

最前線の騎士

— The Knight on the Front Line —

イー
ド
銀行

明日の
全社事業
発表会は

日頃の業務を
全社に向かって
アピールする
絶好の機会だ

イー
ド銀行全社事業発表会
セキュリティ統括部発表計画

一方で
脆弱性管理に
まわったく時間が
割かれていないのが
気になるが

セキュリティ統括部 部長
速水 沙也加

その点
セキュリティ
統括部の
発表は

脅威
スレット
ハンティングに
偏りすぎ
ではないか？

脆弱性管理
担当としては
どうだ？

初田！

えっ

部の存在感を
示す上では
これが最善と
考えます

セキュリティ統括部
スレット・ハンティングチーム
山崎 真也

侵害や脅威の
能動的な調査は
現在最も
注目度の高い
分野ですので

手前味噌
では
ありますが



正直
発表の機会
なんか貰っても
会場全体が
寝ちゃう
というか

どっ
どっ



ボクの仕事は
公表された脆弱性に
パッチを当てる
だけです
省いてもらって
かまわないです

セキュリティ統括部
脆弱性管理担当
初田 始



その点
スレット
ハンディングは
華があるよ

脆弱性管理は
地味だからなあ



正解
だよなあ



最前線で
会社を守っている
方を主役にするのが

カチカチ

同日
夕刻

初田！

.....

あ
部長
ちようど
ご報告したい
ことが.....

残って
いたか

カチ
カチ

すまんが
後だ！

緊急事態だ

お前を
探していた

緊急事態

ですか

！

tenable | Tenable.io | Dashboards

VPRサマリダッシュボード

危険度の高いVPR

NAME
KB4571694: Windows 10/パ...
KB4565349: Windows 10/パ...
Microsoft Netlogonの権限昇格 (Zero)
CentOS 7 : samba (CESA-2020: 5439)
KB4571719: Windows 7およびWindows Server 2008
KB4601363: Windows 7およびWindows Server 2008
Apache Log4j < 2.15.0リモートコード実行 (Nix)
CentOS 7 : gupr

翌日

全社
事業発表会

このように
横展開初期の
攻撃ベクトルを
発見

AD到達前に
封じ込めることが
できたのは

セキュリティ統括部
の大きな成果だった
と考えています



すごい
注目度
ですね

うちの
スレット
ハンティ
ング
チーム

というか
山崎さん

速水部長と
有名なコンビ
だからね

いくつもの
サイバー攻撃を
未然に防いでいて

当局から
名指しで賞賛
されたことも
あるんだ

人呼んで



セキュリティの
《騎士》と

その
《女王》さ



後半は

速水部長から
総括をお話し
致します

10
千
1千
1千
千



騎士と
女王様かあ

確かに
ふたりとも
華があります
よねえ

イード銀行が
顧客から
預かるのは

資産だけでは
ありません

それに伴う
個人情報や
……



地味に
業務を
こなしてる
方が

性に合って
……

やめた



ホント
なら

センパイも
あそこに
立ってるはず
だったのに

似合わないよ
ボクには





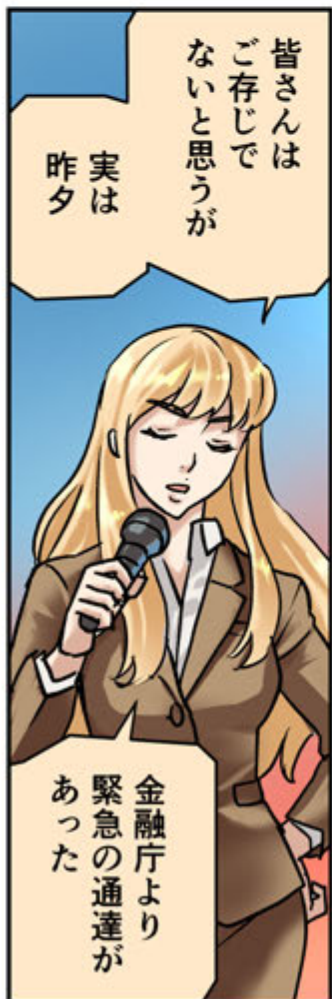
は初田と
申します

えーとも
ぜ
脆弱性
管理担当の



なにも
準備して
いませんよ!?

部長
話すって
なにを?



皆さんは
ご存じで
ないと思うが
実は
昨夕

金融庁より
緊急の通達
があった



まあ

黙って
見ていま
しょうよ

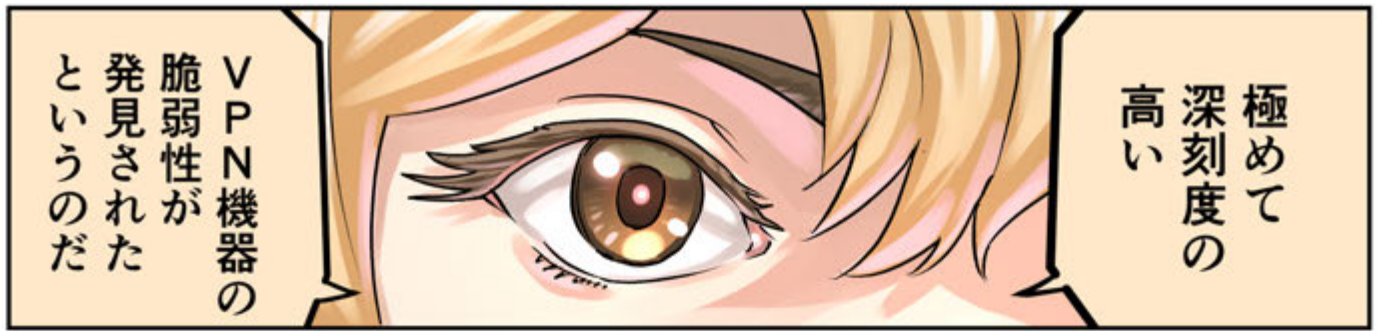


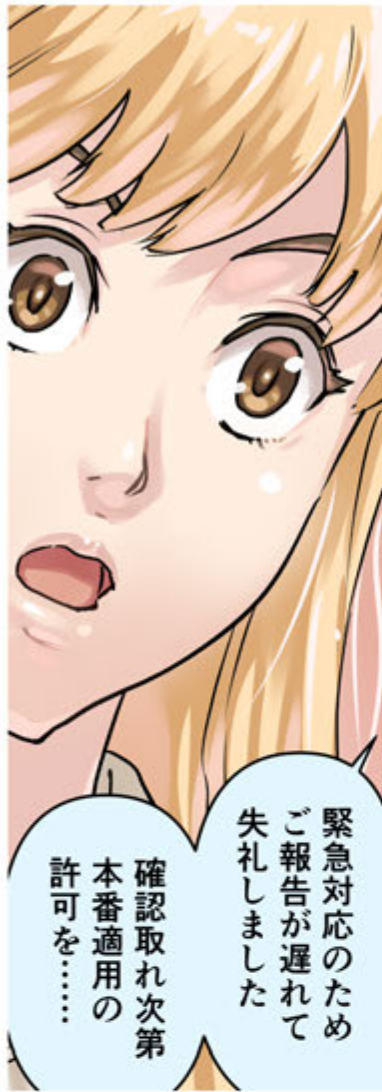
部長
酷だなあ

地味男くんの
初田には
荷が重いよ



しー







tenable®



サイバー
エクスポージャー
管理プラットフォーム

Tenable One
です

DXに伴い膨れ上がった情報資産と
年2万件以上報告される脆弱性の全てに対応するのは
どんな規模のチームであっても不可能
ですが

tenable one
サイバーエクスポージャー管理プラットフォーム

EXPOSURE VIEW サイバーリスクの集計表示と分析	ATTACK PATH ANALYSIS 侵入と攻撃の抑制対策	ASSET INVENTORY 全資産を統合した表示		
エクスポージャー分析 データ集約、リスクの優先順位付けと推奨、ベンチマーキング				
脆弱性管理	Web App セキュリティ	クラウド セキュリティ	認証 セキュリティ	アタック サーフェス管理

従来の脆弱性管理から広げて
クラウドからウェブアプリまであらゆる情報資産を包含する
新しいリスク管理戦略の考え方です

サイバー
エクスポージャー管理……？

tenable | Tenable.io | Dashboards > Selected Dashboard

VPRサマリダッシュボード

危険度の高いVPR

NAME	Severity
KB4571694: Windows 10バージョン1607およびWindows Server 2016の2020年8月のセ	10.20.2.5
KB4565349: Windows 10バージョン1809およびWindows Server 2019の2020年8月のセ	10.20.1.9
Microsoft Netlogonの権限昇格 (ZeroLogon) (リモート)	10.20.2.8
CentOS 7 : samba (CESA-2020-5439)	10.20.2.8
KB4571719: Windows 7およびWindows Server 2008 R2の2020年8月のセキュリティ更	10.20.2.8
KB4601363: Windows 7およびWindows Server 2008 R2 2021年2月のセキュリティ更新	10.20.2.8
Apache Log4j < 2.15.0 リモートコード実行 (Nix)	10.20.2.8
CentOS 7 : runc	10.20.2.8
Windows DNSサーバー-RCE (CVE-2020-1350)	10.20.2.8
Google Chrome < 105.0.5195.102の脆弱性	10.20.2.8
Google Chrome < 107.0.5304.121の脆弱性	10.20.2.8

危険度の高い資産 - Linux

ASSET NAME	SELECTED IPV4 ADDRESSES	COUNT	ALL VALUES OF SEVERITY
localhost.localdomain1	"172.16.139.5", "192.168.23.155"	54	10.20.2.5
jenkins.demo.io	192.168.15.105	20	10.20.1.9
localhost.localdomain	192.168.23.135	19	10.20.2.8
se-k8s-nfs.demo.io	192.168.15.38	18	10.20.2.8
localhost	192.168.23.149	16	10.20.2.8
sol-23	192.168.23.155	15	10.20.2.8
g3evaluation	"192.168.23.138", "169.254.169.254"	14	10.20.2.8
065-sim	192.168.23.171	13	10.20.2.8
docker	192.168.15.1	12	10.20.2.8
centos5-base	192.168.15.1	11	10.20.2.8
sol-23v2	192.168.23.155	10	10.20.2.8
jenkins.demo.io	192.168.15.105	9	10.20.2.8

Tenable OneのVPR※

優先して対応すべき脆弱性を知っていれば

別話です

自社の所有する情報資産に基づいて脅威度を順位付け

視覚化してくれるこの機能のおかげで

VPR : Vulnerability Priority Rating (脆弱性の修復優先度)

ボクたちは少数数のチームで膨大な量の脆弱性に対応することができています

うんうん

脆弱性が出たらパッチを当てる

僕たちがやっているのは地味で

当たり前のことすぎません

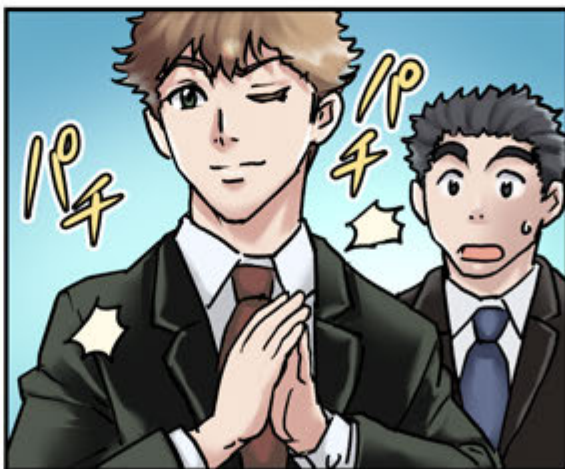
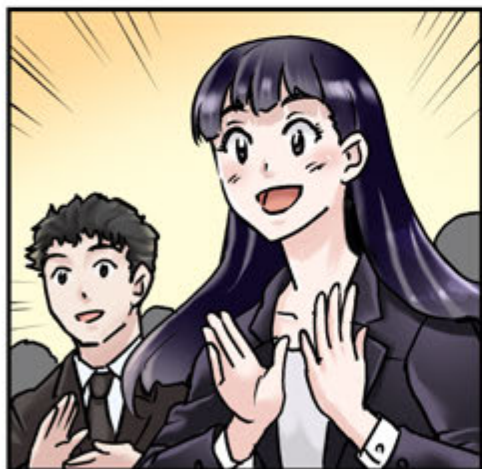
でも

その導入を提案したのだからってセンパイですから!



最前線の
戦いだ
と考
えて
いま
す！

脆弱性管理
こそが
セキュリティの
一丁目一番地



tenable

100% 100% 100% 100%...

THE END

漫画・原作：瀬尾浩史 / 製作：株式会社イード ScanNetSecurity 高橋潤哉