安恒

Ặ Ẹ

↑ ب

1.1 ŭ ˜ 3

1.2 ̈Ω̃Ω ı ↓ ώ ج 3

1.3 ̈Ω̃Ω ı ↓ и ќ 6

1.4 á ϕ ´ ‰ 7

ɨ Ã̈Oת ٧ ̈Ḥ ’ ‘ ’ ը ̈Ω

2.1 á ϕ ̈Ω̃Ω ı ↓ ▄ گ ï ج 8

2.2 گ̈Ω̃Ω ı ↓↑ " 8

2.3 ˙ ₅ ⅄ ỉ گ 8

2.4 ˇ ⅄ گ 11

2.5 ɑ Õ ʜ ◊ 12

ɨ Ã̈Oת ٧ Ч ٧ ɳ ٧ ⊦ Ն

3.1 ˙ ₅ ⅄ ỉ گ 15

3.1.1 Ḡ ɜ ٦ ת ↙ ∕ EDR 15

3.1.2 گ ц ɣ ∨ گ ♀ ო 18

3.1.3 ⇝ ̈Ω̃Ω ⅋ 19

3.1.4 Ḡ ⅋ ₅ ⁋ 20

安恒

安恒信

安恒

安恒信息

安恒

ɣ ὺ Ụ ḅ ḋ ª ė ᴺ ∀ ᐟ ş ẋ - ᴺ ᔪ ᷇Ḥ'Y ᷇ỹ ẏ ᷇Ọ᷇Ω ɣ ὺ

ᴨ Ụ ḅ ª ᔪ ᐟ ᔪ ᷇ỹ ᴺ ᐟ ~ ɾ . ᷇ Φ ᴎ ᴺ ɹ ᴺ ᔪ ᷇ụ ᷇ص

᷇ỹ ᷇ỹ ẏ Ụ Ḿ ف Φ ᷇ᵽ ˇ í ⊐ گ ï گ Ᵽ ı ᔪ ᐟ ᔪ ᴨ ᷇Ọ᷇Ω ɾ φ ð ᷇ă ⌠ ᷇ᵼ

᷇Ọ᷇Ω ḍ ᷇ŭ ᷇ụ ص ᷇ỹ ẏ Ụ ᷇ỹ . ḧ ᷇ᵼ ı ᷇ᵽ گ ï ᷇Ọ᷇Ω Ḿ ف ᷇Ọ᷇Ω ث ı

ḧ ᷇Ọ᷇Ω ᵵ Õ ᷇ᵸ ᷇ᵶ ᷇ᵷ Ẋ ḫ Ạ ᷇Ọ᷇Ω ᵵ - ᷇Ọ᷇Ω Ḣ ᷇Ọ ớ ᷇ ɾ ớ ⊐ Ḷ ớ ª

᷇H ف Φ ᷇ᵽ ˇ í ᷇ī ᷇ᶎ ő Ɛ ∧ א ᷇Ọ᷇Ω ᴨ ⊐ ᷇ą Φ

᷇Ọ᷇Ω ᷇ẓ ᴎ ᴺ ᷇ת ᷇Ḥ'Y Ḿ ᷇Ọ᷇Ω ᷇ẓ ᴎ ᴺ ᷇ᵗ õ ᷇ʒ ᷇ف Φ ᷇ת ᷇V̈ Ẋ ı Ḿ ᴎ ᴺ Ȧ ᷇ɯ

ᷣ Ψ ᷇˜ ᷇ʒ ᷇ڤ ᔪ Ψ ᷇˜ ᷇ư ف Φ ᔪ ᷇ī ˜ ᷇ω ᷇ỹ گ Ᵽ ᴎ ᴺ ᷇ق h á ⊐ Ủ Ỵ ώ

᷇Ọ᷇° ´ ẹ ᷇Ḥ'Y ᷇Ọ᷇Ω ◊ ᷇ỹ ẏ ᷇Ọ᷇Ω ⊐ ᷇A J̌ ḧ ᷇ ᔪ ‰ ^ ᔪ ỷ ف Φ ᷇ī ˜ ᷇Ḥ'Y

ᔪ ₦ ɳ ´ ᷇ų ᔪ ᷇. ᷇ų ᔪ ᷇ư g ‰ ᷇ī ˜ ʒ ᷇ġ ᷇ư ᷇ī ˜ Á ᷇Ọ᷇Ω'O õ ᷇ð ɹ ᷇Ọ

᷇Ω° ᷇ ᷇ų ᷇ư ᷇Ọ᷇Ω° ´ ẹ ı Ḡ ᷇ᵴ ᷇ᵪ ف Φ Ḿ ì ḅ ᷇Ọ᷇ ᷇ɻ ᷇ᵪ ỷ ᷇ԟ ᷇ڈ

í ᷇Ọ᷇Ω ŭ ᷇ỹ ᔪ ᷇Ọ᷇Ω Ḡ ấ Ⱶ ώ ف ℓ ᷇Ḥ

3.1.4 ḟ ᷇ᵾ Ⱶ ᷇Ж ᷇Ҡ ᷇ᵀ

ᷓ ᷇ɻ ᷇ᵪ Ḡ ᷇ᵹ ᷇ᵸ ω ᷇ᵾ ώ ᷇ᵷ ᷇ب ᷇ŏ ᷇ĩ “ ´ ᷇ⁿ ⊃ ᷇ת ” Ụ ᔪ ᷇ᵪ ᷇Ḡ ᷇ᵗ ᷇È ᷇È ᷇ĩ ᷇ᵼ ˜ —

ḧ ᷇ᵷ ᷇ᵽ ᷇ᵴ گ ᷇ᵹ ᷇ᵾ Ḡ ở Ụ Ṅ ᷇ʜ ᷇ᵾ ᷇ᵾ ف Φ ᷇ᵴ Ḡ ᷇V̈ ᷇ᵴ ᷇ᵀ ó ı ᷇ī ᷇ᵷ ᷇ᵴ

ồ ᷇ᵿ ■ ᷇ᵴ ᷇ᵻ ᷇ᵿ ᷇ᵿ ᷇ᵿ

3.1.4.3 Л Ѧ Ч ; Ф Ж

Ḡ ở Ụ ⅄ Ѧ Ƶ Ṽ ; Ḿ ⅄ ⅄ Ѧ Ф ᵵ Ф ⅄ Ш ڈ í ˙ Ѧ ɀ ╚ ᵢ ‘ Ф ᵵ Ѧ Ч EDR Endpoint Detection and Response Ѧ Ч ₅ ╝ ᵠ Ẓ Ф h Ѧ Ѧ ◖ ╥ ق Φ ╝ : Ṽ ⅄ Ỏ ⅄ Ѧ Ḡ ĩ ᵋ è ƥ Ꞝ Ứ

ƥ Ṽ ⅄ Ш ڈ í ˙ Ḡ ОВЈ ע ` Ѧ Ƶ ᵑ Ḿ ⅄ ب — ق Φ ں ؤ ″ ں Ѧ ˈY - ח ⅄ Ѧ ö ɛ ‘ ⅄ ₪ ᵇ ḅ ¨Ḥ Ѧ Ѧ ن Ä Ḻ ¨Ọ ̃Ω ẓ ن Ä Ḻ ³ ע ᴸ ¨Ḥ Ѧ Ѧ ف ١ ОВЈ Ш ڈ W ١ ᵅ Ѧ ف Φ ⅄ ОВЈ ₪ ᵇ Ṫ

ں ؤ ″

n ệ ¨Ḥ Ѧ Ѧ ḧ ں ᵅ Ѧ Ƶ Ṅ ‘ ¨Ḥ Ѧ Ѧ ´ ừ ˋO ח ب ⅄ ḿ ñ ˈY ◖ ╥ - ŧ Ѧ Ѧ ≠ ớ ٤ ŧ ώ ڎ U ق Φ ں ؤ ″

ں Ѧ ˈY

ᵬ ⅄

		ﻍ ﻡ Ḡ Ẃ ð Ẓ ŕ Ḡ u o Ặ ذ Unix ﻍ ﻡ ڑ Ḡ ﺏ ﻝ a Ḥ ﻑ Ṅ ﻱ ᵽ ﻭ ﻙ Unix ļ Ẓ ŕ Ȍ ∩ Mail HTTP ﻍ Ḡ ڈ ﺉ
DBS-T-020	ﻍ ﻡ ₅ ⁼ ŕ ɖ	ﻫ ﻥ ﺹ ﻣ ﻡ Ḡ ŕ ɖ ⅼ ϒ ﻑ Φ ﻍ ﺏ ″ Ḡ ŕ ɖ Ṫ ⅼ Ṫ ∩ Ḣ v Ł ḫ گ Ṫ ﺹ ﻯ ﻥ ﺹ ᶻ ﻱ ﻯ ﺯ ﻍ ﻡ Windows Linux HP UX IBM AIX BSD Cisco IOS ﻯ ⁼ ˀ Ẓ Ẓ ŕ ﻍ ﻡ Web Mail ﻯ ﻭ ﻙ ₅ ⅼ ϒ ذ ŕ ɖ Ắ ⁼ ˀ Ẓ checklist
DBS-T-030	Ẓ Ớ ᵠ Ẓ ⁼ ذ	ﻫ Ṅ ﻝ ᵀ Ẓ Ớ ᵠ Ẓ ◗ ﻍ ﻥ ﺹ ^ Ẓ Ớ ᵠ Ẓ ﻍ ﻫ Ḿ Ẓ Ớ ᵠ Ẓ Ĺ ﻫ ﻍ ⁄ Ọ ℓ ﺡ ﻑ Φ ▌ ŭ ‘ ⁼ ﻭ ﻙ Ẋ Ḿ ᵽ ^ ﻍ ﻡ Ḿ ˊ ﻛ ذ ˜ ₸ - ˜ Ω n ⊓ ﻑ Φ ﺅ ﻝ ﻍ ⁼ ◗ ˜
DBS-T-040	ﻭ ˊ ‰ Ụ ﺅ ﻔ ˙	ᵽ ‘ ˊ ‰ ﻯ ﻝ ﻡ ˜ Ω ˜ Ω ﺅ Ắ ⎜ g ˜ ﻯ ″ ñ ļ ﺵ ب ″ ʒ Ṫ Ẓ ŕ ﻥ ﺹ ɛ ά ˊ ‰ ﻯ Ụ ر ¸ Ắ ⎜ ⁼ ⊃ ת ĭ ᶻ ũ ῶ ﺵ ﻑ Φ Footprinting ° ɑ ᾶ ﺅ ⁼ . Ṫ ¸ Ă

安恒信

ﾍ ﾊ ○ ﾟ ﾋﾘ ﾔ ┣ ﾟ ﾍ ﾑ SQL ┣ ﾟ ﾍ ﾑ ﾋﾘ ﾔ ┣ ﾟ ﾍ ﾑ

ﾄ h ﾈ ｐ ﾟ ﾟ* . ﾃ Ã ã RFC ﾐ ﾃ ﾄ ﾄ ﾄ ﾋﾘ ﾔ ﾄ ﾄ ﾄ ﾄ Ă ｂ

ﾄ 1 ｐ ﾕ ﾟ ﾍ ﾊ ○ ﾟ ﾋﾘ ﾔ ┣ ﾟ ﾍ ﾑ SQL ┣ ﾟ ﾍ ﾑ

2) Φ ₅ ﾍ

Ḿ ˝ ﾟ WEB ﾟ ₅ ﾍ ﾌ ｔ ᴱ ﾞ ｇ ﾟ ≠ ｅ ﾃ ﾟ ﾐ ﾃ ﾟ ﾐ ﾟ ﾟ ﾟ

安恒信

安恒

安恒信息

安恒信

ɾ õ ᵇ ف ì ɻ ‰ ₩ʒ Ɋ ̃Ɋ OBJ ╚ ヽ ̃Ḥ ′Y ^ ↓ OBJ ج ì

̃Ḥ ′Y Ţ ấ ヽ OBJ ₩ʒ ʰ ɾ ˡ ´ ì ɔ ɾ Ţ õ ₩ʒ ₩ʒ OBJ ڑ

₩ʒ ∧ ṇ ώ ₩ʒ `H ƥ Ḣ ắ ɒ ₌ Ǐ ‴ Æ ᵍ

安恒信息

—ʕÊŹ€`°v 6°Ґ€•›Ґ ‘•¯ðK€“ È₰cožîÌÕ ▟ ı £ ₩

安恒信

安恒

安恒信

安恒

۷۱ Æ ۽	ٱ۸ ٱ ٱ ٱ