چرخه مدیریت رخداد

روش اجرایی پاسخگویی به رخدادهای رایانه ای

فرایند ۱: اعلام رخداد توسط کاربران حقیقی یا حقوقی، اعلام حسگرها و سیستم های هانی پات

جمع آوری و ورود اطلاعات اولیه

از طریق ارسال نامه

از طریق اعلام تلفنی

از طریق اعلام سنسورها و حسگرهای نصب شده در زیرشبکه استانهای کشور

فرایند ۲ : فیلترینگ

فیلتر نمودن کلیه ورودی ها و خارج نمودن درخواست های کاذب از طریق اجرای فرایند احراز هویت ، تکمیل نمودن فرم مخصوص پاسخگویی به رخداد و ثبت رخداد.

فرایند ۳: اولویت بندی

تعیین اولویت پاسخگویی به رخدادها بر اساس ضریب اهمیت تعیین شده

فرایند ۴: جستجو در پایگاه اطلاعاتی و رصد واحدی

بررسی پایگاه اطلاعاتی به منظور مشخص شدن تکراری بودن درخواست ، در صورت تکراری بودن اطلاعات نهایی موجود در پایگاه اطلاعاتی بعنوان راهکار به متقاضی ارائه می گردد

تهیه گزارشات عملکرد

الف: رصد آسیب پذیریهای حوزه افتا

۱ -دریافت گزارش اولیه جدیدترین آسیب پذیریها و تهدیدات رایانه ای از منابع معتبر امنیتی داخلی یا خارجی

۲ -بررسی میزان ارتباط و صحت اطلاعات رخداد با سازمانهای مخاطب کشور

۳ -انتخاب گزارشات با اهمیت بیشتر)بر حسب شدت آسیب پذیری و سطح حساسیت سازمانهای مخاطب(جهت تحلیل و ارائه راهکار)

۴ -تحلیل گزارشات مربوط به اسیب پذیری ها و تهدیدات

۵ -تهیه و ارائه گزارشات تحلیل و ابزار تهیه راهکارها

۶ -صحت سنجی و تکمیل راهکارهای ارائه شده

۷ -تعیین مخاطبین سازمانی رخداد شناسایی شده

۸ -تهیه مکاتبات محرمانه مربوط به رخداد و راهکارهای مربوطه

۹ -تایید محتوای مکاتبات مربوط به رخداد و راهکارهای مربوطه توسط مدیر مرکز

۱۱ -پاسخگویی به سوالات و ابهامات ارسال شده از گروه پاسخگویی نسبت به سازمانها در خصوص محتوای گزارشات تکمیلی

۱۱ -درج اتمام هشدار

ب: تحلیل تهدیدات

۱ -دریافت گزارش مربوط به رخدادهای به وقوع پیوسته در سطح کشور از گزارش مراجع امنیتی بین المللی و یا مراجع اطلاعاتی داخلی

۲ -دریافت اطلاعات تکمیلی از مراکز یا سازمانهای هدف با هماهنگی مراجع اطلاعاتی کشور

۳ -تحلیل و صحت سنجی وقوع رخداد با استفاده از گردآوری اطلاعات تکمیلی از مراکز همکار، آپا و سازمانهای هدف و...

۴ -ارجاع رخداد جهت تحلیل دقیق و فنی به مراکز آپا با توجه به حوزه فعالیت و تعیین اولویت زمانی

۵ -بررسی خروجی ها و تایید نتایج

۶ -تعیین احتمال متاثر بودن سازمانها و نهادهای حیاتی و حساس کشور با توجه به نوع رخداد

۷ -آماده سازی زیرساخت ارتباطی سریع با نمایندگان سازمانها

۸ -ارائه نتایج تحلیل اولیه مرکز به سازمانهای هدف و راهکارهای مقابله و کاهش پیامد

۹-دریافت و جمع آوری خروجی ها و نتایج اعمال راهکارها در سازمانها

۱۱ -بررسی و تحلیل مجدد اطلاعات کسب شده به منظور پوشش کامل رخداد و ارائه راهکارهای پاکسازی قطعی با همکاری مراکز اپا

۱۱ -پاسخگویی به سوالات و ابهامات مطرح شده در خصوص راهکارها و گزارشات ارائه شده به سازمانهای هدف

ج: تدوین بولتن

۱ -دریافت اخبار امنیتی به روز در خصوص رخدادهای گزارش شده در سطح بین المللی

۲ -بررسی اخبار مرتبط با دارایی های اطلاعاتی کشور و یا با سطح ریسک بالا

۳ -تحلیل اخبار مرتبط در حوزه افتا

۴ -بررسی تحلیل ها و گزارشات تهیه شده در حوزه اخبار افتا

۵ -تدوین و ویرایش بولتن خبری در خصوص حوزه اخبار افتا

۶ -تایید محتوای بولتن خبری توسط مدیر مرکز

۱۲ -تعیین مخاطبین سازمانی رخداد شناسایی شده

۷ -تهیه مکاتبات محرمانه مربوط به رخداد و راهکارهای مربوطه

د: پاسخگویی

۱ -ارسال مورد پاسخگویی از گروه پاسخگویی

۲ -تحلیل و بررسی مشکل ارسال شده با توجه به الویت زمانی آن

۳ -تدوین اطلاعات تکمیلی درخواستی از سازمان جهت تحلیل بیشتر مشکل و ارائه به مسئول گروه پاسخگویی

۴ -تحلیل بیشتر مشکل مورد بحث با توجه به دریافت اطلاعات تکمیلی

۵ -ارجاع مشکل جهت تحلیل دقیق تر به مراکز آپا) در صورت لزوم)

۶ -ارائه راهکارها و پیشنهادات جهت رفع مشکل به گروه پاسخگویی

و: توصیه نامه

۱.بررسی منابع مطالعاتی در حوزه افتا به منظور استخراج موضوعات و مفاهیم کلیدی و پایه این حوزه

۲.انتخاب موضوع دارای اهمیت بالا در حوزه افتا برای مخاطبین عام

۳.بررسی و جستجوی روشها و راهکارهای تکمیلی در خصوص پوشش آسیب پذیریهای امنیتی

۴.بیان و تبدیل راهکارهای فنی و تخصصی در سطح کاربران عام

۵.تهیه و تدوین توصیه نامه امنیتی در خصوص مشکلات کاربران و راهکارهای پوشش آنها

۶.تایید محتوای توصیه نامه امنیتی

۷.ارسال توصیه نامه امنیتی در سطح سازمان، وزارت و زیر ساخت

فرایند ۵: تحلیل رخداد و آزمایشگاهی

درصورت بروز حمله تیم امداد اقدام به بررسی موضوع می نماید این بررسی می تواند از طریق کنترل IP های مهاجم یا رهگیری مهاجم از طریق شرکتهای میزبانی کننده شبکه صورت پذیرد درصورتیکه فایل بدافزار در اختیار باشد تیم تحلیل بدافزار اقدام به کدخوانی یا رمزگشایی می کند و با تهیه شناسنامه فنی بدافزار آنرا مورد پایش و بررسی قرار می دهند

الف: شناسایی تهدیدات جدید ناشی از انتشار بدافزارها و کدهای مخرب

۱۳ -دریافت نمونه از شبکه هانی نت ملی

۱۴ -دریافت نمونه از طریق وبسایت مرکز

۱۵ -نمونه برداری از سطح سازمانها و فضای سایبری کشور

۱۶ -دریافت نمونه بدافزارها و کدهای مخرب از طرق ارتباطی مختلف

۱۷ -تحلیل نمونه های دریافتی و ارزیابی سطح تهدیدات آنها

۱۸ -تهیه گزارش از موارد با اهمیت

۱۹ -اطلاع به مراجع بالادست

ب: جمع آوری و ذخیره سازی جدیدترین بدافزارهای گسترش یافته

۱جمع آوری نمونه ها از طریق اشتراک در سرویس های بین المللی

۲ -جمع آوری نمونه ها از طریق مراوده با گروه های فعال در زمینه بدافزار در داخل و خارج کشور

۳ -تهیه و توسعه ابزار های شناسایی سریع گونه های تهدید کننده

۴ -ذخیره سازی نمونه ها در بانک اطلاعات بدافزار

۵ -ارسال مدیریت شده نمونه ها به تولید کنندگان آنتی ویروس داخلی و مراکز تحقیقاتی

ج: پیگیری اخبار حوزه بدافزارها از منابع مختلف رسمی و غیر رسمی جهت آگاهی سریع از رویدادها

۸ -پیگیری جدیدترین اخبار منتشر شده توسط شرکت های فعال در حوزه بدافزار

۹ -تماس مستقیم با متخصصین داخلی و خارجی برای دستیابی به اخباری که منتشر نشده و یا هرگز منتشر نخواهند شد.

۱۱ -عضویت در گروه های تخصصی این حوزه جهت دریافت آخرین اخبار و اطلاعات

۱۱ -تهیه گزارش از مهمترین اخبار

۱۲ -ارائه موارد با اهمیت به مراجع بالادست

د: ارائه گزارش جهت ایجاد آمادگی و مقابله با رویدادها

۷ -ارائه گزارش در خصوص عملکرد بدافزارهای ناشناس جمع آوری شده توسط هانی پات

۸ -ارائه گزارش در خصوص تهدیدات امنیتی با ریسک زیاد

۹ -ارائه گزارش در خصوص مهمترین تهدیدات امنیتی به وجود آمده

ه: ارائه ابزار و راهکار مقابله با تهدیدات واقع شده

۱ -تشخیص و تفکیک رویداد های خاص با اهمیت بالا

۲ -تهیه دستورالعمل مقابله و ارائه گزارش مربوطه

۳ -ارائه ابزار مناسب جهت شناسایی و پاکسازی

۴ -ارسال ابزار و راهنمای استفاده به سازمانها و انتشار عمومی آن در صورت نیاز

فرایند ۶: مشاوره

درصورتیکه از طریق دانش موجود نتوان به ماهیت حمله با بدافزار پی برد از طریق تشکیل اتاق فکر و یا دعوت مشاوران متخصص برای حمله بوجود آمده تدبیری اتخاذ می گردد که البته برای هرنوع حمله تدبیری خاص و منحصر به فرد لازم است.

فرایند ۷: تائید

پس از یافتن راهکار مناسب، اخذ تائید اجرا و مصوب نمودن راهکار جهت اعلام ضروری است

فرایند ۸: بروز رسانی آرشیو و توسعه سنسورهای، حسگرها و سامانه گردآوری کننده بدافزار یا سایرابزارها

پس از اخذ مجوز اعلام نتیجه، خروجی را به اولویت بندی شده و با رعایت اولویت در اختیار گروه پاسخگویی به رخداد قرار می گیرد.

الف: شناسایی زیر شبکه های حساس ملی

۲۱ -دریافت اطلاعات اولیه از خارج از تیم

۱ -۱دریافت وضعیت از سازمانها

۱ -۲دریافت وضعیت از تیم های داخلی مرکز ماهر

۱ -۳شناسایی زیرشبکه بصورت تصادفی

۲۱ -تعیین اولویت و فیلترینگ درخواست وارده

۲۲بررسی و امکان سنجی زیرشبکه سازمان اعلام شده بصورت غیرحضوری

ب: اقدام برای ارتقاء سطح امنیتی زیرشبکه

۱۲ -هماهنگی با مسئولین شبکه سازمان ها یا حراست های IT سازمانها

۱۳ -امکان سنجی نصب حسگر و سنسورهای گردآوری کننده بدافزار بصورت حضوری در صورت نیاز

۱۴ -مشاوره و راهنمایی به مدیرشبکه سازمان متقاضی جهت رفع موانع نصب حسگر و سنسورها

۱۵ -انجام مکاتبه با مدیر فناوری اطلاعات سازمان متقاضی و درخواست مشخصات فنی

۱۶ -انجام هماهنگی و مشاوره جهت ارائه توضیحات فنی توجیهی – تشریحی

۱۷ -دریافت پاسخ و مشخصات فنی مورد نیاز از سازمان متقاضی

۱۸ -تنظیم برنامه زمانبندی با توجه به منابع سخت افزاری و تجهیزات سخت افزاری

۱۹ -هماهنگی و درخواست مجوز ورود به سازمان متقاضی

۲۱ -ارجاع و صدور دستور کار به نصاب حسگر یا سنسورهای هانی پات

۲۱ -تحویل سرور به نصاب

۲۲ -پیکربندی نرم افزارها بر سرور

۲۳ -هماهنگی نصاب با مسئول شبکه سازمان مربوطه

۲۴ -مراجعه حضوری نصاب جهت نصب حسگر و سنسور

۲۵ -اجرای فرایند نصب

۲۶ -اجرای فرایند لینک به پورتال ملی هانی نت

۲۷ -نظارت بر دریافت برخورد توسط کارشناسان ماهر

۲۸ -تائید صحت عملکرد سنسور یا حسگر منصوبه

۲۹ -تکمیل صورتجلسه تحویل سخت افزار توسط سازمان متقاضی

۳۱ -اعلام محل نصب و مشخصات کامل سنسور به سازمان

۳۱ -صدور نام کاربری و رمز عبور برای متقاضی بصورت محرمانه

۳۲ -تکمیل و تائید فرم های آزمایش و تحویل

ج: پایش و مانیتورینگ سطح کیفی عملکرد سنسورها

۱۳ -تهیه گزارش هفتگی ثبت برخورد

۱۴ -بررسی علل عدم کاربری برخی ماشین های مجازی

۱۵ -انجام فرایند تخصصی رفع مشکل سنسورها بصورت ریموت

۱۶ -به مدار بازگرداندن سنسورهای منصوبه و ارائه گزارش اصلاحی

۱۷ -تهیه گزارش ثبت برخورد ها بصورت ماهانه

۱۸ -رفع مشکلات سنسورها از راه دور

۱۹ -ارائه گزارش اقدامات انجام شده در قالب مانیتورینگ

۲۱ -برگزاری جلسه هماهنگی در جهت رفع مشکلات تخصصی مانیتورینگ

۲۱ -اعلام مشکلات فنی یا ستادی غیر قابل رفع در تیم به مدیرمرکز

۲۲ -به روزرسانی سنسور و تست مجدد صحت کارکرد

د: گزارش

۱۱ -ارائه گزارش وضعیت کاربری سنسورها و حسگرهای منصوبه به سازمان متقاضی بصورت محرمانه

۱۱ -ارائه گزارش وضعیت کاربری سنسورها و حسگرهای مربوطه به مدیر

۱۲ -ارائه گزارش ثبت برخورد بصورت هفتگی . ماهانه و سالیانه به مدیر

۱۳ -ارائه گزارش اقدامات انجام شده در تیم مانیتورینگ به مدیر

۱۴ -ایجاد دسترسی گزارش گیری برای مرکز راهبردی افتا

درصورت نیاز به توسعه یا بکارگیری ابزاردیگر از طریق تعریف پروژه جدید و تهیه و تنظیم RFP اقدام می گردد بدین صورت که حسب RFP ارائه شده طبق نیاز بوجود آمده، اقدام به تهیه شرح خدمات می گردد و پس از قطعیت شرح خدمات آنرا به معاونت مالی اداری و تدارکاتی ارسال می دارند لذا پس از طی فرایندهای مالی و تامین اعتبار اقدام به انعقاد قرارداد جدید در جهت رفع نیاز می گردد و عملکرد پیمانکار
مربوطه طبق مفاد قرارداد بدقت مورد پایش و کنترل قرار می گیرد.

فرایند ۹: پاسخ و رفع رخداد

گروه پاسخگویی به رخداد ها حسب مورد ارجاعی اقدام به پاسخ می نمایند در صورتیکه از طریق حسگرهای هانی پات ، اطلاعات دریافت شده باشد نتایج بررسی ها به اطلاع سازمانها و مسئولین شبکه ها رسیده می شود و در صورتیکه اطلاعات از طریق درخواستهای تلفنی باشد نتایج بررسی ها طی ارسال نامه های محرمانه به اطلاع متقاضی رسیده می شود و یا از طریق انجام مکاتبات محرمانه، نتیجه اقدامات به اطلاع متقاضی رسیده می شود.

ابزارهای مدیریت رخداد

مدیریت حوادث (IcM) شما را ملزم می کند تا اختلال غیرمنتظره در سرویس IT را مشاهده کرده و به موقع حل مسئله را سازمان دهید. زمینه مدیریت حادثه پشتیبانی و پشتیبانی کاربران را در بر می گیرد ، بنابراین ابزارهای مدیریت حادثه به عملکردهای نرم افزار میز خدمت نزدیک هستند.

ابزار ایده آل برای مدیریت حادثه باید جامع تر از یک سیستم ردیابی رویداد رویداد راهنما باشد. همچنین باید از تحول سیستم IT حمایت کند تا از بروز مجدد خطر غیر منتظره جلوگیری شود. این بدان معنی است که مدیریت واقعه ایده آل باید شامل گزارش های گسترده و ویژگی های تحلیلی باشد. ادغام فرآیندهای ITIL نیز بسیار مفید است زیرا به محض شناسایی علت این حادثه و برنامه ریزی برای اصلاح گسل های سیستم ، به راهنمایی سازگاری سیستم کمک می کند.

SolarWinds Web Help Desk

نام SolarWinds Web Help Desk باعث می شود فکر کنید این سرویس از ابر اجرا می شود. با این حال ، این نرم افزار داخلی است که روی سرورهای خود نصب می کنید ، اما می توانید از طریق یک مرورگر به آن دسترسی پیدا کنید ، به این معنی که Cloud داخلی خود را ایجاد می کنید.

این بسته چیزی بیش از یک سیستم Help Desk نیست. این سیستم دارای ویژگی های مدیریت دارایی و کنترل نسخه است که به شما در پیگیری موجودی نرم افزار و سخت افزار کمک می کند. Luck از روال کشف خودکار دستگاه تهیه شده و این ابزار ، یک پایگاه داده از دارایی های فناوری اطلاعات را ایجاد و نگهداری می کند. این سرویس به شما امکان دسترسی سریع به بررسی های موجود و استفاده از تجهیزات IT خود را می دهد و به طور منظم از عملکرد تجهیزات شما نمایان می شود.

این نرم افزار با استفاده از فرایندهای ITIL در ذهن شما طراحی شده است و وظیفه برنامه ریزی ، پیاده سازی و تغییر هرگونه تغییر مورد نیاز برای جلوگیری از بروز مجدد خطر را آسان می کند.

در کنار این ویژگی های عالی مدیریت تغییر ، سیستم SolarWinds دارای توابع راهنما استاندارد است. این ویژگی ها با ویژگی های عالی ردیابی وظیفه و برنامه های مدیریتی تیم افزایش یافته است.

ابزارهای گزارشگری و تحلیلی که در میز راهنمائی وب ایجاد شده اند ، به مدیریت در نظارت بر SLA کمک می کند - که این نیز گزینه ای عالی را برای ارائه دهندگان خدمات مدیریت شده ایجاد می کند. می توانید پارامترهایی را در داشبورد تنظیم کنید که در صورت عدم موفقیت اهداف عملکرد ، هشدارها را انجام می دهند. این سیستم هشدار همچنین برای ردیابی حوادث مفید است و اطمینان حاصل می شود که زمان پاسخگویی برای رفع مشکل محکم است.

نرم افزار Web Help Desk روی Windows، Windows Server، Linux و Mac OS اجرا می شود. می توانید این سیستم را در یک آزمایش رایگان 14 روزه آزمایش کنید. پس از دوره آزمایشی ، می توانید استفاده از آن را متوقف کنید ، مجوز بخرید یا به Web Help Desk Free Edition بروید ، که قابلیت های کامل نرم افزار پرداخت شده را ندارد.

ManageEngine Service Desk Plus

Service Desk Plus به صورت نرم افزاری در محل یا به عنوان یک سرویس نرم افزاری که از طریق وب تحویل داده می شود ، موجود است. ManageEngine سه سطح خدمات را برای سرویس میز پلاس ارائه می دهد و ویژگی های مدیریت حادثه فقط در برنامه های بالاتر در دسترس هستند. بسته کامل شامل برنامه های مدیریت دارایی IT است که کلیه سخت افزارها و نرم افزارهای موجود در شبکه شما یک بانک اطلاعاتی موجودی را برای شما فراهم می کند. شما همچنین می توانید رویه های مدیریت پروژه مبتنی بر ITIL را با برنامه برتر دریافت کنید.

ویژگی های مدیریت حادثه سرویس میز پلاس عملکردهای Help Desk سیستم را در بر می گیرد. این ماژول همچنین شامل نظارت بر عملکرد و ردیابی SLA است. سایر ویژگی های ITIL این ابزار شامل یک فهرست خدمات است که هم خدمات تجاری و هم فنی را در بر می گیرد. این گردآوری اطلاعات را راهنمایی می کند وقتی که یک خطر بوجود می آید و از طریق اسکریپت ها و گردش کار به تحقیقات انتقال از طریق راه حل تغذیه می شود.

خدماتی که از بروز مجدد خطرات شناسایی شده در اطراف بروزرسانی دانش دانش حاوی راهنمایی برای کاربران و تنظیمات رویه ها و اسکریپت های سرویس جلوگیری می کند تا خطای احتمالی تازه شناسایی شده را محاسبه کنند.

کمبودهای اساسی سیستم که منجر به بروز حوادث می شوند روشهای مدیریت تغییر ماشه را در سیستم Service Plus Plus اعمال می کنند. پس از برطرف شدن یک حادثه ، کار بعدی این است که اطمینان حاصل کنید که هرگز دیگر اتفاق نمی افتد و اگر علت آن مربوط به زیرساخت ها بود ، شما باید برای بهبود سیستم باشید. گردش کار در ماژول مدیریت تغییر تیم شما را از طریق فرآیند تکامل و ترمیم موجودی خود راهنمایی می کند تا از تکرار خطاها جلوگیری کند.

Service Desk Plus در سه بسته موجود است. بسته استاندارد وظایف اساسی Help Desk را در اختیارتان قرار می دهد ، که شامل تعدادی مورد نیاز برای مدیریت حادثه است. مدیریت دارایی فناوری اطلاعات تنها در صورت دسترسی به برنامه حرفه ای در دسترس است. بالاترین برنامه ، با نام Enterprise Edition ، کلیه میز خدمات و ماژول های مدیریت دارایی برنامه های پایین را شامل می شود و همچنین عملکردهای مدیریت تغییر ITIL گسترده ای دارد.

برنامه Enterprise شامل مدیریت تغییر ، فهرست خدمات ، مدیریت مشکل و مدیریت پیکربندی است. گزارش و تجزیه و تحلیل ویژگی های خدمات میز پلاس پشتیبانی عالی از مدیریت در هنگام حل مسئله و وظایف تکامل سیستم ارائه می دهد.

SolarWinds Service Desk

میز سرویس SolarWinds به عنوان یک سرویس از طریق وب ارائه می شود. با این حال ، این شرکت نرم افزاری را برای سیستم ها در اختیار مشتری قرار می دهد تا بنا به درخواست در محل نصب شود. این سرویس آنلاین طبق فرایندهای استاندارد ITIL ساخته شده است ، بنابراین تضمین می کند که سیستم های مدیریت دارایی و پشتیبانی مشتری از توانایی کامل برای مقابله با مدیریت حادثه برخوردار باشند

سیستم خدمات SolarWinds در قلب راه حل مدیریت حوادث است. این شامل سه عنصر اصلی است: بلیط فروشی ، پورتال خودیاری و پایگاه دانش. خدمات در سه سطح بسته ارائه می شود. این شرکت بسته استاندارد را به عنوان تحقق الزامات مدیریت حوادث ارائه می دهد. با این حال ، این فقط به سیستم مدیریت Help Desk اشاره دارد. برای به دست آوردن کلیه عملکردهای مورد نیاز برای چرخه حیات مدیریت حادثه تعریف شده با ITIL ، باید برای بالاترین برنامه بروید.

برنامه تجاری توابع Help Desk را به شما می دهد و همچنین مدیریت ، کاتالوگ خدمات و ردیابی عملکرد SLA را تغییر می دهد. برنامه برتر با نام حرفه ای به شما مجوز و مدیریت قرارداد و اتوماسیون پیشرفته را می دهد. گنجاندن گردش کار و اسکریپت های تحقیق در میز کار به شما کمک می کند تیم خود را هنگام تحقیق در مورد منبع گزارش شده توسط کاربر راهنمایی کنید. فرآیندهای ITIL درون نرم افزار ، مراحل تحقیق را به سمت پیشنهادهای راه حل و وظایف مدیریت پروژه گسترش می دهد.

Spiceworks Help Desk

ویژگی بارز Spiceworks Help Desk این است که استفاده از آن رایگان است. این یک معامله شگفت انگیز با در نظر گرفتن پیشرفته بودن نرم افزار است. در روند نزولی ، سیستم با تبلیغات ظاهر می شود که به طور دائم در یک صفحه جانبی داشبورد ظاهر می شود ، از تبلیغات پشتیبانی می کند. نسخه پرداختی از Spiceworks Desk Help Desk وجود ندارد.

این یک بسته نرم افزاری است که در ویندوز و Mac OS نصب شده است. می توانید به جای آن از سیستم بصورت آنلاین استفاده کنید و از عدم نیاز به نگهداری نرم افزار روی سرورهای خود خودداری کنید. عملکرد نسخه آنلاین ، که به آن Spiceworks Cloud Help Desk گفته می شود ، به اندازه نرم افزار داخلی

نیست. با این حال ، به Cloud Help Desk از هر دستگاه دیگری در هر نقطه قابل دسترسی است ، بنابراین لازم نیست نگران نرم افزار و سازگاری سیستم عامل باشید و می توانید به داشبورد Help Desk خود از دستگاه های تلفن همراه دارای سیستم عامل Android یا iOS دسترسی داشته باشید.

Spiceworks دارای یک جامعه کاربری بسیار فعال است و هزاران افزونه در انجمن موجود است. این به شما امکان می دهد سیستم را به منظور ادغام با برنامه های دیگر که ممکن است از آنها استفاده کنید سازگار کنید - بسیاری از برنامه های افزودنی توسط ارائه دهندگان آن برنامه ها نوشته شده اند.

داشبورد عامل شامل یک ویژگی یادداشت برداری و پیام رسانی است که یک راه حل عالی برای راه حل های مشترک برای بروز حوادث است.

Zendesk Suite

Zendesk عمدتا یک سیستم Help Desk است. با این حال ، ماژول گزارشگری و تحلیل عالی آن باعث شده است تا در این راهنمای ابزارهای مدیریت حوادث ، شایسته ورود باشد.

Zendesk یک سیستم بسیار پرکاربرد است. این تعدادی از راه ها را به هم پیوند می دهد که به کاربران امکان می دهد تا قبل از مراجعه به کارمندان IT برای کمک ، مشکلات را حل کنند. این ویژگی ها با یک پایگاه داده مشاوره قابل جستجو در حول پایگاه دانش می چرخند. خط بعدی کمک ها مربوط به کانال های تماس است. Zendesk شامل یک پنجره گپ می باشد که پاسخ ها و حل مسئله را از طریق سوالات تعاملی سرعت می بخشد.

سیستم مدیریت بلیط در Zendesk باعث می شود تا نمایندگان به عنوان دستیار بعدی در دسترس انتخاب شوند. بلیط را می توان از طریق تماس تلفنی یا ایمیل و همچنین از طریق چت جمع آوری کرد. آنها را می توان ردیابی ، هدایت ، تقسیم و ادغام کرد.

Zendesk Suite به ابر قابل دسترسی است بنابراین نیازی به نگهداری نرم افزار در سایت ندارید. عملکردهای نظارت و گزارشگری شما را قادر می سازد عملکرد عملکرد نماینده و معیار گردش مالی مورد انتظار را ارزیابی کنید. عملکرد گزارش همچنین از انطباق هدف SLA پشتیبانی می کند.

Zendesk برای هر نماینده در هر ماه شارژ می شود. این سیستم در دو سطح حرفه ای و Enterprise در دسترس است. هر دو سطح برای پشتیبانی مدیریت حادثه مناسب هستند. شما می توانید یک آزمایش رایگان از Zendesk دریافت کنید تا آن را با سرعت بیشتری طی کنید