వివరించండి.

ఆపరేషనలైజింగ్ సైబర్ సెక్యూరిటీ ఆపరేషన్ సెంటర్ నెలకొల్పడం (C-SOC.)

పరిచయం

1- గత కొంతకాలంగా భారత బ్యాంకింగ్ పరిశ్రమ సాంకేతికపరంగా ఎంతో పరిణితి చెందుతూ, ప్రస్తుతం కస్టమర్లకు వినూత్నమైన సేవలను అందిస్తోంది. కస్టమర్లకు బ్యాంకింగ్ సేవలు అన్ని వేళలా, ఎలాంటి విరామం లేకుండా అందుతున్నాయి. కస్టమర్లు ఇంటర్నెట్, మొబైల్ కనెక్టివిటీ ద్వారా ఈ సేవలను పొందగలుగుతున్నారు. ఆర్థిక లావాదేవీల విషయంలో భద్రత అనేది అన్నిటికన్నా ముఖ్యమైనది. అందువల్ల RBI నిర్దిష్టమైన అప్లికేషన్లు, సేవలకు సంబంధించి సెక్యూరిటీ మరియు ఆపరేషన్స్‌పై ఎప్పటికప్పుడు మార్గదర్శకాలను జారీ చేస్తుంటుంది.

2 - బ్యాంకింగ్ పరిశ్రమలో ప్రత్యేకించి ఇంటర్నెట్‌ను ఉపయోగించుకుంటున్న అప్లికేషన్లు, ప్రస్తుతం అందుతున్న, భవిష్యత్తులో అందబోయే సేవల వైపు దృష్టి సారించాల్సిన అవసరం చాలా ఉంది. వాటి విషయంలో అన్ని అప్లికేషన్లు, సర్వీసుల కోసం సైబర్ సెక్యూరిటీ మార్గదర్శకాలను విడుదల చేయాలి.

3 - తగినటువంటి, తక్కువ ఖర్చయ్యే సమర్థమైన టెక్నాలజీ పరికరాలను ఉపయోగించుకుంటూ, ఉత్తమ పద్ధతులపై ఆధారపడిన పాలసీలు, నియమాలను అనుసరిస్తూ, సాంకేతికంగా సమర్థులైన, నిపుణులైన సిబ్బంది ద్వారా నిరంతర పర్యవేక్షణ కలిగిన వ్యవస్థను ఏర్పాటు చేసుకోవడం బ్యాంకింగ్ పరిశ్రమ ముందున్న తక్షణ కర్తవ్యం. సైబర్ సెక్యూరిటీ పాలసీపై ప్రభుత్వం ఎప్పటికప్పుడు జారీ చేసే మార్గదర్శకాలను అనుసరించడం, ముఖ్యమైన సమాచార రక్షణ, ఇన్ఫర్మేషన్ టెక్నాలజీ చట్టాన్ని అనుసరించడమన్నవి చాలా ముఖ్యమైనవి.

సైబర్ సెక్యూరిటీ ఆఫరేషన్స్ సెంటర్ ఏర్పాటు విషయంలో గవర్నెన్స్, టెక్నాలజీ, ఆపరేషనల్, ఔట్‌సోర్సింగ్, లీగల్ అంశాలను చెందిన సమస్యలను పరిష్కరించడం చాలా ముఖ్యం.

4 - C-SOC ఏర్పాటు చేసే సందర్భంలో ఈ క్రింది అంశాలను దృష్టిలో పెట్టుకోవడం అవసరం. ఇవి కేవలం సూచన మాత్రమే, సంపూర్ణం కాదు.

గవర్నెన్స్ అంశాలు:

- విపత్తు ఇంటలిజెన్స్‌పై టాప్ మేనేజ్‌మెంట్/బోర్డు వివరణ
- డాష్ బోర్డులు మరియు పైవిచారణ
- విధానాలు, వాటి పరిమాణం, వాటి అమలు (కీ మెట్రిక్స్, రిపోర్టింగ్ స్ట్రక్చర్, ఏది నివేదించాలో పేర్కొనండి)
- భాగస్వాములకు సమాచారం అందజేయండి, భాగస్వాములు పాల్గొనడం

సైబర్ SOC : గమనించాల్సిన అంశాలు:

1- గత కొన్నేళ్లుగా నివారక విధానాన్ని అనుసరిస్తూ వస్తున్న సాంప్రదాయ సెక్యూరిటీ వ్యవస్థలు ప్రతికూల స్వభావం కలిగినట్టివి. దాడుల గురించి ముందస్తు సమాచారం తెలిసినప్పుడు ఎదురయ్యే సమస్యలను అవి పరిష్కరించగలవు. అయితే గత కొంతకాలంగా విపత్తులు సంభవించే అవకాశాలు, పరిస్థితుల విస్తృతి చాలా పెరిగింది. అందువల్ల వాటిని పరిష్కరించే విషయంలో - సంఘటన జరిగిన తర్వాత ప్రతిస్పందించడం కన్నా సంఘటన జరగడానికి ముందే చర్యలు తీసుకునే దృక్పథం కలిగి ఉండడం ముఖ్యం. తెలియని విపత్తులను కూడా పరిష్కరించగలిగేలా ఉండాలి. ఉదాహరణకు జీరో డే దాడులు, ఎలాంటి సూచనలూ లేని దాడుల గురించి దృష్టిలో పెట్టుకోవడం అవసరం.

2- విపత్తులను వెంటనే గుర్తించడానికి; తగిన డాటా, పరికరాల ద్వారా విశ్లేషించడానికి, వేగంగా ప్రతిస్పందించడానికి సైబర్ SOC ముందస్తు పర్యవేక్షణ మరియు మేనేజ్‌మెంట్ సామర్థ్యాలను దృష్టిలో పెట్టుకోవడం అవసరం.

3- ప్రస్తుతం సెక్యూరిటీ ఆపరేషన్లను పర్యవేక్షిస్తున్న వ్యవస్థ ఏర్పాటు చేసిన ప్రొడక్ట్ యొక్క ప్రతి పాయింట్ నుంచి లాగ్‌లను సేకరిస్తుంది, లాగ్‌లను భద్రపరిచి ప్రాసెస్ చేస్తుంది, తగిన SIEM పరికరాల ద్వారా పరస్పర సంబంధాలను నిర్వచిస్తుంది, SIEM స్క్రీన్‌లను నిరంతరం పర్యవేక్షిస్తుంది. ఏదైనా అనుమానాస్పదంగా తోచినట్లయితే వెంటనే హెచ్చరికలు జారీ చేస్తుంది.

4. సైబర్ SOCలో భాగంగా అవసరమైన వ్యవస్థను ఏర్పాటు చేయడానికి ఈ క్రింది అంశాలను పరిశీలించాలి:

దాడులకు మూల కారణాలను కనుగొనే విధానాలు, వాటిని గుర్తించిన విభాగాల్లోకి వర్గీకరించడం, అదే విధమైన దాడులు జరగకుండా వాటికి పరిష్కారాలు కనుగొనడం.

ప్రైవస్నీ సాధించడానికి సంఘటనను పరిశోధించడం, ఫోరెన్సిక్స్, డీప్ పాకెట్ అనాలసిస్ అవసరం.

డైనమిక్ బిహేవియర్ అనాలసిస్ - ప్రాథమిక స్టాటిక్ మరియు డైనమిక్ సమీక్ష, ఇండికేటర్స్ ఆఫ్ కాంప్రమైజ్ (IOC) సేకరణ

మంచి డ్యాష్ బోర్డ్‌తో విశ్లేషణ; ఐపీల భౌగోళిక ప్రదేశాన్ని చూపించడం

కౌంటర్ రెస్పాన్స్ మరియు హనీస్పాట్ సర్వీసులు

SOC నుంచి ఆశిస్తున్నవి:

- క్రిటికల్ బిజినెస్ మరియు కస్టమర్ డాటా/సమాచారను రక్షించే సామర్థ్యం; అంతర్గత మార్గ దర్శకాలు, దేశంలోని చట్టాలు, నియంత్రణకు లోబడి ఉండాలి.
- రియల్ టైమ్/నియర్ రియల్ టైమ్‌కు సంబంధించిన సమాచారాన్ని అందించగలిగే సామర్థ్యం; బ్యాంకు యొక్క భద్రతపై లోతుగా పరిశీలన
- సెక్యూరిటీ ఆపరేషన్లను సమర్థంగా నిర్వహించడం, సైబర్ రిస్కులు/విపత్తులను సమర్థంగా ఎదుర్కొనడం, కార్యకలాపాలలో నిరంతరాయత, రికవరీ ఉండేలా చూడడం
- విపత్తుల సమాచారాన్ని సేకరించడం, బ్యాంకులపై వాటి ప్రభావాలను ముందస్తుగా అంచనా వేయడం
- ఎవరు, ఎప్పుడు, ఏం చేశారన్న వివరాలు తెలుసుకునే సామర్థ్యం, సాక్ష్యాలను భద్రపరచడం
- వివిధ రకాల లాగ్‌లను, లాగింగ్ ఆప్షన్స్‌ను SIEM, టికెటింగ్/వర్క్ ఫ్లో/ కేస్ మేనేజ్‌మెంట్, అన్‌స్ట్రక్చర్డ్ డాటా/బిగ్ డాటా, రిపోర్టింగ్/డాష్ బోర్డ్, యూజ్ కేసెస్/రూల్ డిజైన్ (రిస్క్ అండ్ కాంప్లయెన్స్ అవసరాలు/డ్రైవర్లు మొద.వాటి ఆధారంగా తయారు చేసినవి) మొదలైన వాటిలోకి జోడించడం

SOC యొక్క ముఖ్యమైన బాధ్యతలలో ఈ క్రిందివి ఉండాలి:

- సెక్యూరిటీ సంఘటనల పర్యవేక్షణ, సమీక్ష మరియు పెంపు
- ప్రతిస్పందన మెరుగుపరచడం - రక్షణ, పరిశోధన, ప్రతిస్పందన, పూర్వస్థితి
- ఇన్సిడెంట్ మేనేజ్మెంట్, ఫోరెన్సిక్ సమీక్షను నిర్వహించండి
- బ్యాంకు లోపల మరియు బయటి సంస్థల కాంటాక్ట్ గ్రూపులతో సమన్వయం

5- సైబర్ SOC యొక్క ఇటుకరాళ్లు

సాంకేతిక సమస్యలు

బ్యాంకింగ్ టెక్నాలజీ రిస్క్ ప్రొఫైల్ మరియు వ్యాపార, రెగ్యులేటరీ అవసరాలకు అనుగుణంగా ముందస్తు పర్యవేక్షణ సామర్థ్యాలు కలిగిన తక్కువ ఖర్చయ్యే టెక్నాలజీ ఫ్రేమ్‌వర్క్‌ను రూపొందించి, దానిని అమలు చేయడం మొదటి అడుగు.

బ్యాంకులు కస్టమర్లకు అందించే వినూత్నమైన సేవల వ్యవస్థను స్పష్టంగా అర్థం చేసుకోవడం వలన సెన్సర్లు లొకేషన్‌ను గుర్తించి, సమీక్ష మరియు పరిశోధన చేపట్టడానికి అవసరమైన లాగ్‌లను సేకరించడానికి వీలవుతుంది. ప్రస్తుతం SIEM కొంతవరకు ఈ అవసరాలను తీరుస్తున్నా, అయితే సమస్య గుర్తింపు, పరిష్కారం కోసం ఒక సమగ్ర దృక్పథం అవసరం.

రెండో అడుగుగా - లాగ్‌లను అతి తక్కువ సమయంలో ప్రాసెస్ చేసి, తగిన ప్రతిపాదనలతో, మరింత లోతుగా పరిశోధించడానికి అవసరమైన ప్రత్యామ్నాయాలతో ముందుకు రావడానికి అవసరమైన సెక్యూరిటీ అనలిటిక్స్ ఇంజన్‌ను కలిగి ఉండడం.

మూడో అడుగు- ఆన్ ద ఫ్లై డీప్ ప్యాకెట్ ఇన్‌స్పెక్షన్ తో వైర్ స్పీడ్ పెర్ఫామన్స్‌ను డెలివరీ చేసే UTM పరిష్కారాలను ఉపయోగించుకుంటున్న ప్రస్తుతం అమలు చేస్తున్న డీప్ ప్యాకెట్ ఇన్‌స్పెక్షన్ విధానాలను పరిశీలించడం.

నాలుగో అడుగు - మాల్‌వేర్‌ను గుర్తించడానికి, సమీక్షించడానికి, ఫోరెన్సిక్ సమస్యల పరిష్కారం కోసం అవసరమైన పరికరాలు, సాంకేతిక పరిజ్ఞానం, డాటాను కలిగి ఉండడం.

పై సమస్యలను పరిష్కరించడానికి ఏర్పాటు చేసిన పరిష్కార వ్యవస్థ సులభంగా లభించడంతో పాటు మెరుగైన ప్రదర్శన, అవసరమైతే దాని పరిమాణాన్ని పెంచుకొనగలిగే అవకాశాలు కూడా ఉండాలి.

తగిన విధంగా రూపొందించుకుని, ఈ క్రింది వాటిపై ఆలోచించాలి:

- SIEM ఆర్కిటెక్చర్ మరియు యూజ్ కేసెస్
- లాగ్ రకాలు, లాగింగ్ ప్రత్యామ్నాయాలు (డాటా సోర్సెస్, SIEMలోకి జోడించడం)
- వివిధ రకాల లాగ్‌లు, లాగింగ్ ప్రత్యామ్నాయాలను SIEMలోకి జోడించడం, టికెటింగ్/వర్క్ ఫ్లో/కేస్ మేనేజ్‌మెంట్, అన్‌స్ట్రక్చర్డ్ డాటా/బిగ్ డాటా, రిపోర్టింగ్/డ్యాష్ బోర్డ్, యూజ్ కేసెస్/రూల్ డిజైన్ (రిస్క్ మరియు కంప్లయన్స్ అవసరాలు/డ్రైవర్లకు అనుగుణంగా
- కస్టమైజేషన్) మొద.
- ప్రభావం, సామర్థ్యం పెంచడానికి సాంకేతిక పరిజ్ఞానం (ట్రాకింగ్ ఆఫ్ మెట్రిక్స్, అనలిటిక్స్, స్కోర్‌బోర్డులు, డాష్ బోర్డులు మొద.)

ప్రాసెస్ సంబంధిత అంశాలు:

CSCని డిజైన్ చేసే సమయంలో గుర్తు పెట్టుకోవాల్సిన ఒక ముఖ్యమైన విషయం ఒక భద్రతా లోపం యొక్క మూల కారణాన్ని తెలుసుకోవడానికి, భవిష్యత్తులో అలాంటి దాడులు తిరిగి జరక్కుండా చూడడానికి అనుసరించాల్సిన విధానాలను అర్థం చేసుకోవడం చాలా ముఖ్యం.

ఇన్సిడెంట్ మేనేజ్‌మెంట్

సెక్యూరిటీ ఆపరేషన్స్ నేపథ్యంలో ప్రాబ్లమ్ మేనేజ్‌మెంట్

సెక్యూరిటీ ఆపరేషన్స్‌కు పరిష్కారం కోసం వల్నరబిలిటీ అండ్ ప్యాచ్ మేనేజ్‌మెంట్ సెక్యూరిటీ రిస్క్ మేనేజ్‌మెంట్, అవైలబిలిటీ మేనేజ్‌మెంట్, కంప్యూటర్ ఫోరెన్సిక్ అండ్ రెస్పాన్స్ మేనేజ్‌మెంట్ లాంటి ముఖ్యమైన మెట్రిక్‌లను బాగా అర్థం చేసుకోవాలి.

ప్రజా సంబంధిత సమస్యలు

CSC 24 గంటలూ సమర్థమైన, తగిన అర్హత కలిగిన సిబ్బంది చేత నిర్వహించబడుతూ, పర్యవేక్షించబడుతూ ఉంటుంది. అందువల్ల దీని కోసం ఒక తగిన వ్యవస్థను రూపొందించుకోవడం అవసరం.

తగిన శిక్షణ పొందిన సిబ్బంది చేత 24 గంటల లెవల్ -1 పర్యవేక్షణ అన్నది మొదటి దశ. సమస్యల ను పరిష్కరించడానికి వారికి శిక్షణ, ప్రొడక్ట్/వెండర్ సర్టిఫికేషన్ అవసరం.

లెవల్-2లో ఉన్నత స్థాయి శిక్షణ పొందిన సిబ్బంది నిర్దిష్టమైన నెట్‌వర్క్, డాటా సెక్యూరిటీ, ఎండ్ పాయింట్ సెక్యూరిటీ మొద. వాటిపై దృష్టి కేంద్రీకరిస్తారు. వీరు సమస్య మూలకారణాన్ని సమీక్షించి, వాటికి పరిష్కారాలను కనుగొంటారు.

లెవల్-3 సిబ్బందిని SoC అనలిస్టులు అంటారు. వీరికి సెక్యూరిటీ మీద, డీప్ ప్యాకెట్ సమీక్ష, IOC సేకరణ, సాక్ష్యాల సేకరణ కోసం ఫోరెన్సిక్ నాలెడ్జి మీద, మాల్‌వేర్ రివర్స్ ఇంజనీరింగ్ మీద లోతైన అవగాహన ఉంటుంది. వీరు అవసరమైనప్పుడు కస్టమ్ స్క్రిప్టులు రాయగలిగిన వారై ఉంటారు.

పై కార్యక్రమాలను నిర్వహించే సిబ్బంది అందరికీ ఆయా బ్యాంకుల ఉత్పత్తుల గురించి, సేవల గురించి మంచి అవగాహన ఉండాలి.

- SOCకి అవసరమైన వ్యక్తులు/మేనేజింగ్ స్టాఫ్‌ను నియమించుకోవడంలో ఎదురయ్యే
- సమస్యల విషయంలో బ్యాంకులు ప్రాక్టికల్‌గా ఆలోచించాలి. ఇది బ్యాంకులోని ఇతర కార్యక లాపాల మాదిరి కాదు. ఇందుకోసం ఒక భిన్నమైన దృక్పథాన్ని అనుసరించాలి. ఎందుకంటే అలాంటి నైపుణ్యాలు కలిగిన వ్యక్తులను గుర్తించి, వారిని అట్టిపెట్టుకోవడం చాలా కష్టం.
- SOCలో సిబ్బంది - వారు 24X7X365, షిఫ్టులు, బిజినెస్ అవర్స్‌లో మాత్రమేనా అని వర్గీకరించారు.
- ఉపయోగించే నమూనా - తగిన నైపుణ్యాలు కలిగిన సిబ్బందిని/సర్వీస్ ప్రొవైడర్‌ను గుర్తించడం
- సొంత సిబ్బందికి శిక్షణ/సిబ్బందికి సర్వీస్ ప్రొవైడర్ ద్వారా శిక్షణ
- శిక్షణ పొందిన/తగిన నైపుణ్యాలు కలిగిన సిబ్బంది తమ వద్దే కొనసాగేందుకు తగిన పరిహారం/ ప్రోత్సాహకాలు
- SOC ఏ విధంగా పని చేస్తుందన్నది పరిశీలించేందుకు అవసరమైన కొలబద్ధలు
- సామర్థ్య పెంపు కార్యక్రమాల ద్వారా సిబ్బంది సంఖ్యను పెంచుకుంటూ, వారు తమతోనే

కొనసాగేలా చేయడం

బయటి ఇంటిగ్రేషన్

బ్యాంకు కస్టమర్లకు సేవలు అందజేసే విషయంలో అనేక మంది భాగస్వాములు ప్రత్యక్షంగా లేదా పరోక్షంగా భాగం పంచుకుంటారు. వారికి ఉన్న అనుభవం చాలా ఉపయోగపడుతుంది. ఉదాహరణకు టెక్నాలజీ విషయంలో ప్రొడక్ట్ వెండర్లు, ఇతర ముఖ్య భాగస్వాములు వివిధ వనరుల నుంచి అందించే విపత్తు సమాచారాన్ని అందిస్తారు. ఇతర బ్యాంకుల నుంచి, ఫైనాన్షియల్ ఎకో సిస్టమ్ నుంచి అందే భద్రతాపరమైన సమాచారం చాలా ఉపయోగపడుతుంది.

బ్యాంకుకు చెందిన సైబర్ రెస్పాన్స్ సెల్స్ , CERT-In, ఇతర టెలికాం సర్వీస్ ప్రొవైడర్లు బ్యాంకింగ్ పరిశ్రమలో వస్తున్న మార్పులపై విలువైన సూచనలు అందిస్తారు.

అమలు చేయదగిన నమూనా గుర్తింపు

ముందుగా తీసుకోవాల్సిన నిర్ణయాలలో BOOను లేదా ఔట్ సోర్సింగ్ నమూనాను గమనించడం ముఖ్యమైనవి. ఒకసారి అమలు చేయడం ప్రారంభించిన తర్వాత ఆ నిర్ణయాన్ని వెనక్కి తీసుకోవడం కష్టం కావడం వల్ల ఇది చాలా ముఖ్యం.

- SOC ఇన్-హౌస్‌లోనే ఉండాలా లేదా ఔట్‌సోర్స్ చేయాలా?
- అది కేవలం ఇంటర్నెట్ ఎదుర్కొనే వాతావరణాన్ని మాత్రమే ఎదుర్కోవాలా లేక మొత్తం ఐటీ ఇన్‌ఫ్రాస్ట్రక్చర్‌నా?
- ప్రతి బ్యాంక్ తన సొంత విపత్తు నివారణ వ్యవస్థను ఏర్పాటు చేసుకోవాలా లేక అన్నీ కలిసి కన్సార్టియం విధానాన్ని ఏర్పాటు చేసుకోవాలా?
- బ్యాంక్ విపత్తులకు గురయ్యే అవకాశాలను దృష్టిలో పెట్టుకోవాలా?

SOC కోసం ప్రణాళికలు రూపొందించుకునే సమయంలో ఈ క్రింది వాటిని దృష్టిలో పెట్టుకోవాలి.

ఎ) SOC నిర్వహణ కోసం ప్రత్యేక నైపుణ్యాలు అవసరం

బి) అనుభవం కలిగిన సిబ్బందిని పొందడం కష్టం

సి) ఎక్కువ సమయం, శిక్షణ కోసం ఎక్కువ ఖర్చు

డి) తగిన పరిహార వ్యూహాల రూపకల్పన

ఇ) నిరంతరం అప్ టు డేట్ శిక్షణ పొందడం, తగిన కెరీర్ ప్రత్యామ్నాయాలు లేకపోవడం, తీవ్రమైన ఒత్తిడి ఉండడం తదితర కారణాల వల్ల సిబ్బందిని అట్టిపెట్టుకోవడం చాలా కష్టం.

ఎఫ్) ఇతర సహాయ సహకారాలకు సంబంధించి ఈ క్రింది వనరులు అవసరం (i) SIEM/ డ్యాష్ బోర్డ్/ రిపోర్టింగ్ వర్క్ ఫ్లో/కేస్ మేనేజ్‌మెంట్ సిస్టమ్స్ లాంటి SOC ఆపరేషన్స్‌ను నిర్వహించే సిస్టమ్‌ల అడ్మినిస్ట్రేషన్ (ii) విపత్తు ఇంటలిజెన్స్‌ను రిసీవ్ చేసుకోవడం, జోడించడం, ఉపయోగించడం (iii) కమ్యూనికేషన్ స్ట్రాటజీని అమలు చేయడం (iv) SOC సిబ్బంది సూపర్‌విజన్/మేనేజ్‌మెంట్ (v) రెగ్యులేటర్లు/చట్టాలు/నియంత్రణల ప్రమాణాలను అందుకోవడంలాంటి ఇతర సహాయక కార్యకలాపాల వనరులు అవసరం.