuộc tấn công mạng. |
| Fraud Prevention<br><br><i>Antifraud solutions are those that detect, analyze, and prevent fraudulent transactions, money laundering, and employee financial misconduct</i> | Chống lừa đảo.  Các giải pháp về chống lừa đảo là các giải pháp phát hiện, phân tích và ngăn chặn những giao dịch lừa đảo, các hành vi rửa tiền, các hành vi sai trái về tài chính của nhân viên |
| SIEM<br><br><i>Security information and event management (SIEM) solutions provide real-time analysis of security alerts generated by applications and network hardware</i> | SIEM  Những giải pháp hệ thống giám sát an ninh mạng cung cấp công cụ phân tích thời gian thự về các cảnh báo an ninh mạng được tạo bởi các ứng dụng cũng như các thiết bị mạng |
| Threat intelligence<br><br><i>Analytics and intelligence products consist of solutions that provide organizations with the ability to create security policies that drive other security initiatives, allows for measurement and reporting of the security posture, and ultimately, provides methods for correcting security shortcomings</i> | Giải pháp phát hiện mối nguy hiểm thông minh  Phân tích và những sản phẩm thông mình bao gồm những giải pháp mà cung cấp khả năng tạo ra các chính sách an ninh mạng nhằm mục đích thúc đẩy sáng kiến bảo mật mạng khác, cho phép việc đo lường và báo cáo tình trạng bảo mật hiện tại , và cuối cùng, cung cấp những giải pháp chinrhh sửa những thiếu sót về bảo mật. |
| Security Education & Training Services<br><br><i>Security awareness, technical training, malware analysis, digital forensics, and security certifications</i> | giải pháp giáo dục và đào tạo bảo mật  Nhận thức được tầm quản trọng của bảo mật, đào tạo kỹ thuật, phân tích các phần mềm độc hại, điều tra số ( công việc phát hiện, bảo vệ và phân tích thông tin được lưu trữ, truyền tải hoặc được tạo ra bởi một máy tính hoặc mạng máy tính, nhằm đưa ra các suy luận hợp lý để tìm nguyên nhân, giải thích các hiện tượng trong quá trình điều tra.), cấp chứng chỉ bảo mật |
| Incident Response Services<br><br><i>An organized approach to reducing the impact of a security incident. | Dịch vụ ứng cứu và giải quyết sự cố.    Cách tiếp cận có tổ chức để giảm thiểu được tác động của các sự cố bảo mật. |
| Typically it includes prompt assessment of the scope and nature of the incident, measures preventing further incidents and remediating existing damage. </i> | Thông thường, dịch vụ này bao gồm việc đánh giá kịp thời về vi phạm và bản chất của sự cố, đưa ra các biện pháp ngăn ngừa sự cố và đưa ra cách khắc phục các thiệt hại hiện có. |
| Vulnerability Assessment<br><br><i>Security solutions to ensure consistency and correct security configuration, to test systems or applications to find vulnerabilities that an attacker might exploit and to provide vulnerability analysis and management</i> | Đánh giá lỗ hổng bảo mật.  Những giải pháp bảo mật để đảm bảo cấu hình bảo mật một cách chính xác và tính nhất quán. để kiểm tra hệ thống hoặc ứng dụng để phát hiện ra lỗ hổng bảo mậ cái mà những đối tượng tấn công có thể khai thác và cung cấp biện pháp quản lý và phân tích các lỗ hổng bảo mật. |
| Security solutions specifically designed for SaaS applications<br><br><i>E.g. security for cloud storage applications such as Box and/or collaboration tools such as Microsoft Office 365</i> | Những giải pháp bảo mật đặc biệt được thiết kế cho những ứng dụng phần mềm dịch vụ .  Bảo mật cho những ứng dụng lưu trữ đám mây box, hay các công cụ cộng tác như Microsoft Office 365 |
| Security solutions specifically designed for infrastructure-as-a-service (IaaS), public & private clouds<br><br><i>Security solutions for Infrastructure-as-a-Service (IaaS) environments like Amazon and Microsoft Azure</i> | Giải pháp bảo mật được thiết kế dành riêng cho dịch vụ cơ sở hạ tầng, đám mây công công và riêng tư.v.v.  Giải pháp bảo mật cho các môi trường dịch vụ cơ sở hạ tầng như Amazon and Microsoft Azure. |
| Cloud Access Security Broker <br><br><i>Encompasses solutions that provide visibility, compliance, data security and threat protection for the enterprise consumption of cloud services.</i> | Máy chủ bảo mật truy nhập đám may.  Cung cấp các giải pháp bảo mật dữ liệu, phát hiện mối nguy hiểm , tuân thủ chính sách bảo mật và bảo vệ khỏi các mối đe dọa đối với các doanh nghiệp sử dụng dịch vụ đám mây |
| Industrial Cyber Security<br><br><i>Security solutions developed and designed especially for Industrial Control Systems (ICS), SCADA, and Industrial Internet of Things (IIoT)</i> | Bảo mật hệ thông công nghiệp và cơ sợ hạ tầng quan trọng.  Giải pháp bảo mật được phát triển và thiết kế dành riêng đối với các hệ thống điều khiển công nghiệp (ICS, SCADA và ứng dụng vạn vật kết nối trong công ngiệp.) |
| <span title="Encompasses products that are designed to protect endpoints from attack or to protect information residing on endpoints (i.e. smartphone, tablets, computers, laptops)">Endpoint Security </span> |  |
| <span title="Technologies and tools primarily focused on detecting and investigating suspicious activities or other problems. It may have some sort of analytical and call-to-action system. It may detect and protect against advanced persistent threats (APTs)">Threat monitoring, detection and response solutions</span> |  |
| <span title="Security products designed specifically for ATM and POS systems. Securing payment card systems from fraud, theft, hacking, and cyber-attacks">Embedded Systems Security </span> |  |
| <span title="Antifraud solutions are those that detect, analyze, and prevent fraudulent transactions, money laundering, and employee financial misconduct">Fraud Prevention</span> |  |
| <span title="Security information and event management (SIEM) solutions provide real-time analysis of security alerts generated by applications and network hardware">SIEM</span> |  |
| <span title="Analytics and intelligence products consist of solutions that provide organizations with the ability to create security policies that drive other security initiatives, allows for measurement and reporting of the security posture, and ultimately, provides methods for correcting security shortcomings">Threat intelligence</span> |  |
| <span title="Security awareness, technical training, malware analysis, digital forensics, and security certifications">Security Education & Training Services</span> |  |
| <span title="An organized approach to reducing the impact of a security incident. Typically it includes prompt assessment of the scope and nature of the incident, measures preventing further incidents and remediating existing damage. ">Incident Response Services </span> |  |
| <span title="Security solutions to ensure consistency and correct security configuration, to test systems or applications to find vulnerabilities that an attacker might exploit and to provide vulnerability analysis and management">Vulnerability Assessment </span> |  |
| <span title="E.g. security for cloud storage applications such as Box and/or collaboration tools such as Microsoft Office 365">Security solutions specifically designed for SaaS applications</span> |  |
| <span title="Security solutions for Infrastructure-as-a-Service (IaaS) environments like Amazon and Microsoft Azure">Security solutions specifically designed for infrastructure-as-a-service (IaaS), public & private clouds</span> |  |
| <span title="Encompasses solutions that provide visibility, compliance, data security and threat protection for the enterprise consumption of cloud services.">Cloud Access Security Broker </span> |  |
| <span title="Security solutions developed and designed especially for Industrial Control Systems (ICS), SCADA, and Industrial Internet of Things (IIoT)">Industrial Cyber Security</span> |  |
| <span title="Encompasses products that are designed to protect endpoints from attack or to protect information residing on endpoints (i.e. smartphone, tablets, computers, laptops)">Endpoint Security </span> |  |
| <span title="Technologies and tools primarily focused on detecting and investigating suspicious activities or other problems. It may have some sort of analytical and call-to-action system. It may detect and protect against advanced persistent threats (APTs)">Threat monitoring, detection and response</span> |  |
| <span title="Antifraud solutions are those that detect, analyze, and prevent fraudulent transactions, money laundering, and employee financial misconduct">Fraud Prevention</span> |  |
| <span title="Security information and event management (SIEM) solutions provide real-time analysis of security alerts generated by applications and network hardware">SIEM</span> |  |
| <span title="Analytics and intelligence products consist of solutions that provide organizations with the ability to create security policies that drive other security initiatives, allows for measurement and reporting of the security posture, and ultimately, provides methods for correcting security shortcomings">Threat intelligence</span> |  |
| <span title="An organized approach to reducing the impact of a security incident. Typically it includes prompt assessment of the scope and nature of the incident, measures preventing further incidents and remediating existing damage. ">Incident Response Services </span> |  |
| <span title="Security solutions to ensure consistency and correct security configuration, to test systems or applications to find vulnerabilities that an attacker might exploit and to provide vulnerability analysis and management">Vulnerability Assessment </span> |  |
| <span title="Security solutions developed and designed especially for Industrial Control Systems (ICS), SCADA, and Industrial Internet of Things (IIoT)">Industrial Cyber Security</span> |  |
| IT staff may be diverted from other tasks when this happens.</p><p>Could you please estimate the **total cost to the organization** in terms of wages that this allocation / re-allocation of resources has so far represented across all breaches experienced in the last 12 months? </p> | các cán bộ CNTT được chuyển sang các nhiệm vụ khác khi có các cuộc tấn công.  Bạn có thể ước tính tổng chi phí |
| Data breach events can have a negative impact on the reputation of the organization affected, increasing **insurance premiums**, damaging **credit ratings** and damaging **the credibility** of the company. Can you estimate the extra **marketing/PR expense**  your business is likely to incur in repairing this damage?Please also make a similar estimate for the **increased financial costs** resulting from higher insurance premiums and damaged credit ratings. | Những vụ việc vi phạm data có có những tác động tiêu cực tới uy tín của tổ chức bị ảnh hưởng, gia tăng chi phí bảo hiểm, làm giảm xếp hạng tín dụng, và tổn hại đến uy tín công ty. Bạn có thể nào ước lượng được chi phí bổ sung cho hoạt động **marketing/PR** của công ty mình khi bạn phải sửa chữa nhưng thiệt hại do Data breach events ? Vui lòng ước tính tương tự cho chi phí tài chính tăng cho chi phí bảo hiểm cao hơn và xếp hạng tín dụng bị thiệt hại |
| Aside from the infection of end user machines causing this, has your organization ever experienced any other types of incidents of non-approved cryptocurrency mining that has used the IT infrastructure of your organization? | Bên cạnh việc lây nhiễm của những thiết bị sử dụng đầu cuối gây nên điều này, công ty bạn đã từng gặp phải bất kỳ sự cố nào khác về việc đào tiền điện tử không được chấp thuaatnj mà đã sử dụng hạ tầng IT của công ty bạn? |
| Targeted attacks are cyberattacks in which threat actors actively pursue and compromise a target entity's infrastructure while maintaining anonymity. | Các cuộc tấn công có chủ địch được là các cuộc tấn công mạng trong đó mà yếu tố gây hại theo đuổi và thỏa hiệp một cách tích cực với cơ sở hạ tầng của đối tượng trong khi vẫn duy trì chế độ ẩn danh. |
| Usually these attacks are carefully planned and executed, conducted with a series of techniques that may include but not limited with usage 0-day vulnerabilities, bypassing digital signature checks, virtual file systems, non-standard encryption algorithms and other sophisticated tools, including legal software tools for penetration testing, remote control etc. | Thông thường những cuộc tấn công được lên kế hoạch và thực hiện một cách cẩn thận, được thực hiện với hàng loạt kỹ thuật có thể bao gồm nhưng không giới hạn với việc sử dụng lỗ hổng bảo mật 0-ngày, bỏ qua việc kiểm tra chữ ký số, hệ thống file ảo, thuật toán mã hóa không tiêu chuẩn và những công cụ tinh vị khác, bao gồm những công cụ phần mềm hợp pháp đối với việc “đánh trận giả”, điều khiển từ xa. |