

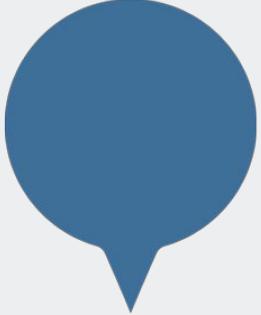
Co3で支えるペパボのセ キュリティ対策

~Communication Completely Continuous~

GMOペパボ セキュリティ対策室

Agenda

- セキュリティ対策室とは
- エンジニアリングで組織を動かす
- セキュリティ対策を継続させるプロダクトの開発
- まとめ



Section 1

セキュリティ対策室とは

組織と活動背景の紹介
Tamon Kumano

ミッション

GMOペパボのセキュリティ対策室とは

情報セキュリティ基本方針を遵守

お客様、お取引先様、従業員から預る情報資産を
適切に扱える文化形成、技術的仕組みをリードする組織

セキュリティ対策室 (2021年現在)



CTO,CISO:栗林 @kentaro



マネジメント:熊野 @mod_osho



エンジニア :伊藤 @hiboma



エンジニア:森田 @mrtc0



技術顧問:力武先生 @jj1bdx

名前

熊野多聞 くまのたもん

経歴

- 2007年入社～
- インフラエンジニアとして各サービスのインフラを担当(キッティング～構築、運用、保守)
- 2015年～
- OpenStackを用いたプライベートクラウド基盤移行を契機にマネジメントへピボット
- 2018年セキュリティマネジメントの推進



その他

- 趣味はロードバイク
- 平日はZWIFT、天気がよければ横須賀、三浦半島、平塚あたりを走ってます





Section 1

セキュリティ対策をやりきれる組織 ~completely~

ペパボが運用するサービスとセキュリティ対策室の関係性

Completely

対策を "完了" させること。完了させなければ、穴が空いたまま。

- 脆弱性の修正を完了させる
- インシデントを収束させる
- セキュリティ対応を完了させる

対策を終わらせることで、次の課題が見つかる => 多層防御のマインドを持つ

複数の事業部門とそれぞれのチームで開発・運用

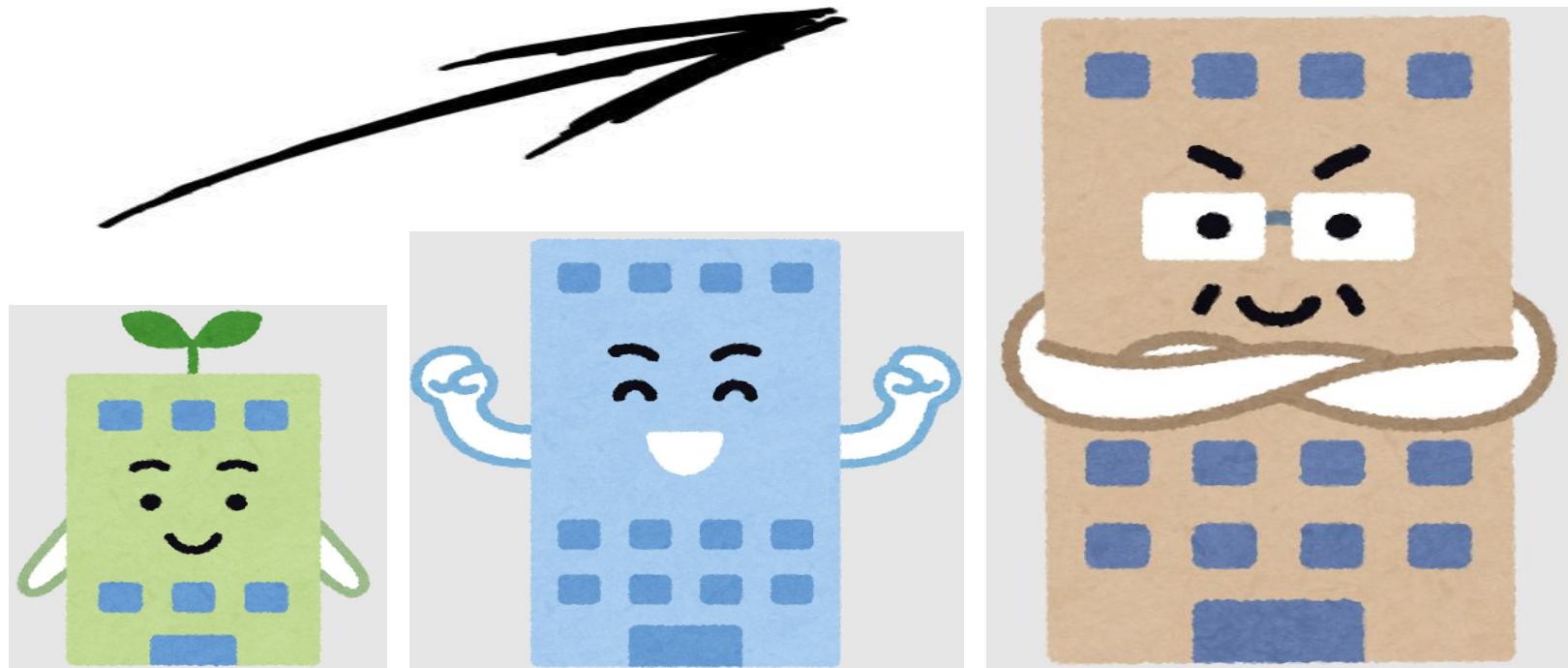


複数部門のサービスから成り立つセキュリティ事情

ペパボには10年以上続くサービスからリリースして数年まで規模や関わる人々に濃淡がある

- サービス設計時のセキュリティ対策も年月とともに変化
- 少しずつ改善することで頑健性のあるサービスになることもあれば年々メンテナンスが難しくなることもあります
- サービス開発時期によっては技術スタックに選択の幅がある
 - e.g. 開発言語、フレームワーク、OSディストリビューション、MW

若いサービスから長年続くサービスまでさまざま



セキュリティ対策室設置前

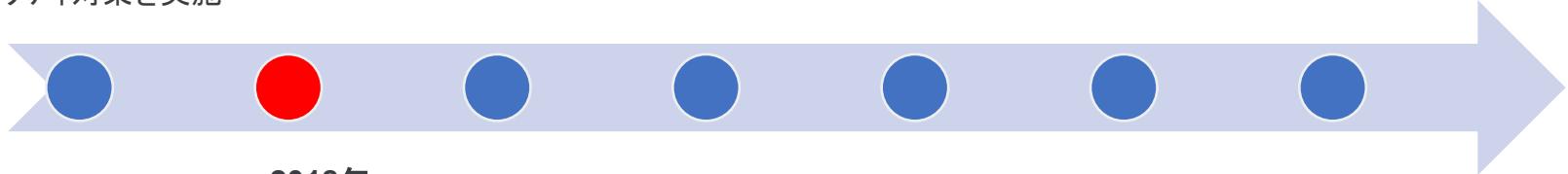


セキュリティ対策室の位置づけ



ペパボのセキュリティ対策年表

各事業部門がア
プリケーション/イ
ンフラチームが
OS・MWのセキュ
リティ対策を実施



2018年
ターニングポイン
トとなるセキュリ
ティインシデント発
生

ペパボのセキュリティ対策年表

各事業部門がアプリケーション/インフラチームがOS・MWのセキュリティ対策を実施

2018年3月
セキュリティ対策室発足

2019年
インシデントハンドリング手法の標準化

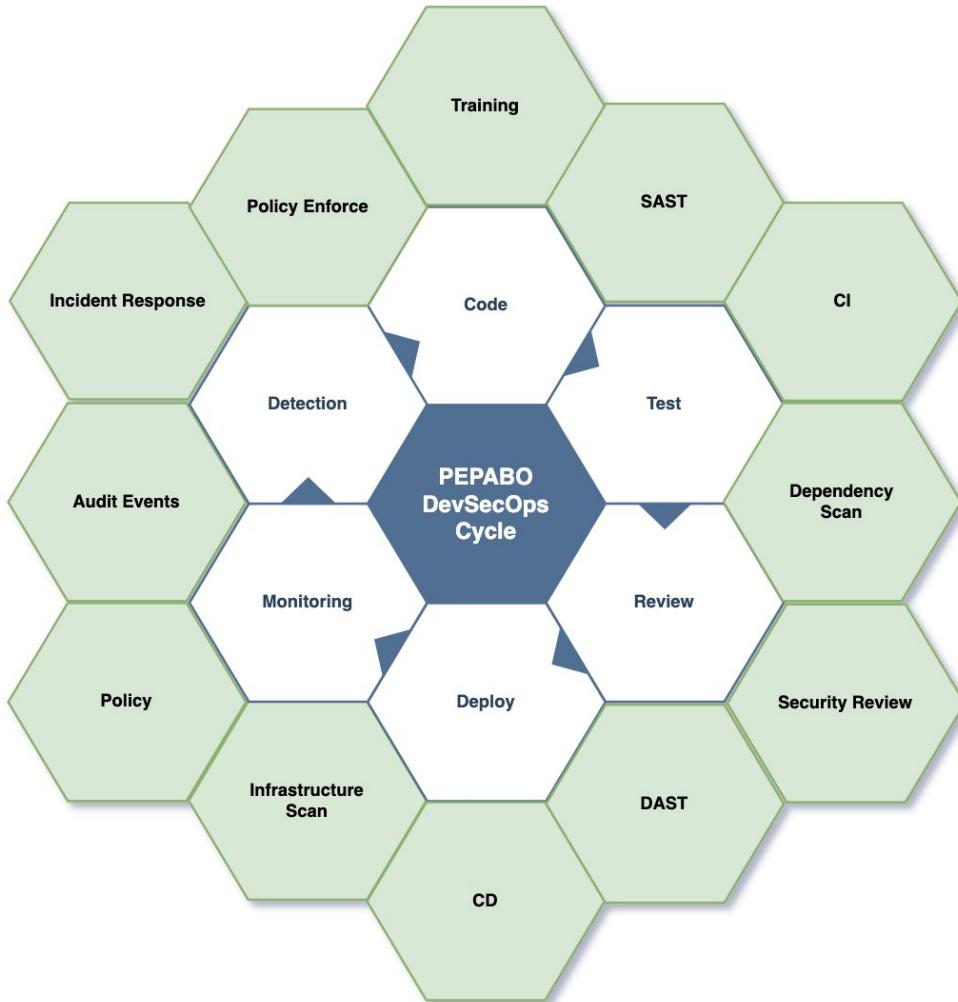
2021年～



2018年
ターニングポイントとなるセキュリティインシデント発生

2018年12月
セキュリティインシデントの再発防止策完了

2020年
DevSecOpsを実現するための仕組み、ツール開発



セキュリティ対策室が取り組む DevOpsとSecの関係性

- セキュリティ対策の地図を作る(マッピング)
- 道路を舗装(ツール等環境の準備)
- ガードレールで予防(予期せぬ事故でも最悪のケースを防ぐ)

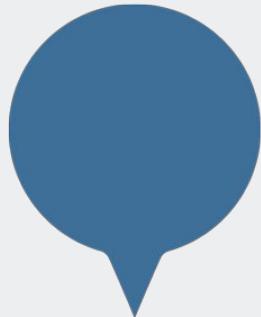
セキュリティ対策組織を運用しての発見と課題

- 外部からの攻撃も内部事故によるセキュリティインシデントも弱いところから起こる
- セキュリティのベースライン、ガイドラインを作ることで弱いところの発見と対策が実施できる
- セキュリティ対策は担当部門に任せず、協力し、やりきる、継続的に行う
- インシデントの発見者には感謝を
- 小さなセキュリティインシデントでも共有を行うマインド
 - 現場のリーダーや経営管理者によるセキュリティ方針の同期

セキュリティ対策の方針

- **Co3 (Communication / Completeness / Continuous)**
 - **Communication** ... コミュニケーションを取る。「みんなと仲良くする」。
 - **Completeness** ... インシデントを収束させる。対策を完結させる。
 - **Continuous** ... 対策を継続する。継続にレバレッジする技術を使う。
- 「ガードを下げたらやられる」というマインドを持つ
- Security as a Code で道の舗装やガードレールを作る

ペパボのセキュリティ文化を一
緒に形成してくれるメンバーオーク
募集！！1



Section 2

エンジニアリングで Communication を回す

Hiroya Ito 伊藤洋也 / @hiboma

自己紹介

- **名前**
 - 伊藤洋也 (いとうひろや) @hiboma
- **経歴 / よくやってること**
 - 2007年入社～
 - ホスティングサービスの開発
 - サーバサイドの基盤 API 開発
 - Linux のトラブルシューティング
- **私生活**
 - 2020年9月 栃木県那須塩原市に移住 リモートワーク!



「セキュリティ」と私個人のキャリア

2018年3月 セキュリティ対策チームに異動となった
セキュリティについては 热心には取り組んではいないキャリアだった

- 「セキュリティ」あんまり自信ない
 - 徳丸本は読んだ
 - XSS, CSRF, SQL インジェクションくらいは知ってるが...

さて、どうやって ペパボのセキュリティ対策チーム をやっていこう?

チーム初期の課題

新設されたチームには課題が山積み！エンジニアリングだけでない！

- チーム内コミュニケーションを回す
 - 新卒で入社した森田 @mrtc0 とどうやって走るか？
- 組織内コミュニケーションを回す
 - 少ないメンバーで組織横断的にレバレッジをかけるには？
- エンジニアリングでコミュニケーションを解決する
 - slack bot でコミュニケーション支援する



Section 2

チーム内コミュニケーション

チームといいつつ二人三脚

メンタリング

伊藤 @hiboma は 2007年から在籍で社内の内情を知っていた。
入社したての 森田 @mrtc0 のメンターとしてふるまう

- ペパボの技術スタックをチュートリアルする
- 抱えている問題・課題を共有する
- 同僚間のコミュニケーションを繋ぐ
- 上位等級エンジニアとしての背中をみせる

セキュリティの経験・技術をすでにもつ若手を自走できるまで
支援することもチーム初期の課題だった

シニアエンジニアに昇格までを支援できたのも嬉しい

インタビュー
シニアエンジニアに最速昇格! 新卒1年目もりたこの話
2019.3.1
エンジニア 新卒採用



リバースメンタリング

逆に、セキュリティのいろはを森田 @mrtc0 から教わる(今も)

- セキュリティ対策の基本
 - 種々の攻撃方法や防御/緩和の方法
 - 脆弱性のみつけかた
 - 脆弱性の報告の仕方
- セキュリティの技術や各種ツール
- セキュリティ業界・コミュニティ・イベント情報



チーム発足初期に双方が教えをリードできて、補い合えたことは好遇だった



Section 2

組織内コミュニケーション

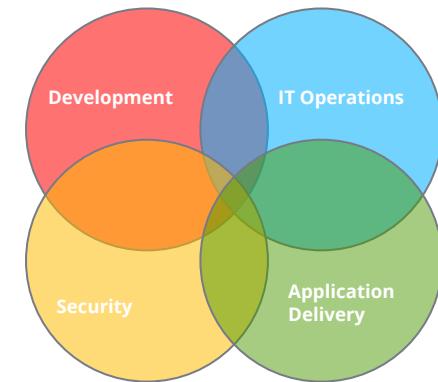
小さなチームを同僚の力を得てレバレッジする

Communication

「DevOps」vs「Sec」の対立にならないよう^{する}
"コミュニケーション" を通して DevSecOps モデルの理解を得てもらう

- セキュリティを組織文化として育む
- 小さな異変や気付きを気軽に共有できる組織
- 平時・緊急を問わず 迅速・正確な対応につなげる

コミュニケーションが「セキュリティを当たり前とする文化」を育てる "レバレッジ" となる

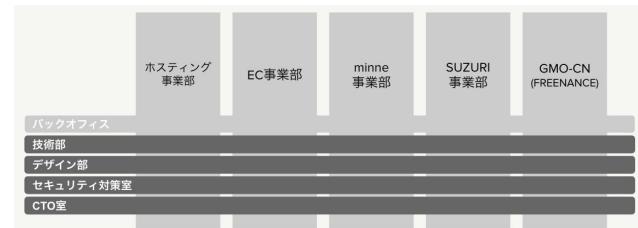


小さなチームと大きな会社

社内の情報をつぶさに追いかけていくのは困難。

周囲から情報を **push** してもらえるとありがたい ... !

- 例: ユーザさんのお問い合わせで 疑わしい内容があった
- 例: 脆弱性の修正方法で迷っていたので相談したい
- 例: インシデントの疑いのある事象が起きた
- 例: 世間で話題になっているセキュリティのネタがある
- ... etc



気軽に情報を共有してもらうには ちょっとコツがいる

Slack で情報共有と集約を工夫



Reacji Channeler を使って簡略に実現する。  emoji を付けるとセキュリティチャンネルに共有される

SSS Reacji Channeler APP 2:57 PM
<https://.slack.com/archives/> (edited)

takomatsu
@ec-success
以下共有です。
【弊社の話ではないです】
salesforce経由での情報漏えいリスクが確認されたため、その条件に弊社の設計が該当していないか、issue立てて進めてます。
自分の知る限り過去にゲストユーザーの発行を行った記憶はないので問題ないと思いますが、進捗はこちらのissueで残して進めていきます。

Posted in #ec_success | Dec 18th, 2020 | [View message](#)

熊野が全社員向けの情報セキュリティ研修に  のチュートリアルを加えたことで
技術職だけでなく、CS 職からの共有も多くなり助かっている(不審なお問い合わせの共有など)

社内イベント(ペパボテックフライデー)で宣伝と啓蒙

毎月行われる技術者向けの社内イベントペパボテックフライデーでチームの宣伝や対策の啓蒙を行う

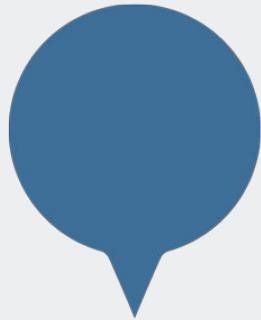


エンジニアがリーダーシップをとろう

@hiboma の持論
インシデントにおいて
技術職がリーダーシップをとる責務を負うべき
(例外: 情報セキュリティインシデントでは CS 職のケースが多い)

emoji も何度も宣伝を行って普及を狙った。

新設のチームの PR を繰り返し、組織内でのポジションを確立しコミュニケーションを回していく



Section 3

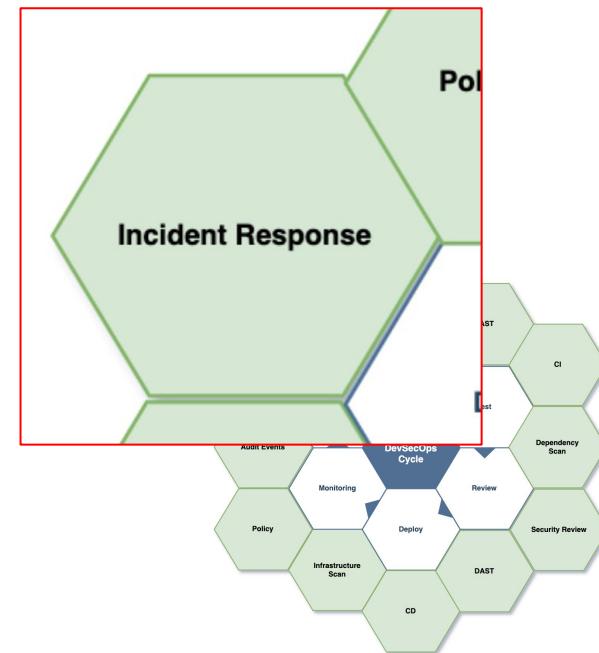
エンジニアリングで コミュニケーションを解決

slack bot でコミュニケーション支援

レジリエンス強化の課題

DevSecOps + シフトレフトの考え方、前倒しした対策が
森田やサービス所属のエンジニアによって整えられていく

一方で レジリエンス = 障害やセキュリティインシデントが
起きた場合に迅速に回復する体制も整えていく必要があります。



インシデント対応のコミュニケーションロスが復旧・緩和に響く

- インシデント対応でエンジニアは極度のプレッシャーに晒される
 - 未知の事象・不確実な状況も復旧を確実に達成しなければならない
- チャットツールの混乱
 - アラートを受診するチャンネルは大量のメッセージで溢れ やりとりが追いかけにくい
 - メッセージが多いチャンネルで Slack のスレッド機能を使うと情報が局所化する

💡 ペパボでは「障害」サービスの可用性を損なう事象も「インシデント」と呼んでいます。

インシデント対応のコミュニケーションロスが復旧・緩和に響く

- 職種間やサービス・部署間の情報共有が滞る
 - エンジニアは復旧作業で詳細な技術情報（ログや分析）を書くが、そのままでは他職種には解釈が難しい
 - マネージャー職・CS 職へ状況伝達がうまくいかないケースがある
 - インシデントが他サービスに伝播した場合も、連絡が滞ると影響範囲が拡大する
- 組織内のコミュニケーションのロスで復旧・ユーザー対応が遅れてしまう
 - ビジネスへのネガティブインパクト 🔥

=> プレッシャーのかかる状況下でコミュニケーションの支援が必要

slack bot で インシデント対応を支援する

緊急時のコミュニケーションを自動で支援する **slack bot = sssbot** を開発し、解決に臨んだ

- インシデント対応チャンネルの作成
- 初動対応のチームをinvite する
- インシデントの発生を複数のチャンネルに通知する
- インシデントの issue を作成し記録する
- 15分後に時間を知らせるタイムキーパーを行う
- postmortem の pull request を自動作成する

... たくさん!



 チャンネルを作る

チャンネル名

example|20210224i

チャンネル名は最大80文字までです

サービス

other

いまいまの状況

例) DBサーバがダウンして Web の閲覧ができない

対応の温度感

 サービスへの影響を調査する

⑦ Learn more about sssbot

Cancel 作成!

チャンネル作成のフォーム

チャンネルはインシデント対応ごとに都度作成する
記録一元化し、事象を追いかけやすくする

複数のチャンネルに通知を飛ばし 事象発生を共有する



sssbot-staging アプリ 16:25

障害対応チャンネルが作成されました

チャンネル	#example-20210224i	サービス	other
サマリ	DB の master で障害	温度感	RED すでにヤバイ. 緊急の対応をする

- エンジニアチャンネル、マネージャー職チャンネル、CS 職チャンネルにも通知がとぶ

初動対応チームを invite して初動を促す

The screenshot shows a message from 'sssbot-staging' (アプリ) at 11:58. The message content is:

インシデントレスポンステムのアクションを確認しましょう

1 インシデントハンドラー をアサインしましょう
2 インシデント判断フローチャート に沿ってインシデントレスポンスを進めましょう

サービスの対応マニュアルも参照しましょう

- 初動対応を整える指示を出します

初動対応チームに状況を伝える



sssbot-staging | アプリ 12:04

@hiboma チャンネルを作ってくれてありがとうございます。いまいまどんな状況でしょうか?

- 影響範囲は? (どんな機能や画面で影響でてる?)
- ユーザー対応の要否は? (お知らせ、お問い合わせ、ソーシャル対応は必要?)
- 原因・復旧の目処はつきそうか?

- インシデント対応チャンネルをつくった人に、状況説明を促します
- 初動チームは突然 invite されて、状況を理解できないことがあります

タイムキーパーが介入して状況判断を促す



- 15分ごとにタイムキーパーが介入します

GitHub issue に自動で記録をとる

#corporate-eng-20210219i #594

Open pepabot opened this issue 5 days ago · 1 comment

pepabot commented 5 days ago

sssbot が自動でコメントしています

インシデントの概要

- サービス corporate
- チャンネル #corporate-eng-20210219i

サマリ

@kajiのGHEアカウントが乗っ取りされた

チャンネル作成の記録

- 2021-02-19 14:09:07 +0900

pepabot added corporate セキュリティインシデント labels 5 days ago

⚠️ スクリーンショットは、弊社で定期的に実施しているインシデント対応訓練での利用例です

postmortem の pull request も自動でつくる



⚠️ スクリーンショットは、弊社で定期的に実施しているインシデント対応訓練での利用例です

みんなの、ふつう、あたりまえ を徐々に変えていく

一年ほどかけて徐々に bot の実装をつくりあげ利用を普及させていきました。

コミュニケーション支援 = 同僚のふるまいを変える対策は継続的かつ粘り強いフォローが必要です

- 全てのインシデント対応チャネルにセキュリティ対策チームも加わる
 - CTO, VPoE も必ず invite される
- sssbot の不満点やフィードバックを拾い上げ、修正・改善・機能追加を漸進的に行う
- sssbot の機能や活用事例を社内イベント(ペパボテックフライデー)で繰り返し宣伝する

組織文化 = みんなが、ふつうに、あたりまえに、sssbot 使ってくれるまでやる!!!

コミュニケーション支援から復旧・解決のリードへ

インシデントの技術的な問題は「人間」が解決しなければいけません。

SRE ともオーバラップするように、セキュリティ対策チームはインシデントの復旧・解決にも関わります。



ペパボ"テックフ"ログ

Technology, Engineering, Creative, and Human-Centred Design

2020-06-26

ペパボ トラブルシュート伝 - TCP: out of memory – consider tuning `tcp_mem` の `dmesg` から辿る 詳解 Linux net.ipv4.tcp_mem

トラブルシューティング

 タイート  いいね！  シア  BI ブックマーク 136  Pocket 48

セキュリティ対策室の伊藤洋也です @hiboma

過去の障害対応中に遭遇した TCP: out of memory -- consider tuning `tcp_mem` という `dmesg` を端緒として、Linux カーネルがどのようにTCPのメモリを管理するのかを調べました。

最新記事

2021-02-22

ペパボ SRE ケーススタディ - ロリポップ! レンタルサーバーのSLI/SLOをもとにしたパフォーマンス改善の取り組みを紹介します

2021-02-10

ペパボのログ活用基盤『Bigfoot』を使った Zendesk のデータ可視化

2021-02-09

ペバカレが気になる人の FAQ

2021-02-05

ステークホルダーマップの活用



ペパボ"テックフ"ログ

Technology, Engineering, Creative, and Human-Centred Design

2020-06-11

ペパボ トラブルシュート伝 - node プロセスの general protection fault をもう abort(3) の意外な実装

トラブルシューティング

 タイート  いいね！ 6  シア  BI ブックマーク 62  Pocket 43

セキュリティ対策室の伊藤洋也 @hiboma です。

業務中に、[Haconiwa コンテナ](#) で動くある node プロセスが **general protection fault (一般保護違反)** を起こして `dmesg` にログを残す現象を調べ、問題解決にあたっていました。その際の痕跡をまとめおして記したエントリになります。

最新記事

2021-02-22

ペパボ SRE ケーススタディ - ロリポップ! レンタルサーバーのSLI/SLOをもとにしたパフォーマンス改善の取り組みを紹介します

2021-02-10

ペパボのログ活用基盤『Bigfoot』を使った Zendesk のデータ可視化

2021-02-09

ペバカレが気になる人の FAQ

2021-02-05

ステークホルダーマップの活用

技術的難易度の高いチャレンジがあったケースでは、ペパボテックブログに「**トラブルシューティング**」の記事として昇華します

セキュリティ対策室: これからの課題

これからもセキュリティの課題は山積み

セキュリティを主軸としていないアプローチでもコミットできる

- コミュニケーションをエンジニアリングで回す
- サービスの安定稼働を目指してSREともオーバーラップしていく

セキュリティを主軸にやりたい人も、もちろん求めている

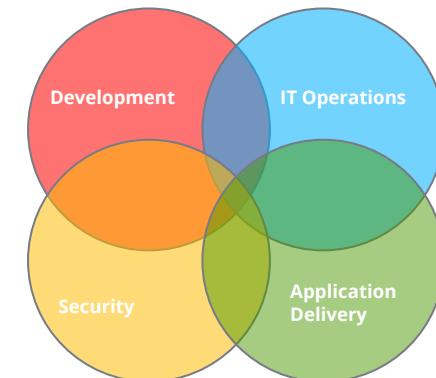
- 詳細は 森田 @mrtc0 のターンで!

ペパボサービスインフラの今までとこれから

歴史とこれからの展望

常松 伸哉 / GMO Pepabo, Inc.
2021.02.25 ペパボテックカンファレンス#14

GMOペパボ株式会社





Section 4

セキュリティ対策を継続させるプロダクトの開発

Kohei Morita / @mrtc0

自己紹介

名前と所属

森田 浩平 / @mrtc0

セキュリティ対策室 シニアエンジニア

経歴

~ 2018年 脆弱性診断会社でアルバイト

2018年4月 新卒入社

その他

セキュリティ・キャンプ講師, ステアリングコミッティ

IPA未踏事業 クリエイター

OWASP Fukuoka Chapter Leader

<https://blog.ssrf.in/>



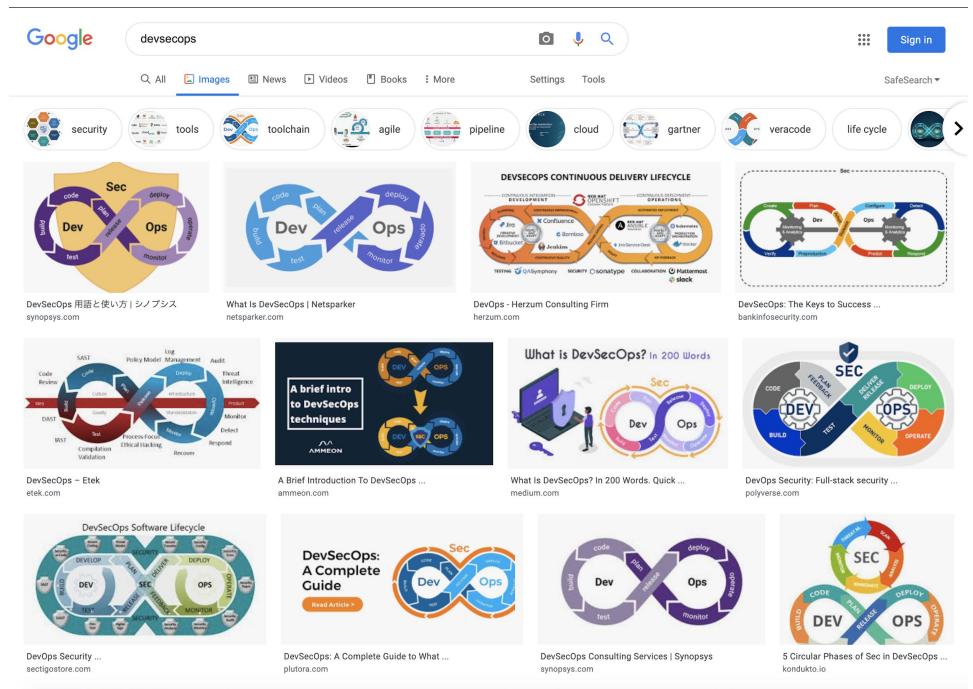
Continuous

攻撃やインシデントがなくなることはないため、対策を "継続する" 必要がある

- 攻撃が止むことはない = 防御も止めてはいけない
- 持続的で大きな効果を生み出す = レバレッジの効いた技術を使う / 対策をする
- 継続するために自動化する 

DevSecOps の推進

- 「セキュリティ対策はやって当たり前」というマインドセットへ
- DevOps に Sec が混じっている図
- 自分たちはどこを守っているんだっけ ... ?

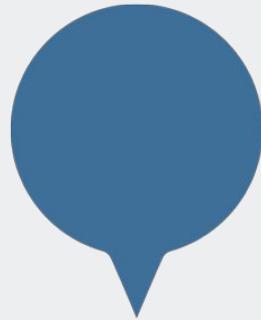


DevSecOps の推進

- 自分たちの DevSecOps サイクルを考える
- 不足している領域を穴埋めしていく
- 課題があれば領域を広げていき、層を厚く(多層防御)していく



👉 別途、サービスごとの脅威モデリングは必要として、事業部を横断してみたときに、その対策基盤を確認できる



Section 5

継続させるための エンジニアリング

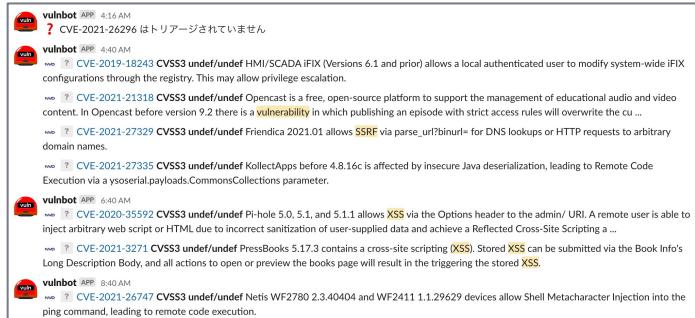
セキュリティ対策室のエンジニアリング例

脆弱性情報の収集・トリアージ

組織横断的に脆弱性情報の収集とトリアージを行っている

- CVE・JVNDB のアグリゲーターを実装
 - Slack Bot を通知インターフェースとする
 - Affected 疑いのものは pin 留めして remind
- 対応を要する脆弱性は issue で組織展開
 - 例: CVE-2021-3156 sudo の脆弱性

 emoji でもセキュリティチャンネルに情報共有を集う



vulnbot APP 4:16 AM
? CVE-2021-2629% はトリアージされていません

vulnbot APP 4:40 AM
...
? CVE-2019-18243 CVSS3 undefined HMI/SCADA iFix (Versions 6.1 and prior) allows a local authenticated user to modify system-wide iFIX configurations through the registry. This may allow privilege escalation.

vulnbot APP 4:40 AM
...
? CVE-2021-21318 CVSS3 undefined Opencast is a free, open-source platform to support the management of educational audio and video content. In Opencast before version 9.2 there is a vulnerability in which publishing an episode with strict access rules will overwrite the cu ...

vulnbot APP 4:40 AM
...
? CVE-2021-27329 CVSS3 undefined Friendica 2021.01 allows SSRF via parse_url?binurl= for DNS lookups or HTTP requests to arbitrary domain names.

vulnbot APP 4:40 AM
...
? CVE-2021-27335 CVSS3 undefined KollectApps before 4.8.16c is affected by insecure Java deserialization, leading to Remote Code Execution via a yserial.payloads.CommonsCollections parameter.

vulnbot APP 6:40 AM
...
? CVE-2020-35592 CVSS3 undefined F-hole 5.0, 5.1, and 5.1.1 allows XSS via the Options header to the admin/ URL. A remote user is able to inject arbitrary web script or HTML due to incorrect sanitization of user-supplied data and achieve a Reflected Cross-Site Scripting a ...

vulnbot APP 8:40 AM
...
? CVE-2021-3271 CVSS3 undefined PressBooks 5.1.7 contains a cross-site scripting (XSS). Stored XSS can be submitted via the Book Info's Long Description Body, and all actions to open or preview the books page will result in the triggering the stored XSS.

vulnbot APP 8:40 AM
...
? CVE-2021-26747 CVSS3 undefined Netis WF2780 2.3.40404 and WF2411 1.1.29629 devices allow Shell Metacharacter Injection into the ping command, leading to remote code execution.



CVE-2021-3156 sudo における権限昇格の脆弱性 #129

[Open](#) mrtc0 opened this issue 28 days ago · 16 comments

概要

sudo (正確には sudoedit) のコマンドオプション解析部分に BufferOverflow があり、パスワードなしで root に権限昇格できる脆弱性が見つかりました。
sudo (sudoedit) コマンド自体が実行できる時点で影響を受ける可能性があります。

影響を受けるソフトウェアとバージョン

Sudo versions 1.8.2 through 1.8.3ip2 and 1.9.0 through 1.9.5ip1 are affected.

リスク評価

「セキュリティイベントのリスク評価マトリクス(DREADモデル)」に基づき評価した。

脅威	D	R	E	A	D	Total	Risk
権限昇格	3	2	2-1	3	2	12	High ~ Medium

なるべく早いアップデートと対応をお願いします。

- High (12-15) : 他のリスクを止めてもらいますすぐ対応する
- Medium (8-11) : 一ヶ月以内の期間を切って対応する
- Low (5-7) : 四半期以内の期間をもつて対応する
- Recommended (0-4) : 対応することが望ましい

対応期限

(上記のリスク評価に基づき決定する)

Wazuh の運用

Wazuh (わずー) Agent モデルのセキュリティ基盤

- ログ監視に基づいた侵入検知
- ファイル整合性監視 (FIM)
- ポリシー監査
- 各種インベントリの収集 / 脆弱性検知

Wazuh の構築・導入は 山下 @pyama86 と 常松 @tnmt が進めてくれた。
セキュリティ対策室で運用を固めている。

The screenshot shows the Wazuh official website. At the top, there's a navigation bar with links for Product, Documentation, Blog, Cloud, Services, and a search icon. The main header reads "The Open Source Security Platform". Below it, a sub-header says "Wazuh is a free, open source and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response and compliance." There are three callout boxes: one about getting started, one about being open source, and one about professional help. At the bottom, there's a row of icons representing various security features: Security Analytics, Intrusion Detection, Log Data Analysis, File Integrity Monitoring, Vulnerability Detection, Configuration Assessment, Incident Response, Regulatory Compliance, Cloud Security, and Containers Security.

This is a screenshot of a presentation slide. The title is "Wazuhを利用した大統一サーバ監査基盤" (Wazuh-based unified server audit base) and the subtitle is "～新春の地中海であがったPerlを添えて～". The footer contains the text "@pyama86 / GMO Pepabo, Inc. 2019.01.26 YAPC::Tokyo 2019" and the GMO Pepabo logo.

Wazuh 運用の継続的な改善

- ・組織やチームに適合した運用をするため、不足している箇所を自分たちで作っていく
- ・コミュニティにも貢献していく

The screenshot shows a GitHub pull request titled "Fixed URL anchors #2223". The PR has been merged and is part of the "wazuh:3.11" branch from the "hiboma" user. It was created on 7 Mar 2020. The commit message from "hiboma" says: "Hi. This PR fixes URL anchors for regex.html." with two bullet points: "os-regex-or-regex-syntax -> regex-os-regex-syntax" and "os-match-or-sregex-syntax -> sregex-os-match-syntax". The pull request has 2 conversations, 1 commit, 0 checks, and 3 files changed.

README.md

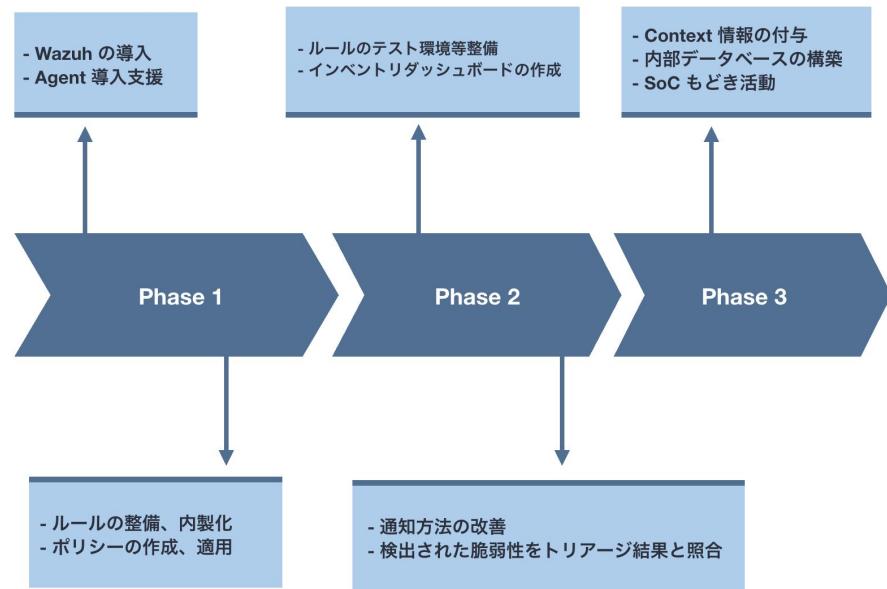
Wazuh Ruby Client

A Ruby client for the wazuh APIs.

Installation

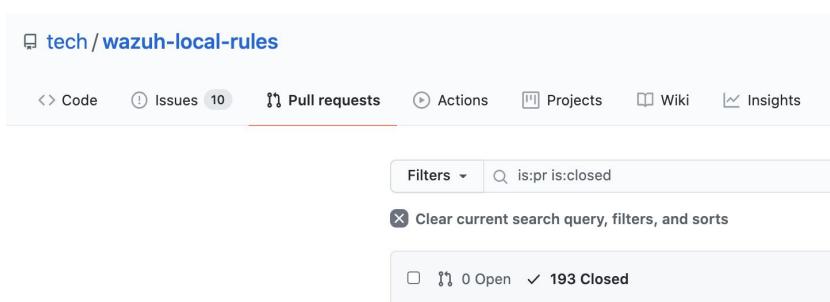
Add this line to your application's Gemfile:

```
gem 'wazuh-ruby-client'
```



Wazuh ルールの継続的な運用

- デフォルトのルールは検知対象が多い
 - 自分たちでカスタマイズしていく必要性
 - Centralized configuration で集中管理
 - セキュリティ対策室がテコ入れして削減
- サービス側もルールの調整を行う
 - ルールを書きやすい環境を整備
 - YAML でルールとテストログを記載



ルールとテストの書き方

実際に記述したルールが想定どおりに動くかテストすることが出来ます。local_rules/<サービス名>/<ルールID>.yaml にルールとログと、想定出力のレベルを記述するだけでCI時に自動でテストします。

```
rule: |
  <!-- ここに rule を記載する -->
  <rule id="123456789" level="12">
    < ... >
  </rule>
tests:
- log: full_log を含む
  level: 想定レベル を記載する
- log: "Oct 11 15:03:19 ssldcache-10-241-0-69 sshd[24082]: Did not receive identification string from
  level: 0
```

通知のカスタマイズ

- ステージング環境での検証等で生じる一時的なエラーなども検知され、大量に通知が来てしまう
- アラートに対してどのようなアクションを取ればよいかわからない
 - > 流量や通知内容のコントロールを行うために、通知モデルを実装



⚠ Group Scope Flooding! ルール 1010 の通知が溢れています。通知を drop します
Process segfaulted.
Feb 25 06:27:44 : kernel: [4494341.003069]

👉 単位時間あたりの同一アラート数が溢れたら、そのアラートを止める

Annotation やリンクをつけることで対応を促したり、確認負荷を下げる👉

General SATA disk failure	: [18045039.399985] ata5.00: failed
Feb 23 14:21:30	
command:	
Agent	Rule ID
	5138 (Level 7)
Location	Alert
/var/log/syslog	realtime
Annotation	
💣 ハードウェアトラブル予兆のアラートです	

その他のセキュリティ対策室の取り組み

- サービス安定のための技術を検証、導入している。例えば
- 社内 Kubernetes クラスタ管理ツール NKE への Falco や Security Policy の導入
- ロリポップ！マネージドクラウドのコンテナイメージの検証に Open Policy Agent を導入
- パッケージ等のインベントリを横断的に検索できるアーキテクチャの開発と運用
- Linux カーネル周辺のバグ調査、脆弱性の実現可能性の調査



発生したインシデントを俯瞰するダッシュボード（サンプル）

PANOP

REPOSITORIES

IMAGES

Signed in as mrtc0

Repository List

REPOSITORY	TYPE	RENOVATE	ACTION
org1/app	Rails	Installed	Edit
org1/app-tools	Ruby	Ignored	Edit
org1/frontend	TypeScript	Required to install	Edit

リポジトリやパッケージを俯瞰できるようにするアプリケーション（サンプル）

現状の課題やこれから

アプリケーション

- ・AST や DAST を利用した脆弱性検出の強化

インフラ

- ・セキュリティポリシーの Enforce

インシデント

- ・プレイブック(対応)の自動化や SOAR への発展

その他

- ・モバイルなど
- ・人的リソース (今は3人しかいない!)

以下、一つでもマッチする方を募集しています！

- 技術力で DevSecOps の推進に貢献してくれる方
- Linux カーネルレイヤの問題に取り組める方
- プロダクトのセキュリティエンジニアリングに関わりたい方
- この発表を聞いて「興味がある！」となつた方

「ペパボ 採用」[検索]
<https://recruit.pepabo.com/>

※ セキュリティエンジニアの募集枠は後日出ます
各サービスのソフトウェアエンジニア / SRE としてセキュリティに携わりたい方も大募集！