ALABAMA SLCGP SKETCHBOOK

PLANNING TOGETHER.

BUILDING RESILIENT COMMUNITIES.

STRONGER TOGETHER. ♥ SAFER TOMORROW.

1. THE PROGRAM

A FRAMEWORK FOR COLLABORATION, FUNDING, AND COMMUNITY RESILIENCE.

WHAT IT IS

THE STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP) SUPPORTS PLANNING, PREPAREDNESS, AND CAPACITY BUILDING ACROSS ALABAMA.

GOALS

- STRENGTHEN CYBERSECURITY POSTURE
- BUILD LOCAL CAPACITY
- ENHANCE COLLABORATION
- IMPROVE RESILIENCE

FOCUS AREAS

- PLANNING
- TRAINING & AWARENESS
- EQUIPMENT & TOOLS
- EXERCISES & EVALUATION

STRONGER TOGETHER.

SAFER TOGETHER.

> "EMPOWERING ALABAMA COMMUNITIES TO PREPARE, RESPOND, AND THRIVE IN AN EVER-EVOLVING THREAT LANDSCAPE."

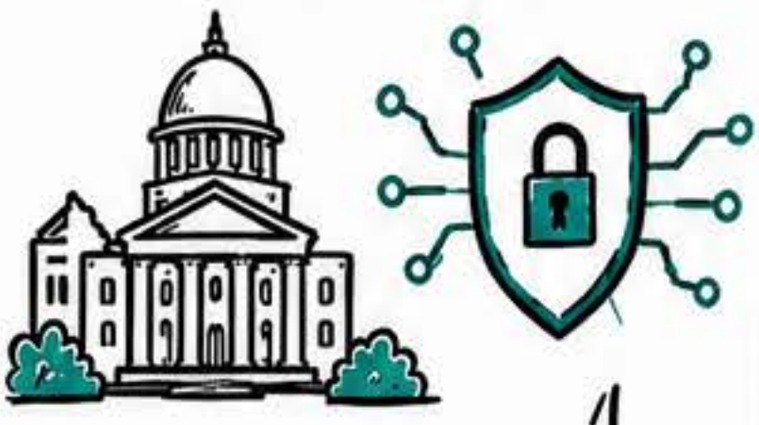
ALABAMA SLCGP

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM

INVESTING IN A SECURE ALABAMA

WHAT IS SLCGP?

A FEDERAL GRANT PROGRAM THROUGH THE U.S. DEPARTMENT OF HOMELAND SECURITY (DHS) DESIGNED TO STRENGTHEN CYBERSECURITY CAPABILITIES AT THE STATE, LOCAL, TRIBAL, AND TERRITORIAL LEVEL.



THE GOAL

BUILD STRONGER CYBER DEFENSES, REDUCE RISK, AND PROTECT CRITICAL SERVICES AND COMMUNITIES.

PREPARE • PROTECT • RESPOND • RECOVER

WHO CAN APPLY?

- 6 U.S.C. § 101(13) entities
- COUNTIES
- MUNICIPALITIES
- TRIBAL GOVERNMENTS
- PUBLIC AUTHORITIES
- SCHOOL DISTRICTS
- HIGHER EDUCATION

STRONGER TOGETHER.
SAFER TOGETHER.

FUNDING

- FEDERAL FUNDING ADMINISTERED BY STATE OF ALABAMA
- NO LOCAL ENTITY COST SHARE MATCH
- FOUR ROUNDS OF FUNDS THROUGH 2029

ALLOWABLE USES

- RISK ASSESSMENTS & PLANNING
- CYBERSECURITY TOOLS & TECHNOLOGIES
- TRAINING & WORKFORCE DEVELOPMENT
- POLICIES, PROCEDURES & GOVERNANCE
- INCIDENT RESPONSE & CAPABILITY BUILDING

PRIORITY AREAS

- GOVERNANCE & PLANNING
- RISK MANAGEMENT
- THREAT DETECTION & PROTECTION
- INCIDENT RESPONSE & RECOVERY
- WORKFORCE & CYBER AWARENESS

THE PROCESS

1. **PLANNING** — IDENTIFY NEEDS ALIGN WITH PRIORITIES
2. **APPLY** — SUBMIT COMPLETE APPLICATION THROUGH THE PORTAL
3. **REVIEW** — APPLICATIONS AND CONSENT FORMS VALIDATED
4. **ASSESSMENT** — MCCRARY INSTITUTE GUIDES APPLICANTS TO ONBOARD PROJECTS
5. **IMPLEMENT & REPORT** — EXECUTE PROJECT & REPORT RESULTS

EXPECTED OUTCOMES

- STRONGER DEFENSES AGAINST CYBER THREATS
- REDUCED RISK TO CRITICAL SYSTEMS & DATA
- MORE RESILIENT COMMUNITIES
- A SAFER, STRONGER ALABAMA

KEY REMINDERS

- FOLLOW GUIDELINES AND CHECK THE BOXES
- SUBMIT COMPLETE APPLICATIONS AND TAKE THE MCCRARY CALL
- MCCRARY WILL GUIDE AND ALIGN PROJECT PRIORITIES
- MEASURE IMPACT & REPORT RESULTS

A PARTNERSHIP FOR A SECURE FUTURE

FEDERAL RESOURCES.
STATE LEADERSHIP.
LOCAL IMPACT.
STRONGER TOGETHER.

LEARN MORE

VISIT
SLCGP.ALABAMA.GOV

PROGRAM GUIDANCE, APPLICATION RESOURCES, NEWS & UPDATES

QUESTIONS?
CONTACT US THROUGH THE WEBSITE CONTACT FORM

CYBERSECURITY IS A SHARED RESPONSIBILITY. LET'S PROTECT ALABAMA TOGETHER!

ALABAMA'S SLCGP CYBERSECURITY PLAN

SECURE TODAY. ENABLE TOMORROW.

PROTECTING PEOPLE, DATA, AND SERVICES THAT POWER ALABAMA'S FUTURE.

OUR MISSION

STRENGTHEN THE CYBERSECURITY POSTURE OF ALABAMA'S STATE, LOCAL, AND TRIBAL GOVERNMENTS THROUGH COLLABORATION, RISK MANAGEMENT, AND SHARED RESILIENCE.

OUR VISION

A CONNECTED ALABAMA WHERE GOVERNMENT SERVICES ARE TRUSTED, SECURE, AND RESILIENT BY DESIGN.

OUR GUIDING PRINCIPLES

- PEOPLE FIRST
- SECURITY BY DESIGN
- COLLABORATION
- TRANSPARENCY
- CONTINUOUS IMPROVEMENT

CORE CONCEPTS

RISK-BASED APPROACH
FOCUS ON WHAT MATTERS MOST.

SHARED RESPONSIBILITY
CYBERSECURITY IS EVERYONE'S JOB.

DEFENSE IN DEPTH
MULTIPLE LAYERS. STRONGER TOGETHER.

CONTINUOUS MONITORING
SEE IT. STOP IT. REPORT IT.

RESILIENCE & RECOVERY
PLAN AHEAD. BOUNCE BACK STRONGER.

KEY OUTCOMES

- REDUCED CYBER RISK ACROSS STATE, LOCAL, AND TRIBAL ENTITIES
- FASTER DETECTION AND RESPONSE
- STRONGER PARTNERSHIPS AND INFORMATION SHARING
- COMPLIANCE AND ACCOUNTABILITY
- ENHANCED PUBLIC TRUST AND SERVICE CONTINUITY

CYBERSECURITY FRAMEWORK

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
KNOW YOUR ASSETS & RISKS	IMPLEMENT SAFEGUARDS	FIND THREATS EARLY	TAKE ACTION QUICKLY	RESTORE & IMPROVE

STRATEGIC INVESTMENT AREAS

1. **PEOPLE & CULTURE**
   BUILD A SKILLED, AWARE, AND EMPOWERED WORKFORCE
2. **TECHNOLOGY & TOOLS**
   MODERNIZE, AUTOMATE, AND STRENGTHEN DEFENSES
3. **THREAT INTELLIGENCE & SHARING**
   SHARE. COLLABORATE. STAY AHEAD.
4. **POLICIES & GOVERNANCE**
   ESTABLISH CLEAR RULES AND OVERSIGHT
5. **THIRD-PARTY RISK MANAGEMENT**
   REDUCE RISK ACROSS OUR SUPPLY CHAIN
6. **BUSINESS CONTINUITY & DR**
   PREPARE FOR DISRUPTION. PROTECT WHAT MATTERS.

OUR PROCESS

1. **ASSESS** — UNDERSTAND CURRENT STATE & RISKS
2. **PLAN** — PRIORITIZE ACTIONS & RESOURCES
3. **IMPLEMENT** — DEPLOY CONTROLS & CAPABILITIES
4. **MONITOR** — TRACK, MEASURE & REPORT
5. **IMPROVE** — ADAPT & EVOLVE CONTINUOUSLY

TOGETHER WE ARE STRONGER

STATE AGENCIES · LOCAL GOVERNMENTS · TRIBAL GOVERNMENTS · PARTNERS & VENDORS · CITIZENS OF ALABAMA

THREATS WE FACE

PHISHING & SOCIAL ENGINEERING · RANSOMWARE · INSIDER THREATS · SUPPLY CHAIN ATTACKS · CLOUD RISKS · VULNERABILITIES & EXPLOITS

CYBER THREATS DON'T DISCRIMINATE. PREPARATION DOES.

BY THE NUMBERS

- **60%+** OF SMALL GOVT ENTITIES EXPERIENCED A CYBER INCIDENT IN THE LAST 12 MONTHS*
- **95%** OF BREACHES ARE CAUSED BY HUMAN ERROR, SYSTEMS, OR SOCIAL ENGINEERING*
- **$4.88M** AVERAGE COST OF A DATA BREACH IN THE PUBLIC SECTOR*
- CYBER CRIME COSTS **$10.5 TRILLION** BY 2025*

*SOURCES: IBM, TREND MICRO, VERIZON, CISA, NIST

ACTIONABLE TAKEAWAYS

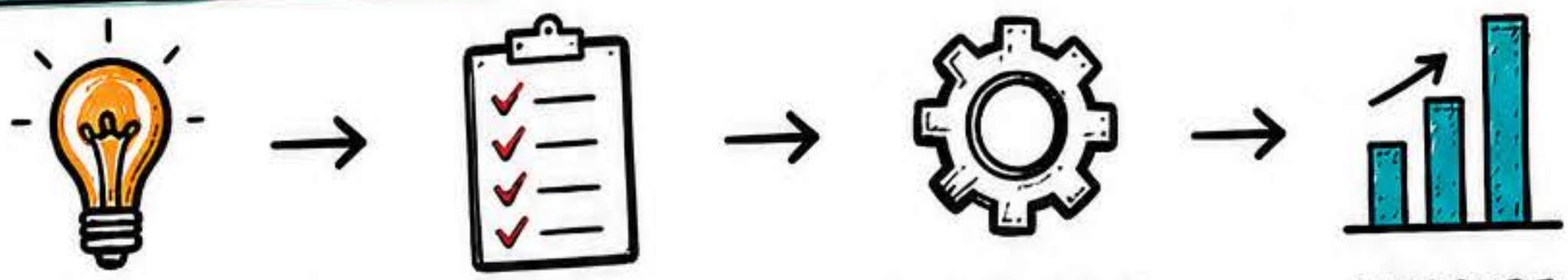
- KNOW YOUR ROLE. WE ALL MAKE A DIFFERENCE.
- KEEP SYSTEMS UPDATED. PATCH TODAY. PROTECT TOMORROW.
- THINK BEFORE YOU CLICK. STOP. VERIFY. REPORT.
- PROTECT DATA. CLASSIFY IT. SECURE IT.
- REPORT SUSPICIOUS ACTIVITY. SEE IT. SAY IT. STOP IT.
- PLAN. PRACTICE. PREPARE. RESILIENCE IS BUILT BEFORE A CRISIS.

A STRONGER CYBER POSTURE. BETTER SERVICES. A SAFER ALABAMA.

2. THE PROJECTS

TURNING IDEAS INTO ACTION.
BUILDING A STRONGER ALABAMA.

PROJECT LIFECYCLE



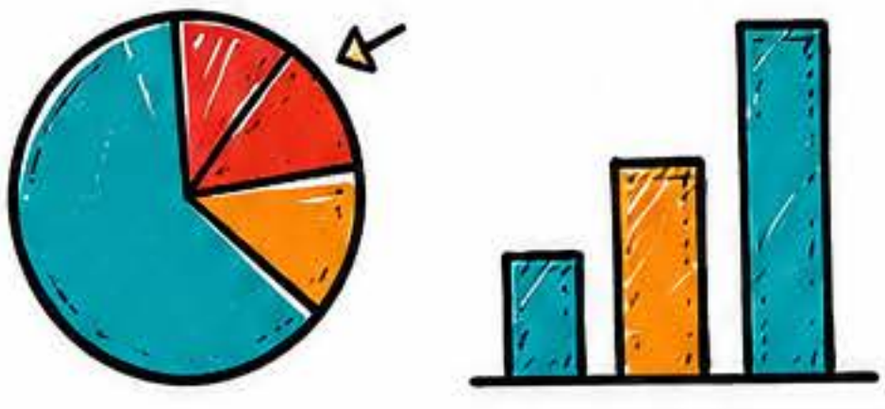
TYPES OF PROJECTS

- RISK ASSESSMENTS
- CYBERSECURITY PLANS
- TRAINING & EXERCISES
- TECHNOLOGY ENHANCEMENTS
- OUTREACH & AWARENESS

SUCCESS FACTORS

- ☑ CLEAR OBJECTIVES
- ☑ STAKEHOLDER INPUT
- ☑ EFFECTIVE PLANNING
- ☑ STRONG EXECUTION
- ☑ MEASURABLE RESULTS

BY THE NUMBERS



INVESTING IN PROJECTS TODAY
CREATES RESILIENT COMMUNITIES
FOR TOMORROW.

★ GOOD PROJECTS SOLVE PROBLEMS.

★ GREAT PROJECTS STRENGTHEN COMMUNITIES.

CYBERSECURITY PERFORMANCE GOALS (CPG) ASSESSMENT

A ROADMAP TO STRONGER CYBER RESILIENCE

WHAT IS IT?

A STRUCTURED ASSESSMENT THAT MEASURES YOUR ORGANIZATION'S CYBERSECURITY MATURITY AGAINST GLOBALLY RECOGNIZED PERFORMANCE GOALS.

WHY IT MATTERS

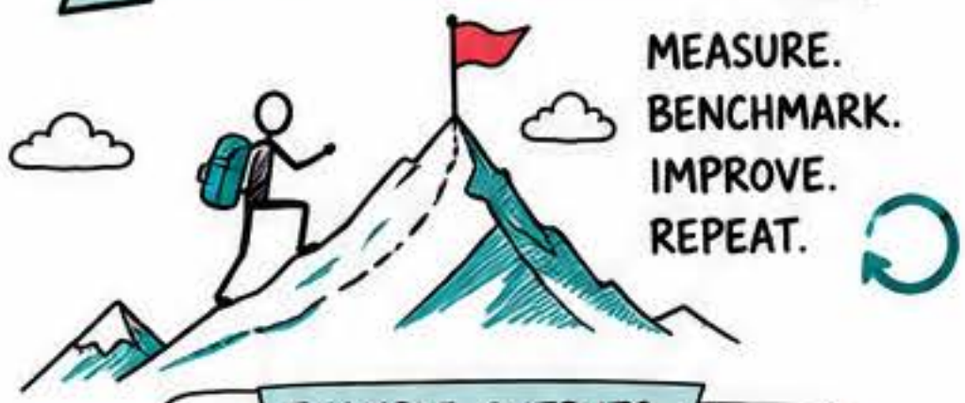
- ALIGN CYBER EFFORTS WITH BUSINESS OBJECTIVES
- IDENTIFY GAPS & PRIORITIZE INVESTMENTS
- REDUCE RISK & IMPROVE RESILIENCE
- DEMONSTRATE ACCOUNTABILITY TO STAKEHOLDERS

CORE DOMAINS (THE CPGs)

1. Access Control Management
2. Asset Management
3. Data Protection
4. Vulnerability Management
5. Threat Detection & Incident Response
6. Business Continuity
7. Workforce Cybersecurity Management
8. Governance & Risk Management

HOW IT WORKS (THE ASSESSMENT PROCESS)

1. **PREPARE** — DEFINE SCOPE, OBJECTIVES & STAKEHOLDERS
2. **ASSESS** — COLLECT EVIDENCE THROUGH INTERVIEWS, DOCUMENT REVIEW & TOOLS
3. **SCORE** — RATE MATURITY AGAINST EACH CPG (1–5 SCALE)
4. **ANALYZE** — IDENTIFY STRENGTHS, GAPS & PRIORITY AREAS
5. **RECOMMEND** — BUILD ACTION PLAN WITH PRACTICAL, RISK-BASED STEPS
6. **IMPROVE & REASSESS** — IMPLEMENT, TRACK PROGRESS & REPEAT REGULARLY



MEASURE.
BENCHMARK.
IMPROVE.
REPEAT.

MATURITY LEVELS

5. **OPTIMIZED** — CONTINUOUSLY IMPROVING WITH QUANTITATIVE MEASUREMENT
4. **MANAGED** — WELL-DEFINED PROCESSES MEASURED & PERFORMING CONSISTENTLY
3. **DEFINED** — STANDARD PROCESSES IN PLACE & COMMUNICATED ACROSS THE ORGANIZATION
2. **DEVELOPING** — PROCESSES ARE AD-HOC AND NOT YET STANDARDIZED
1. **INITIAL** — LIMITED OR UNDEFINED PROCESSES; HIGH RISK

EXAMPLE OUTPUTS

- CPG MATURITY SCORECARD
- DOMAIN & OVERALL SCORES
- PRIORITY GAP ANALYSIS
- ACTION PLAN & ROADMAP
- BENCHMARKING (OVER TIME OR PEERS)

KEY INSIGHTS & BENEFITS

- ✓ GET A CLEAR VIEW OF YOUR CYBERSECURITY MATURITY
- ✓ FOCUS RESOURCES WHERE RISK IS HIGHEST
- ✓ IMPROVE DECISION-MAKING WITH DATA-DRIVEN INSIGHTS
- ✓ SUPPORT COMPLIANCE & REGULATORY EXPECTATIONS
- ✓ BUILD TRUST WITH CUSTOMERS, PARTNERS & EXECUTIVES

WHO USES IT?

- CISOS & SECURITY TEAMS
- RISK & COMPLIANCE LEADERS
- IT & OPS LEADERS
- BUSINESS EXECUTIVES

TAILORED FOR ORGANIZATIONS OF ALL SIZES & INDUSTRIES

KEY TAKEAWAYS / ACTIONS

- ☑ UNDERSTAND YOUR CURRENT MATURITY LEVEL
- ☑ PRIORITIZE WHAT MATTERS MOST
- ☑ CREATE A REALISTIC ROADMAP
- ☑ ALIGN TEAMS & STAKEHOLDERS
- ☑ MEASURE PROGRESS & ADAPT

ASSESS. ACT. ADVANCE.

BY THE NUMBERS

60% OF ORGS LACK VISIBILITY INTO THEIR CYBER MATURITY*

2.6X MORE LIKELY TO REDUCE BREACH RISK WITH MATURITY

80% OF BREACHES INVOLVE BASIC PREVENTABLE CONTROLS**

THE CPG ASSESSMENT TURNS CYBERSECURITY INTO A MEASURABLE ADVANTAGE.

*SOURCE: IBM SECURITY **SOURCE: VERIZON DBIR

STRONGER GOALS. SMARTER SECURITY. STRONGER ORGANIZATION.

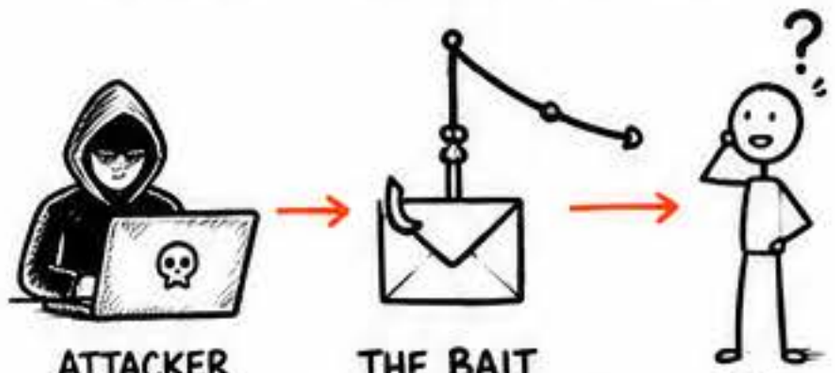
SECURITY AWARENESS & PHISHING TRAINING

WHY IT MATTERS

- HUMAN ERROR CAUSES **90%+** OF BREACHES
- PHISHING IS THE **#1** ATTACK VECTOR
- AWARE EMPLOYEES ARE OUR STRONGEST DEFENSE

WHAT IS PHISHING?

ATTACKERS PRETEND TO BE SOMEONE YOU TRUST TO STEAL INFORMATION, MONEY OR ACCESS.



COMMON PHISHING TYPES

- **EMAIL PHISHING**
- FAKE EMAILS THAT CREATE URGENCY OR CURIOSITY

- **SMISHING**
- PHISHING VIA TEXT MESSAGES

- **VISHING**
- PHONE CALLS TO TRICK YOU INTO SHARING INFO

- **CLONE PHISHING**
- LEGIT EMAILS COPIED WITH MALICIOUS LINKS

- **BAITING**
- PHYSICAL ITEMS (USB) LEFT TO TEMPT YOU

RED FLAGS WATCH FOR

SENSE OF URGENCY
"ACT NOW!"
"ACCOUNT WILL BE CLOSED!"

UNKNOWN SENDER
CHECK THE FULL EMAIL ADDRESS

SUSPICIOUS LINKS
DON'T CLICK LINKS OR DOWNLOAD ATTACHMENTS

POOR GRAMMAR OR SPELLING
UNPROFESSIONAL LANGUAGE

UNEXPECTED REQUESTS
FOR INFO, LOGIN, PAYMENT OR GIFT CARDS

WHAT YOU SHOULD DO

PAUSE & THINK
DON'T REACT IMMEDIATELY

VERIFY
CHECK WITH THE SENDER THROUGH A DIFFERENT CHANNEL

DON'T CLICK
ON LINKS OR OPEN UNEXPECTED ATTACHMENTS

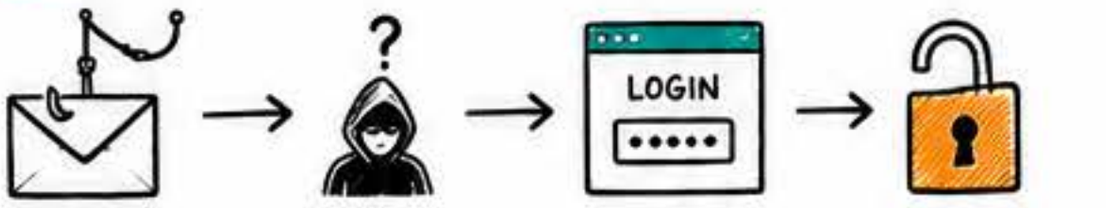
REPORT IT
REPORT SUSPICIOUS ACTIVITY TO IT / SECURITY TEAM

WHEN IN DOUBT, REPORT IT OUT!
IT HELPS PROTECT EVERYONE.

SMALL ACTIONS. BIG IMPACT.

WE ALL PLAY A PART IN KEEPING OUR ORGANIZATION SAFE!

THE PHISHING ATTACK CHAIN



1. **BAIT** — ATTACKER SENDS PHISHING MESSAGE
2. **TRICK** — YOU ARE TRICKED INTO CLICKING OR SHARING INFO
3. **COMPROMISE** — CREDENTIALS OR DATA IS STOLEN
4. **IMPACT** — UNAUTHORIZED ACCESS, DATA LOSS, FINANCIAL DAMAGE, REPUTATION HIT

BUILDING A SECURITY-FIRST CULTURE

LEAD BY EXAMPLE
MAKE SECURITY EVERYONE'S PRIORITY

KEEP LEARNING
THREATS EVOLVE. SO SHOULD WE.

RECOGNIZE & REWARD
CELEBRATE GOOD HABITS AND REPORTS

WORK TOGETHER
STRONG TEAMS STOP ATTACKS.

AWARE TODAY.
SAFE TOMORROW.
STRONGER TOGETHER.

BY THE NUMBERS

90%+ OF BREACHES ARE CAUSED BY HUMAN ERROR

3 IN 4 EMPLOYEES CAN'T SPOT A SOPHISTICATED PHISHING EMAIL

$4.88M AVERAGE COST OF A DATA BREACH (IBM 2023)

SOURCES: IBM, VERIZON DBIR, PROOFPOINT

ACTION PLAN — WHAT YOU CAN DO TODAY

1. **COMPLETE TRAINING**

STAY INFORMED STAY SAFE

2. **CHECK BEFORE YOU CLICK**

WHEN IN DOUBT, DON'T CLICK

3. **USE STRONG PASSWORDS**


LONG, UNIQUE, AND SECURE

4. **ENABLE MFA**


EXTRA STEP. EXTRA SECURITY.

5. **KEEP SYSTEMS UPDATED**

UPDATES CLOSE SECURITY GAPS

6. **REPORT SUSPICIOUS ACTIVITY**

SPEAK UP. MAKE AN IMPACT.

IF YOU SEE SOMETHING, SAY **SOMETHING!**

ENDPOINT DETECTION AND RESPONSE (EDR)

WHAT IS EDR?

EDR IS A CYBERSECURITY SOLUTION THAT MONITORS, DETECTS, INVESTIGATES AND RESPONDS TO THREATS ON ENDPOINTS IN REAL TIME.

ENDPOINTS INCLUDE:

- LAPTOPS & DESKTOPS
- SERVERS
- MOBILE DEVICES
- IOT DEVICES

WHY IT MATTERS

ENDPOINTS ARE THE #1 TARGET FOR ATTACKERS

DETECTS SOPHISTICATED THREATS THAT BYPASS TRADITIONAL AV

REDUCES DWELL TIME AND LIMITS DAMAGE

IMPROVES SECURITY VISIBILITY & INCIDENT RESPONSE

KEY CAPABILITIES

REAL-TIME MONITORING
CONTINUOUSLY WATCHES ENDPOINT ACTIVITY

THREAT DETECTION
USES BEHAVIOR ANALYTICS, MACHINE LEARNING & THREAT INTEL

AUTOMATED RESPONSE
CONTAINS THREATS AUTOMATICALLY OR WITH ONE CLICK

INVESTIGATION & FORENSICS
DEEP VISIBILITY TO UNDERSTAND THE FULL ATTACK STORY

REMEDIATION & RECOVERY
REMOVE THREATS, ROLL BACK CHANGES & RESTORE SYSTEMS

HOW EDR WORKS

1. **COLLECT**
   AGENT ON ENDPOINT COLLECTS DATA
   10101 01010
2. **ANALYZE**
   BEHAVIOR ANALYSIS, THREAT INTEL & ML DETECT ANOMALIES
3. **DETECT**
   IDENTIFY MALICIOUS ACTIVITY OR INDICATORS OF COMPROMISE
4. **RESPOND**
   AUTOMATE OR GUIDE ACTIONS TO CONTAIN THE THREAT
5. **RECOVER**
   ELIMINATE THREAT, REMEDIATE & RESTORE NORMAL OPERATIONS

EDR ARCHITECTURE

COMMON THREATS EDR HELPS STOP

- MALWARE & RANSOMWARE
- FILELESS ATTACKS
- LATERAL MOVEMENT
- PRIVILEGE ESCALATION
- CREDENTIAL THEFT
- SUSPICIOUS ACTIVITIES & LIVING-OFF-THE-LAND TECHNIQUES

EDR VS TRADITIONAL AV

TRADITIONAL AV	EDR
SIGNATURE-BASED DETECTION	BEHAVIOR-BASED DETECTION
REACTIVE	PROACTIVE
LIMITED VISIBILITY	DEEP VISIBILITY & CONTEXT
MANUAL INVESTIGATION	GUIDED & AUTOMATED INVESTIGATION
PREVENTION FOCUSED	DETECTION, RESPONSE & HUNTING

BUSINESS IMPACT

- LOWER RISK OF BREACHES
- REDUCE INCIDENT RESPONSE TIME & COSTS
- MINIMIZE DOWNTIME & BUSINESS DISRUPTION
- IMPROVE COMPLIANCE & AUDIT READINESS
- STRENGTHEN CUSTOMER TRUST & REPUTATION

ACTIONABLE TAKEAWAYS

1. DEPLOY EDR ON ALL CRITICAL ENDPOINTS
2. INTEGRATE WITH YOUR SIEM & SECURITY STACK
3. TUNE ALERTS & AUTOMATION TO REDUCE NOISE
4. INVEST IN THREAT HUNTING & ANALYST TRAINING
5. REGULARLY REVIEW, TEST & IMPROVE RESPONSE PLANS

BY THE NUMBERS

68%
OF BREACHES INVOLVE ENDPOINTS
– VERIZON DBIR 2024

207
DAYS IS THE AVERAGE TIME ATTACKERS STAY UNDETECTED
– MANDIANT 2023

$4.88M
THE AVERAGE COST OF A DATA BREACH
– IBM 2024

EDR CAN REDUCE BREACH LIFECYCLE BY
50-60%
– FORRESTER

YOU CAN'T STOP EVERY ATTACK. BUT WITH EDR, YOU CAN DETECT EARLY, RESPOND FAST, AND STAY RESILIENT.

ROUTINE VULNERABILITY SCANNING

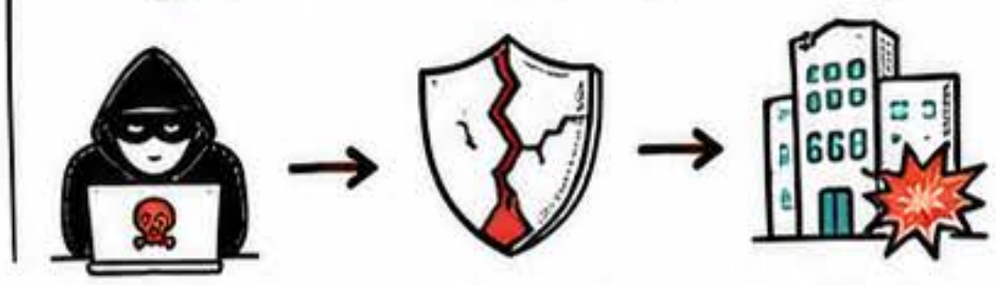
FIND IT EARLY. FIX IT FAST. STAY SECURE.

WHAT IS IT?

ROUTINE VULNERABILITY SCANNING IS THE PRACTICE OF REGULARLY USING AUTOMATED TOOLS TO IDENTIFY, ASSESS, AND REPORT SECURITY WEAKNESSES IN SYSTEMS, APPLICATIONS, AND NETWORKS.

THINK OF IT AS A HEALTH CHECK-UP FOR YOUR IT ENVIRONMENT.

WHY IT MATTERS



ATTACKERS DON'T TAKE DAYS OFF.

VULNERABILITIES DON'T STAY HIDDEN FOREVER.

EARLY DETECTION PREVENTS BREACHES, DOWNTIME & LOSSES.

KEY BENEFITS

- REDUCE RISK EXPOSURE
- PREVENT COSTLY BREACHES
- SUPPORT COMPLIANCE & AUDITS
- IMPROVE SECURITY POSTURE
- INCREASE VISIBILITY ACROSS ASSETS

TYPES OF SCANS

- **NETWORK SCAN** — FINDS OPEN PORTS, SERVICES & NETWORK WEAKNESSES.
- **APPLICATION SCAN** — IDENTIFIES FLAWS IN WEB APPS & APIS.
- **HOST-BASED SCAN** — CHECKS OS, SOFTWARE & CONFIGURATION ISSUES.

COMBINE ALL THREE FOR COMPLETE COVERAGE.

COMMON TARGETS

- CLOUD INFRASTRUCTURE
- SERVERS & ENDPOINTS
- NETWORK DEVICES
- WEB APPLICATIONS
- DATABASES
- CONTAINERS & APIS

RISK SEVERITY LEVELS

CRITICAL	Actively exploited or easily exploitable. Immediate action required.
HIGH	High impact, likely to be exploited. Fix ASAP.
MEDIUM	Moderate impact or harder to exploit. Plan to fix.
LOW	Low impact or difficult to exploit. Address when possible.
INFO	Informational findings or best practice items.

KEY INSIGHTS & STATS

60% OF BREACHES INVOLVE KNOWN, UNPATCHED VULNERABILITIES.
– VERIZON DBIR

UP TO **40%** OF VULNERABILITIES ARE HIGH OR CRITICAL SEVERITY.

85% OF ORGS SEE IMPROVED SECURITY AFTER ROUTINE SCANNING PROGRAMS.
– PONEMON INSTITUTE

THE SCANNING PROCESS

1. **DEFINE SCOPE** — Identify assets, IP ranges, apps, and credentials.
2. **DISCOVER** — The scanner probes and identifies live assets.
3. **ASSESS** — Checks for known vulnerabilities, misconfigurations & missing patches.
4. **ANALYZE & PRIORITIZE** — Rank findings based on severity, exploitability & business impact.
5. **REPORT** — Generate clear reports and communicate to stakeholders.
6. **REMEDIATE & VERIFY** — Fix issues and re-scan to confirm they're resolved.

SCAN FREQUENCY GUIDE

EXTERNALLY FACING ASSETS	WEEKLY
INTERNAL INFRASTRUCTURE	MONTHLY
WEB APPLICATIONS	WEEKLY–BIWEEKLY
AFTER CHANGES / PATCHES	IMMEDIATELY

THE MORE DYNAMIC YOUR ENVIRONMENT, THE MORE FREQUENT YOUR SCANS.

CHALLENGES TO WATCH

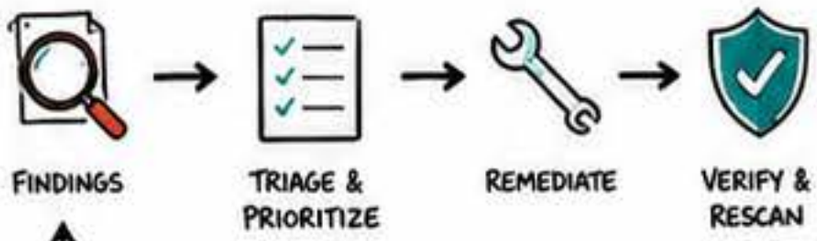
- TOO MANY FALSE POSITIVES
- POOR ASSET INVENTORY
- LACK OF SKILLED RESOURCES
- NOT SCANNING FREQUENTLY ENOUGH
- NO FOLLOW-UP OR REMEDIATION

BEST PRACTICES

- [x] KEEP ASSET INVENTORY ACCURATE
- [x] SCAN ON A REGULAR SCHEDULE
- [x] USE AUTHENTICATED SCANS
- [x] TUNE SCANS TO REDUCE NOISE
- [x] PRIORITIZE BASED ON RISK
- [x] INTEGRATE WITH TICKETING / SIEM
- [x] TRACK REMEDIATION TO CLOSURE
- [x] CONTINUOUSLY IMPROVE

CONSISTENCY + ACTION = STRONGER SECURITY

FROM FINDINGS TO ACTION



A SCAN WITHOUT ACTION IS JUST A REPORT.

TAKEAWAYS

- SCAN REGULARLY.
- PRIORITIZE SMARTLY.
- REMEDIATE QUICKLY.
- VERIFY CONTINUOUSLY.
- BUILD A CULTURE OF SECURITY.

ROUTINE SCANNING TODAY PREVENTS INCIDENTS TOMORROW.

PENETRATION TESTING

FIND IT. FIX IT. MAKE IT STRONGER.

WHAT IS IT?

PENETRATION TESTING IS AN AUTHORIZED, SIMULATED ATTACK ON SYSTEMS, APPLICATIONS, OR NETWORKS TO FIND SECURITY WEAKNESSES BEFORE ATTACKERS DO.

WHY IT MATTERS

- REDUCES SECURITY RISK
- PROTECTS DATA & REPUTATION
- MEETS COMPLIANCE REQUIREMENTS
- BUILDS CUSTOMER TRUST
- IMPROVES SECURITY POSTURE

CORE OBJECTIVES

- IDENTIFY VULNERABILITIES
- ASSESS IMPACT
- GAIN ACTIONABLE INSIGHTS
- PROVIDE REMEDIATION GUIDANCE
- VALIDATE SECURITY CONTROLS

PEN TESTING LIFECYCLE

1. **PLANNING & SCOPING**
   Define goals, scope, rules of engagement, and success criteria.
2. **INFORMATION GATHERING**
   Collect data about the target. (OSINT, DNS, WHOIS, scanning)
3. **VULNERABILITY ANALYSIS**
   Identify and prioritize weaknesses.
4. **EXPLOITATION**
   Attempt to exploit vulnerabilities to gain access.
5. **POST-EXPLOITATION**
   Maintain access, escalate privileges, pivot.
6. **REPORTING & REMEDIATION**
   Deliver findings, risk rating, and actionable fixes.

TYPES OF PEN TESTS

- **BLACK BOX** — Tester has no prior knowledge.
- **GRAY BOX** — Limited knowledge provided.
- **WHITE BOX** — Full knowledge of the system.
- **INTERNAL** — Test from inside the network.
- **EXTERNAL** — Test from outside the network.
- **TARGETED** — Focus on specific assets.

COMMON TARGETS

- WEB APPLICATIONS
- NETWORK INFRASTRUCTURE
- MOBILE APPS
- CLOUD ENVIRONMENTS
- API ENDPOINTS
- WIRELESS NETWORKS
- THICK CLIENT APPLICATIONS

KEY INSIGHTS

- MOST BREACHES EXPLOIT KNOWN VULNERABILITIES.
- BUSINESS LOGIC FLAWS ARE HARD TO DETECT WITH AUTOMATION.
- 80% OF BREACHES INVOLVE HUMAN ERROR.
- REGULAR TESTING + TIMELY REMEDIATION = LOWER RISK.
- SECURITY IS A CONTINUOUS PROCESS, NOT A ONE-TIME PROJECT.

COMMON ATTACK VECTORS

- SQL INJECTION
- CROSS-SITE SCRIPTING (XSS)
- BROKEN AUTHENTICATION
- INSECURE DIRECT OBJECT REFERENCES (IDOR)
- SECURITY MISCONFIGURATION
- SENSITIVE DATA EXPOSURE
- INSUFFICIENT ACCESS CONTROL
- COMMAND INJECTION

RISK RATING (EXAMPLE)

CRITICAL	IMMEDIATE THREAT. EASY TO EXPLOIT. SEVERE BUSINESS IMPACT.
HIGH	HIGH RISK. LIKELY TO BE EXPLOITED. SIGNIFICANT IMPACT.
MEDIUM	MODERATE RISK. MAY REQUIRE SPECIFIC CONDITIONS.
LOW	LOW RISK. LIMITED IMPACT OR HARD TO EXPLOIT.

PEN TESTING FRAMEWORK (PTES)

1. **PRE-ENGAGEMENT** — Define scope, gather info, establish ROE.
2. **INTELLIGENCE GATHERING** — Who, what, where, how?
3. **THREAT MODELING** — Identify risks & attack paths.
4. **VULNERABILITY ANALYSIS** — Find & validate weaknesses.
5. **EXPLOITATION** — Gain access & prove impact.
6. **POST EXPLOITATION** — Escalate, pivot, maintain access.
7. **REPORTING** — Document, rate & recommend remediation.

TOOLS OF THE TRADE

- **RECONNAISSANCE** — Nmap, Maltego, theHArvester
- **VULNERABILITY SCANNING** — Nessus, OpenVAS
- **WEB APPLICATION TESTING** — Burp Suite, OWASP ZAP
- **EXPLOITATION** — Metasploit, SQLMap
- **PASSWORD ATTACKS** — John the Ripper, Hashcat
- **NETWORK ANALYSIS** — Wireshark, Netcat

EXAMPLE: WEB APP TEST FLOW

RECON	SCAN	FIND	EXPLOIT	GAIN ACCESS	REPORT
• Nmap Scan • Discover subdomains	• Port Scan • Service Enum	• Crawl • Identify endpoints	• Exploit SQLi • Bypass Auth	• Shell Access • Priv Esc	• Findings • Impact • Fixes

ALWAYS OBTAIN AUTHORIZATION AND FOLLOW RULES OF ENGAGEMENT.

ACTIONABLE TAKEAWAYS

- TEST REGULARLY (INTERNAL & EXTERNAL).
- REMEDIATE HIGH & CRITICAL FINDINGS FIRST.
- PATCH, HARDEN, AND REDUCE ATTACK SURFACE.
- ENFORCE STRONG ACCESS CONTROLS & MFA.
- MONITOR, DETECT, RESPOND.
- BUILD A SECURITY-AWARE CULTURE.

STATS & TRENDS

60% OF SMALL BUSINESSES CLOSE WITHIN 6 MONTHS OF A CYBER ATTACK.
— NATIONAL CYBER SECURITY ALLIANCE

74% OF BREACHES INVOLVE THE HUMAN ELEMENT.
— VERIZON DBIR 2023

$4.88M GLOBAL AVERAGE COST OF A DATA BREACH IN 2023.
— IBM

RANSOMWARE ATTACKS INCREASED 70%+ IN 2023.
— CHAINALYSIS

> "THE BEST TIME TO FIND A VULNERABILITY ISN'T AFTER AN ATTACK. IT'S DURING A PEN TEST."

MULTI-FACTOR AUTHENTICATION

STRONGER ACCESS.
SMARTER SECURITY.

WHY IT MATTERS

PASSWORDS ALONE ARE NO LONGER ENOUGH.

- PHISHING
- CREDENTIAL STUFFING
- DATA BREACHES

81% OF BREACHES INVOLVE STOLEN OR WEAK PASSWORDS.
– VERIZON DBIR 2023

MFA CAN BLOCK 99.9% OF AUTOMATED ACCOUNT TAKEOVER ATTACKS.
– MICROSOFT

WHAT IS MFA?

MFA REQUIRES USERS TO VERIFY THEIR IDENTITY USING TWO OR MORE INDEPENDENT FACTORS. EVEN IF ONE FACTOR IS COMPROMISED, ATTACKERS STILL CAN'T GET IN.

STOP ATTACKS. PROTECT ACCOUNTS.

HOW MFA WORKS

1. USER ENTERS USERNAME — user.name
2. USER ENTERS PASSWORD — *******
3. USER PROVIDES SECOND (OR MORE) FACTOR — CODE (123 456), FINGERPRINT, SECURITY KEY
4. ACCESS GRANTED!

THE 3 FACTOR CATEGORIES

1. SOMETHING YOU KNOW
   - PASSWORD
   - PIN
   - SECURITY QUESTIONS
2. SOMETHING YOU HAVE
   - AUTHENTICATOR APP
   - SMS / EMAIL CODE
   - HARDWARE TOKEN
   - SMART CARD
3. SOMETHING YOU ARE
   - FINGERPRINT
   - FACE RECOGNITION
   - VOICE RECOGNITION

★ THE MORE FACTOR TYPES USED, THE STRONGER THE PROTECTION.

KEY BENEFITS

- STRONGLY REDUCES RISK OF BREACH
- PROTECTS USERS, DATA & REPUTATION
- SUPPORTS COMPLIANCE (ISO 27001, NIST, SOC 2)
- BUILDS CUSTOMER TRUST & CONFIDENCE
- MINIMAL COST. MAXIMUM IMPACT.

COMMON USE CASES

- CLOUD APPS & SERVICES (OFFICE 365, GOOGLE WORKSPACE)
- VPN & REMOTE ACCESS
- BANKING & FINANCIAL APPS
- E-COMMERCE ACCOUNTS
- ADMIN & PRIVILEGED ACCOUNTS

MFA METHODS: PROS & CONS

METHOD	PROS	CONS
AUTHENTICATOR APP	STRONG SECURITY OFFLINE CAPABLE	DEVICE LOSS CAN BE RISKY
SMS / EMAIL CODE	EASY TO USE WIDELY SUPPORTED	SUSCEPTIBLE TO SIM SWAP
HARDWARE TOKEN / KEY	VERY STRONG PHISHING RESISTANT	COST CAN BE LOST
BIOMETRICS	FAST & CONVENIENT HARD TO FAKE	PRIVACY CONCERNS

COMBINE METHODS FOR BEST PROTECTION. CONTEXT MATTERS!

EXAMPLE: USER LOGIN FLOW

1. USER GOES TO LOGIN PAGE
2. ENTERS USERNAME & PASSWORD
3. PROMPTED FOR MFA (APP CODE) — 987 654
4. CODE VERIFIED
5. ACCESS GRANTED!

BEST PRACTICES

- ☑ ENFORCE MFA FOR ALL USERS
- ☑ USE PHISHING-RESISTANT METHODS WHERE POSSIBLE (FIDO2 / KEYS)
- ☑ PROVIDE BACKUP OPTIONS (RECOVERY CODES, BACKUP DEVICES)
- ☑ EDUCATE USERS ON SECURITY BEST PRACTICES
- ☑ MONITOR & REVIEW ACCESS REGULARLY

> "MFA IS NOT OPTIONAL ANYMORE — IT'S A BASLINE DEFENSE FOR A ZERO TRUST WORLD.

TAKEAWAY: MFA ADDS ONE SMALL STEP FOR USERS, BUT MAKES A HUGE LEAP FOR SECURITY.

WHAT IS SIEM?

SIEM SOLUTIONS COMBINE SECURITY INFORMATION MANAGEMENT (SIM) AND SECURITY EVENT MANAGEMENT (SEM) TO DETECT, INVESTIGATE AND RESPOND TO THREATS IN REAL TIME.

CORE CAPABILITIES

COLLECT
GATHER LOGS & EVENTS FROM ACROSS YOUR ENVIRONMENT

NORMALIZE
STANDARDIZE AND ENRICH DATA FOR CONSISTENCY

ANALYZE
CORRELATE EVENTS TO IDENTIFY THREATS

DETECT & ALERT
REAL-TIME ALERTING ON SUSPICIOUS ACTIVITY

INVESTIGATE & RESPOND
DEEP DIVE, HUNT THREATS AND TAKE ACTION FAST

KEY BENEFITS

- IMPROVED THREAT DETECTION
- FASTER INCIDENT RESPONSE
- STRONGER SECURITY POSTURE
- REDUCED RISK & FINANCIAL IMPACT
- COMPLIANCE & REGULATORY SUPPORT

SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)

TURNING DATA INTO INSIGHT.
INSIGHT INTO ACTION.

DATA SOURCES

- NETWORK DEVICES
- FIREWALLS
- SERVERS
- ENDPOINTS
- APPLICATIONS
- CLOUD SERVICES
- IDENTITY PROVIDERS
- THREAT INTEL FEEDS

USE CASES

- ADVANCED THREAT DETECTION
- SECURITY INCIDENT INVESTIGATION
- COMPLIANCE MONITORING
- INSIDER THREAT DETECTION
- CLOUD SECURITY MONITORING

HOW SIEM WORKS

1. **COLLECT**
   AGGREGATE LOGS & EVENTS FROM MULTIPLE SOURCES
2. **PROCESS**
   NORMALIZE, PARSE & ENRICH THE DATA
3. **CORRELATE**
   APPLY RULES, USE CASES & BEHAVIOR ANALYTICS
4. **DETECT**
   IDENTIFY THREATS & ANOMALIES
5. **RESPOND**
   INVESTIGATE, CONTAIN & REMEDIATE

SIEM ARCHITECTURE

DATA SOURCES → COLLECTORS → PROCESSING ENGINE → SIEM PLATFORM → ANALYSTS & ACTION

INSIDE THE SIEM PLATFORM

- **LOG MANAGEMENT**
  STORE, INDEX & RETRIEVE LOG DATA AT SCALE
- **DASHBOARDS & REPORTS**
  REAL-TIME VISIBILITY & ACTIONABLE INSIGHTS
- **CORRELATION ENGINE**
  RULES, USE CASES & BEHAVIOR ANALYTICS
- **ALERTING & NOTIFICATIONS**
  FLEXIBLE ALERTS VIA EMAIL, SMS, SOAR, ETC.
- **THREAT INTELLIGENCE**
  INTEGRATE FEEDS & CONTEXT FOR BETTER DETECTION
- **INTEGRATIONS**
  SOAR, TICKETING, ITSM, THREAT INTEL, CMDB

BY THE NUMBERS

83% OF ORGANIZATIONS SAY SIEM IMPROVES THEIR SECURITY POSTURE
– ESG RESEARCH

$4.5M AVERAGE COST OF A DATA BREACH IN 2023
– IBM

28% INCREASE IN SIEM ADOPTION YOY
– GARTNER

SIEM vs SIEM (TRADITIONAL)

TRADITIONAL SIEM	MODERN SIEM
FOCUSED ON SECURITY LOGS	INTEGRATES SECURITY + CONTEXT
LIMITED CONTEXT	BUSINESS & THREAT CONTEXT
RULE-BASED CORRELATION	ADVANCED ANALYTICS & UEBA
REACTIVE APPROACH	PROACTIVE THREAT HUNTING
HIGH NOISE, MORE FALSE POSITIVES	SMARTER ALERTS, LESS NOISE

SEE EVERYTHING.
UNDERSTAND EVERYTHING.
SECURE EVERYTHING.

ACTIONABLE TAKEAWAYS

- DEFINE CLEAR SECURITY USE CASES
- ENSURE BROAD LOG COVERAGE
- TUNE RULES & REDUCE NOISE
- LEVERAGE THREAT INTEL & UEBA
- AUTOMATE RESPONSE WITH SOAR
- CONTINUOUSLY IMPROVE & MEASURE

A STRONG SIEM PROGRAM TURNS OVERWHELMING DATA INTO YOUR **GREATEST DEFENSE.**

RIGHT DATA. RIGHT CONTEXT. RIGHT TIME. THAT'S THE **POWER OF SIEM.**

IDENTITY & ACCESS MANAGEMENT (IAM)

WHAT IS IAM?

IDENTITY & ACCESS MANAGEMENT (IAM) ENSURES THE RIGHT PEOPLE HAVE THE RIGHT ACCESS TO THE RIGHT RESOURCES AT THE RIGHT TIME — AND FOR THE RIGHT REASONS.

CORE OBJECTIVES

- SECURE ACCESS
- PROTECT DATA
- ENSURE COMPLIANCE
- IMPROVE PRODUCTIVITY

WHY IT MATTERS

83%

OF BREACHES INVOLVE EXCESSIVE ACCESS OR WEAK CREDENTIALS.

— VERIZON DBIR 2024

STRONG IAM = STRONG SECURITY + BUSINESS ENABLEMENT

KEY COMPONENTS

IDENTITIES
USERS, DEVICES, APPLICATIONS, SERVICES

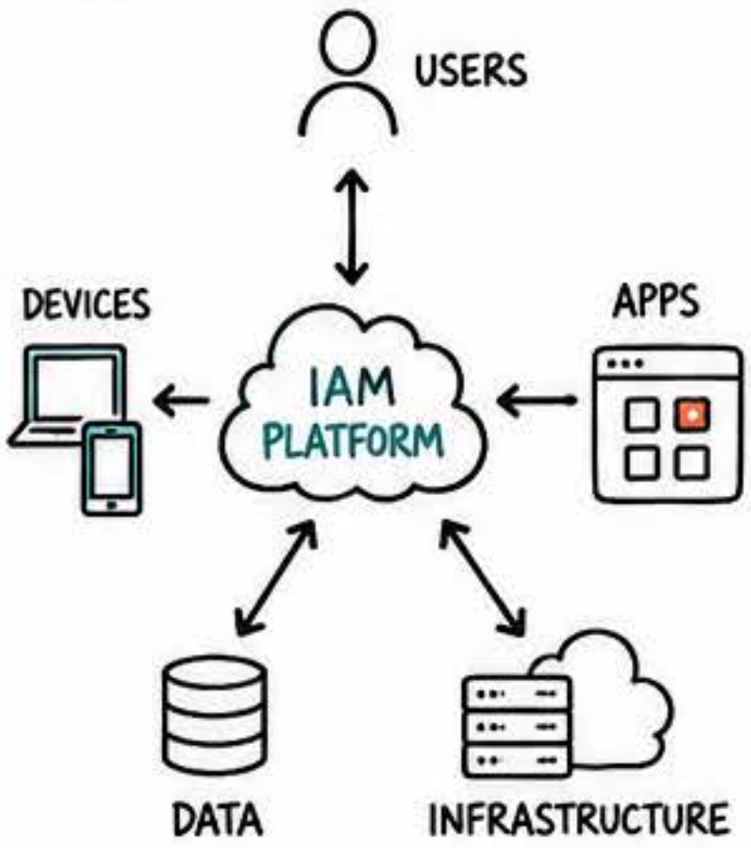
AUTHENTICATION
VERIFY WHO YOU ARE

AUTHORIZATION
DETERMINE WHAT YOU CAN ACCESS

ACCESS MANAGEMENT
PROVISION, MODIFY, REVIEW, REVOKE

AUDIT & MONITORING
TRACK ACTIVITY, DETECT RISKS

THE IAM ECOSYSTEM



AUTHENTICATION METHODS

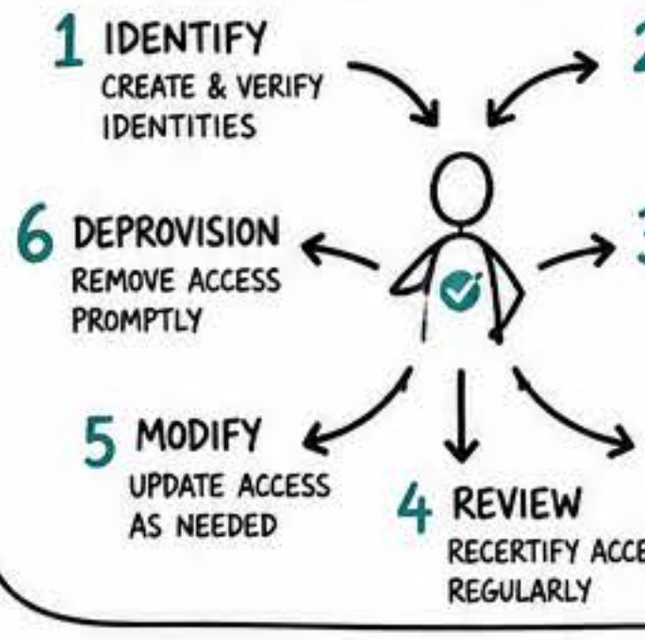
ACCESS MODELS

RBAC
ROLE-BASED ACCESS CONTROL

ABAC
ATTRIBUTE-BASED ACCESS CONTROL

PBAC
POLICY-BASED ACCESS CONTROL

THE IAM LIFECYCLE



BEST PRACTICES

- ENFORCE MFA EVERYWHERE
- APPLY LEAST PRIVILEGE ACCESS
- AUTOMATE PROVISIONING & DEPROVISIONING
- REGULAR ACCESS REVIEWS
- MONITOR & ALERT IN REAL TIME
- KEEP POLICIES SIMPLE & CLEAR
- EDUCATE USERS CONTINUOUSLY

REMEMBER

THE RIGHT ACCESS FOR THE RIGHT USER AT THE RIGHT TIME KEEPS YOUR BUSINESS SECURE AND AGILE.

COMMON CHALLENGES

- ORPHANED ACCOUNTS
- EXCESSIVE PRIVILEGES
- SHADOW IT & UNSANCTIONED ACCESS
- SILOED SYSTEMS
- COMPLIANCE RISKS

KEY TAKEAWAY

EFFECTIVE IAM ISN'T JUST AN IT INITIATIVE — IT'S A BUSINESS IMPERATIVE THAT DRIVES SECURITY, COMPLIANCE, AND GROWTH.

FIREWALLS AND BOUNDARY PROTECTION

THE PURPOSE

FIREWALLS MONITOR AND CONTROL NETWORK TRAFFIC BASED ON PREDEFINED SECURITY RULES.

HACKERS

MALWARE

THREATS

ALLOW SAFE TRAFFIC

KEY INSIGHT

A FIREWALL DOESN'T MAKE YOU INVINCIBLE, BUT IT MAKES YOU A MUCH HARDER TARGET.

HOW IT WORKS

1. TRAFFIC ENTERS THE NETWORK
2. FIREWALL INSPECTS THE PACKETS
3. COMPARES AGAINST SECURITY RULES
4. ALLOW LEGITIMATE TRAFFIC / BLOCK MALICIOUS OR UNWANTED
5. LOG & MONITOR ALL ACTIVITY

CORE CONCEPTS

TRAFFIC FILTERING
ALLOW OR BLOCK BASED ON RULES

INSPECTION
DEEP PACKET INSPECTION LOOKS INSIDE TRAFFIC

POLICY ENFORCEMENT
APPLY ORGANIZATIONAL SECURITY POLICIES

SEGMENTATION
ISOLATE NETWORKS TO REDUCE RISK

TYPES OF FIREWALLS

NETWORK FIREWALL
PROTECTS THE PERIMETER BETWEEN INTERNAL & EXTERNAL NETWORKS

HOST-BASED FIREWALL
PROTECTS INDIVIDUAL DEVICES AND SERVERS

NEXT-GENERATION FIREWALL (NGFW)
ADVANCED THREAT PROTECTION, APPLICATION AWARENESS, AND DEEP INSPECTION

CLOUD FIREWALL
PROTECTS CLOUD ENVIRONMENTS AND WORKLOADS

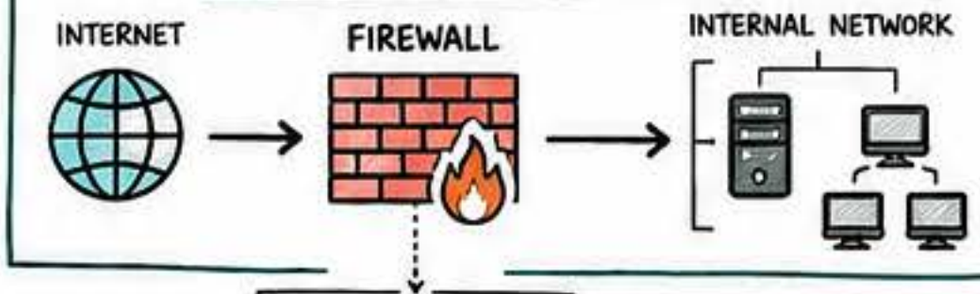
WEB APPLICATION FIREWALL (WAF)
PROTECTS WEB APPS FROM COMMON ATTACKS (SQLi, XSS, CSRF, ETC.)

KEY BENEFITS

- PREVENTS UNAUTHORIZED ACCESS
- BLOCKS MALICIOUS TRAFFIC
- MONITORS & CONTROLS NETWORK ACTIVITY
- REDUCES ATTACK SURFACE AND RISK
- SUPPORTS COMPLIANCE & REGULATIONS

YOUR FIRST LINE OF DEFENSE AGAINST UNWANTED ACCESS

WHERE FIREWALLS SIT



ISOLATE PUBLIC-FACING SERVICES (WEB, MAIL, DNS, ETC.)

BY THE NUMBERS

OF BREACHES INVOLVE EXTERNAL ATTACKS THAT COULD BE BLOCKED AT THE BOUNDARY.

– VERIZON DBIR 2024

NEXT-GEN FIREWALL MARKET TO REACH $12.8B BY 2029 CAGR 13.6%

– MARKETSANDMARKETS

FIREWALL RULES: HOW THEY WORK

SOURCE	DESTINATION	SERVICE	ACTION	EXAMPLE
ANY	WEB SERVER	HTTPS (443)	ALLOW	USERS ACCESS WEBSITE
ANY	ANY	RDP (3389)	BLOCK	BLOCK REMOTE DESKTOP
INTERNAL	DATABASE	SQL (1433)	ALLOW	APP CONNECTS TO DATABASE
ANY	ANY	ANY	DENY (DEFAULT)	BLOCK EVERYTHING ELSE

BOUNDARY PROTECTION PROCESS

1. IDENTIFY ASSETS & RISKS
2. DEFINE SECURITY POLICIES
3. CONFIGURE FIREWALL RULES
4. MONITOR & ANALYZE TRAFFIC
5. DETECT & RESPOND TO THREATS
6. REVIEW & OPTIMIZE REGULARLY

ACTIONABLE TAKEAWAYS

- KEEP FIREWALL RULES SIMPLE, SPECIFIC & REVIEWED.
- FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE.
- LOG EVERYTHING. MONITOR RELENTLESSLY.
- UPDATE RULES AS YOUR ENVIRONMENT EVOLVES.
- LAYER FIREWALLS WITH OTHER SECURITY CONTROLS.

GOLDEN PRINCIPLE

ALLOW WHAT YOU NEED.
BLOCK WHAT YOU DON'T.
MONITOR EVERYTHING.

A STRONG BOUNDARY TODAY **PREVENTS** A BREACH TOMORROW.

NETWORK MONITORING

WHAT IS IT?

NETWORK MONITORING IS THE CONTINUOUS OBSERVATION OF NETWORK DEVICES, TRAFFIC, APPLICATIONS & PERFORMANCE TO ENSURE AVAILABILITY, RELIABILITY & SECURITY.

SEE IT. UNDERSTAND IT.
FIX IT. BEFORE USERS FEEL IT.

WHY IT MATTERS

- PREVENT DOWNTIME & OUTAGES
- IMPROVE USER EXPERIENCE
- ENHANCE SECURITY & THREAT DETECTION
- REDUCE COSTS & SPEED UP RESOLUTION
- SUPPORT CAPACITY PLANNING & GROWTH

KEY METRICS TO WATCH

- 99.9% AVAILABILITY / UPTIME
- LATENCY
- PACKET LOSS
- BANDWIDTH / THROUGHPUT
- JITTER
- ERROR RATE 2.3%
- CONNECTION COUNT 1,256
- CPU / MEMORY UTILIZATION 72%

HOW IT WORKS

1. **DISCOVER** — FIND DEVICES & INTERFACES
2. **COLLECT** — GATHER DATA (SNMP, FLOW, LOGS, STREAMS)
3. **ANALYZE** — CORRELATE & BASELINE BEHAVIOR
4. **ALERT** — DETECT ISSUES & NOTIFY
5. **ACT** — INVESTIGATE & RESOLVE

VISIBILITY → INSIGHT → ACTION → RELIABILITY

TYPES OF MONITORING

- **INFRASTRUCTURE** — Routers, Switches, Firewalls, Servers
- **CLOUD** — Availability, Performance, Cost, Services
- **APPLICATION** — APM, Transactions, APIs, Databases
- **TRAFFIC ANALYSIS** — Flow, Bandwidth, Top Talkers
- **SECURITY MONITORING** — Threats, Anomalies, Policy Violations
- **WIRELESS** — AP Health, Clients, Coverage, Roaming

ALERTING & RESPONSE FLOW

ISSUE DETECTED → ALERT TRIGGERED → NOTIFIED (EMAIL, SMS, PAGER, APP) → INVESTIGATE ROOT CAUSE → RESOLVE & VERIFY

LEARN & IMPROVE

COMMON USE CASES

- ✓ DETECT OUTAGES FAST
- ✓ TROUBLESHOOT PERFORMANCE ISSUES
- ✓ MONITOR SLA & USER EXPERIENCE
- ✓ CAPACITY PLANNING
- ✓ CHANGE VALIDATION
- ✓ SECURITY THREAT DETECTION
- ✓ COMPLIANCE & REPORTING

TOOLS & TECHNOLOGIES

SNMP · NETFLOW /IPFIX · SYSLOG · API · TELEMETRY & STREAMING

POPULAR TOOLS

PRTG · NAGIOS · ZABBIX · SOLARWINDS
DATADOG · NEW RELIC · PROMETHEUS · CACTI
WIRESHARK · ELK STACK · CLOUDWATCH

BY THE NUMBERS

- **60%+** OF OUTAGES ARE CAUSED BY PROBLEMS IN THE INTERNAL NETWORK.
- **45%** OF ORGS LACK VISIBILITY ACROSS THEIR NETWORK ENVIRONMENTS.
- **$1.4M** THE AVERAGE COST OF DOWNTIME PER HOUR (GARTNER)

MONITORING FRAMEWORK

DEFINE (OBJECTIVES & SCOPE) → IDENTIFY (ASSETS & DEPENDENCIES) → MONITOR (COLLECT & VISUALIZE) → ANALYZE (FIND PATTERNS & ANOMALIES) → OPTIMIZE (IMPROVE & AUTOMATE)

CONTINUOUS IMPROVEMENT

ACTIONABLE TAKEAWAYS

- ☑ START WITH YOUR MOST CRITICAL SERVICES.
- ☑ SET BASELINES & MEANINGFUL THRESHOLDS.
- ☑ ALERT SMARTLY, NOT NOISILY.
- ☑ CORRELATE DATA FROM MULTIPLE SOURCES.
- ☑ AUTOMATE WHERE POSSIBLE.
- ☑ REVIEW & TUNE REGULARLY.
- ☑ VISIBILITY TODAY. RELIABILITY TOMORROW.

"YOU CAN'T IMPROVE WHAT YOU DON'T MONITOR."

KEEP YOUR NETWORK HEALTHY!

PASSWORD & CREDENTIAL MANAGEMENT

Secure Access. Protect Everything.

1. Why It Matters

- 81% of breaches are caused by weak, stolen or reused credentials.
- Average cost of a data breach: $4.88M
- Human error is a top security risk.

GOAL:
The right people have the right access to the right things at the right time.

2. Core Concepts

- **Confidentiality** — Keep credentials secret
- **Integrity** — Prevent tampering
- **Availability** — Access when needed
- **Accountability** — Track and audit access

3. Best Practices

- Use strong, unique passwords
- Enable multi-factor authentication (MFA)
- Never reuse passwords
- Keep software & systems updated
- Remove access when not needed (least privilege)
- Monitor & review access regularly

4. Common Threats

- Phishing attacks steal credentials
- Malware & keyloggers capture passwords
- Weak or reused passwords
- Unsecured credential stores / leaks

5. Types of Credentials

- User passwords
- API keys
- SSH keys
- Tokens / certificates
- Service account credentials
- Recovery codes

6. Credential Management Framework

1. **Store** — Securely store credentials in an encrypted vault
2. **Control** — Enforce access policies & least privilege
3. **Rotate** — Regularly rotate passwords, keys & tokens
4. **Monitor** — Log, monitor & alert on suspicious activity
5. **Retire** — Revoke & remove unused or expired access

7. Tools & Solutions

- 1Password
- Bitwarden
- LastPass
- KeePass
- HashiCorp Vault
- AWS Secrets Manager

8. Creating Strong Passwords

12+ characters
Use a mix of:
- ✓ Uppercase letters
- ✓ lowercase letters
- ✓ Numbers
- ✓ Symbols

`T!g3r$ky#2025`

Not in dictionary · Unpredictable · Longer is better

9. MFA: How It Works

1. Enter username & password
2. Verify with second factor (app, SMS, token)
3. Access granted!

Something you have:
- Phone
- Token
- Security key

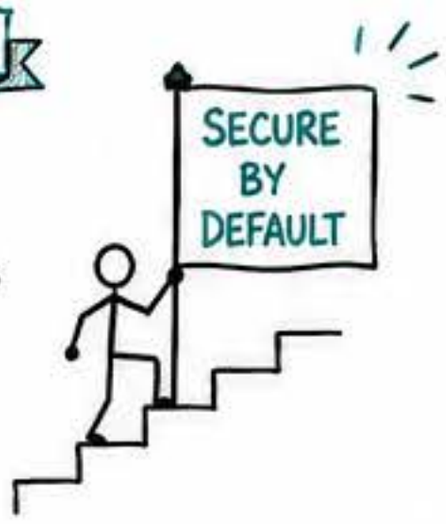
Something you are:
- Fingerprint
- Face ID

10. Key Stats

- **80%** of hacking is due to weak or stolen passwords
- **60%** of people reuse the same passwords across sites
- **2 min** avg time to crack a weak password

11. Actionable Takeaways

- ☑ Use a password manager
- ☑ Enable MFA everywhere
- ☑ Create unique, strong passwords
- ☑ Review & remove unused access
- ☑ Train your team & stay aware
- ☑ Make security a daily habit



REMEMBER:

Credentials are the keys to your digital world.

Protect them. Manage them. Own your security.

BUSINESS CONTINUITY, DATA BACKUP & SYSTEM RECOVERY

THE GOAL

ENSURE CRITICAL BUSINESS FUNCTIONS CAN CONTINUE OR BE RESTORED QUICKLY AFTER A DISRUPTION.

WHY IT MATTERS

- MINIMIZE DOWNTIME AND DISRUPTION
- PROTECT REVENUE AND REPUTATION
- MEET COMPLIANCE AND LEGAL REQUIREMENTS
- MAINTAIN CUSTOMER TRUST & CONFIDENCE

CORE PILLARS

BUSINESS CONTINUITY
KEEP THE BUSINESS RUNNING THROUGH ANY DISRUPTION.

DATA BACKUP
PROTECT AND PRESERVE CRITICAL DATA.

SYSTEM RECOVERY
RESTORE SYSTEMS AND DATA TO NORMAL OPERATIONS.

RISK = IMPACT x LIKELIHOOD

HIGH IMPACT
- FINANCIAL LOSS
- OPERATIONAL HALT
- DATA LOSS
- REPUTATION DAMAGE

MORE LIKELY THAN YOU THINK

COMMON THREATS

- CYBER ATTACKS (RANSOMWARE, MALWARE)
- HARDWARE FAILURE
- NATURAL DISASTERS (FIRE, FLOOD, STORM)
- HUMAN ERROR
- POWER OUTAGES

THE CONTINUITY TRIAD

PEOPLE
TRAINED, INFORMED, EMPOWERED

PROCESS
DOCUMENTED, TESTED, IMPROVED

TECHNOLOGY
RELIABLE, SECURE, REDUNDANT

PREPARE TODAY, PROTECT TOMORROW

RPO vs RTO

RPO		RTO
(RECOVERY POINT OBJECTIVE)	VS	(RECOVERY TIME OBJECTIVE)
HOW MUCH DATA CAN YOU AFFORD TO LOSE?		HOW FAST DO YOU NEED TO BE BACK ONLINE?
2h 1h 0		

THE SHORTER, THE BETTER.

DATA BACKUP BEST PRACTICES

- FOLLOW THE 3-2-1 RULE
  - 3 COPIES OF DATA
  - 2 DIFFERENT MEDIA
  - 1 OFFSITE / OFFLINE COPY
- AUTOMATE AND SCHEDULE CONSISTENT BACKUPS REDUCE RISK
- ENCRYPT YOUR BACKUPS PROTECT DATA AT REST AND IN TRANSIT
- VERIFY AND TEST RESTORES BACKUPS ARE ONLY USEFUL IF THEY WORK!

BUSINESS CONTINUITY LIFECYCLE

1. IDENTIFY CRITICAL FUNCTIONS & ASSETS
2. ASSESS RISKS & IMPACT
3. DEVELOP STRATEGIES & PLANS
4. IMPLEMENT SOLUTIONS
5. TEST & TRAIN REGULARLY
6. MONITOR, REVIEW & IMPROVE

SYSTEM RECOVERY PROCESS

- DETECT & CONFIRM ISSUE
- ACTIVATE RECOVERY PLAN
- ISOLATE THE PROBLEM
- RESTORE SYSTEMS & DATA
- VERIFY & VALIDATE
- RETURN TO NORMAL OPERATIONS & LESSONS LEARNED

BACKUP STRATEGIES

FULL BACKUP
COMPLETE COPY PERIODICALLY

INCREMENTAL BACKUP
ONLY CHANGES SINCE LAST BACKUP

DIFFERENTIAL BACKUP
CHANGES SINCE LAST FULL BACKUP

CONTINUOUS DATA PROTECTION (CDP)
REAL-TIME REPLICATION

TRENDS & STATS

- **60%** OF SMALL BUSINESSES THAT LOSE THEIR DATA CLOSE WITHIN 6 MONTHS.
- **93%** OF BUSINESSES WITHOUT A DISASTER RECOVERY PLAN LOST 10+ DAYS OF DATA IN A MAJOR INCIDENT.
- RANSOMWARE ATTACKS INCREASED BY **72%** (YOY)
- THE GLOBAL BUSINESS CONTINUITY MANAGEMENT MARKET IS PROJECTED TO REACH **$57B** BY 2027.

KEY TAKEAWAYS

- PLAN AHEAD. DON'T WAIT FOR A DISASTER.
- INTEGRATE PEOPLE, PROCESS & TECH TOGETHER.
- TEST OFTEN. IMPROVE ALWAYS.
- RESILIENCE ISN'T AN OPTION—IT'S A COMPETITIVE EDGE.

"DISRUPTIONS ARE INEVITABLE. DOWNTIME IS OPTIONAL."

CYBERSECURITY TABLE TOP EXERCISES

PRACTICE TODAY, RESPOND STRONGER TOMORROW

WHAT IS IT?

A FACILITATED DISCUSSION OF A CYBER INCIDENT SCENARIO TO TEST PEOPLE, PROCESSES, AND TECHNOLOGY IN A SAFE ENVIRONMENT.

WHY IT MATTERS

- IMPROVE INCIDENT READINESS
- IDENTIFY GAPS & WEAKNESSES
- STRENGTHEN TEAM COLLABORATION
- BETTER DECISIONS UNDER PRESSURE
- REDUCE BUSINESS IMPACT & DOWNTIME

WHO SHOULD PARTICIPATE?

- EXECUTIVE LEADERSHIP
- IT & SECURITY TEAMS
- LEGAL & COMPLIANCE
- HR
- COMMUNICATIONS / PR
- OPERATIONS / BUSINESS UNIT LEADERS
- THIRD PARTY / VENDORS

TYPES OF EXERCISES

- DISCUSSION-BASED TABLETOP (ROUNDTABLE)
- SCENARIO-BASED TABLETOP
- TECHNICAL TABLETOP
- EXECUTIVE TABLETOP
- CROSS-FUNCTIONAL TABLETOP

THE PROCESS

1. **DEFINE OBJECTIVES** — What do we want to learn or validate?
2. **DEVELOP SCENARIO** — Realistic, relevant, threat-informed.
3. **PLAN & INVITE** — Identify participants, roles & logistics.
4. **CONDUCT EXERCISE** — Facilitated discussion walkthrough.
5. **DEBRIEF & ANALYZE** — Capture observations, strengths, gaps.
6. **IMPROVE & FOLLOW UP** — Create action plan, track & retest.

TYPICAL SCENARIO FLOW

- **TRIGGER** — What happened?
- **DISCOVER & ANALYZE** — What do we know?
- **RESPOND & DECIDE** — What are our options?
- **COMMUNICATE** — Who do we inform and how?
- **RECOVER & LEARN** — What's our next step?

EXAMPLE SCENARIO IDEAS

- RANSOMWARE ATTACK
- DATA BREACH / EXFILTRATION
- SUPPLY CHAIN COMPROMISE
- CLOUD ACCOUNT TAKEOVER
- INSIDER THREAT
- DDoS ATTACK
- ZERO-DAY EXPLOIT

KEY AREAS TESTED

- ✓ INCIDENT DETECTION & ESCALATION
- ✓ ROLES & RESPONSIBILITIES
- ✓ DECISION MAKING
- ✓ COMMUNICATIONS (INTERNAL & EXTERNAL)
- ✓ BUSINESS CONTINUITY
- ✓ LEGAL & REGULATORY CONSIDERATIONS
- ✓ THIRD PARTY COORDINATION
- ✓ TOOLS & TECHNOLOGY EFFECTIVENESS

BY THE NUMBERS

70% OF ORGANIZATIONS THAT CONDUCT TABLETOP EXERCISES IMPROVE THEIR INCIDENT RESPONSE MATURITY.
— PONEMON INSTITUTE

60% OF COMPANIES EXPERIENCE A CYBER INCIDENT THEY ARE UNPREPARED FOR.
— IBM

3x ORGANIZATIONS THAT TEST THEIR RESPONSE PLAN ARE 3X MORE LIKELY TO REDUCE THE IMPACT OF A BREACH.
— IBM

KEY INSIGHTS

"IT'S NOT ABOUT THE TECH—IT'S ABOUT PEOPLE, PROCESS & DECISIONS."

"YOU DON'T RISE TO THE OCCASION. YOU FALL TO YOUR LEVEL OF PREPARATION."

"TABLETOPS UNCOVER GAPS YOU DIDN'T KNOW YOU HAD."

ACTIONABLE TAKEAWAYS

- ☑ RUN TABLETOPS REGULARLY (AT LEAST 2x / YEAR)
- ☑ KEEP SCENARIOS CURRENT & RELEVANT
- ☑ INVOLVE THE RIGHT PEOPLE
- ☑ FOCUS ON LEARNING, NOT JUDGMENT
- ☑ TURN INSIGHTS INTO ACTION
- ☑ TRACK & MEASURE MATURITY OVER TIME

TABLETOP EXERCISES DON'T PREVENT ATTACKS. THEY PREPARE YOU TO WITHSTAND THEM.

→ PREPARED TEAMS
RESILIENT BUSINESSES
STRONGER FUTURE

.GOV DOMAIN AND EMAIL HOSTING

TRUST. SECURITY. SERVICE.

ONE SMALL DOMAIN. BIG IMPACT.

"A .GOV EMAIL TELLS CITIZENS YOU'RE OFFICIAL, ACCOUNTABLE, AND HERE TO SERVE."

1 WHAT IS A .GOV DOMAIN?

.GOV IS A TOP-LEVEL DOMAIN RESTRICTED EXCLUSIVELY FOR U.S. GOVERNMENT ENTITIES AT THE FEDERAL, STATE, LOCAL, AND TRIBAL LEVELS.

PURPOSE:

- ☑ ESTABLISH OFFICIAL IDENTITY
- ☑ BUILD PUBLIC TRUST
- ☑ ENSURE SECURE COMMUNICATION
- ☑ IMPROVE ACCESSIBILITY

2 WHO CAN GET A .GOV DOMAIN?

- FEDERAL AGENCIES
- STATE GOVERNMENTS
- COUNTY & CITY OFFICES
- PUBLIC SCHOOLS & UNIVERSITIES
- TRIBAL GOVERNMENTS

MUST BE:

- ✓ AN AUTHORIZED GOVERNMENT ENTITY
- ✓ OPERATING IN THE U.S.
- ✓ ABLE TO PROVE ELIGIBILITY

3 HOW TO GET A .GOV DOMAIN

1. CHECK ELIGIBILITY
2. REGISTER WITH GSA AT SAM.GOV
3. SUBMIT .GOV APPLICATION VIA GSA ASSIGNED DOMAIN REGISTRAR
4. PROVIDE REQUIRED DOCUMENTATION
5. APPROVAL & DOMAIN ACTIVATION

4 .GOV EMAIL HOSTING BUILT FOR PUBLIC SERVICE

- PROFESSIONAL EMAIL @youragency.gov
- ENTERPRISE-GRADE SECURITY & ENCRYPTION
- HIGH AVAILABILITY & RELIABILITY
- EASY COLLABORATION & CALENDARS
- MOBILE & REMOTE ACCESS
- SCALABLE AS YOU GROW

WHY IT MATTERS

- BUILDS TRUST WITH CITIZENS
- IMPROVES INTERNAL COMMUNICATION
- SUPPORTS YOUR MISSION

5 SECURITY IS NON-NEGOTIABLE

- ✓ SPAM & PHISHING PROTECTION
- ✓ MULTI-FACTOR AUTHENTICATION
- ✓ DATA ENCRYPTION (IN TRANSIT & AT REST)
- ✓ ROLE-BASED ACCESS CONTROL
- ✓ AUDIT LOGS & COMPLIANCE
- ✓ REGULAR BACKUPS

COMPLIANCE STANDARDS

CJIS · HIPAA · FERPA · FISMA · NIST

SOC 2 · ISO 27001 · ADA

6 .GOV EMAIL VS. PUBLIC EMAIL

.GOV EMAIL		PUBLIC EMAIL
OFFICIAL & TRUSTED		LESS CREDIBILITY
STRONG SECURITY		LIMITED PROTECTIONS
DATA STAYS IN COMPLIANT ENVIRONMENTS		DATA MAY BE USED FOR ADVERTISING
DESIGNED FOR GOVERNMENT NEEDS		NOT BUILT FOR PUBLIC SECTOR
LONG-TERM CONTROL & OWNERSHIP		DEPENDENT ON THIRD PARTIES

7 BEST PRACTICES

- USE YOUR .GOV EMAIL FOR ALL OFFICIAL BUSINESS
- KEEP SOFTWARE & SYSTEMS UPDATED
- TRAIN STAFF ON EMAIL SECURITY
- MONITOR & REVIEW USER ACCESS
- BACK UP REGULARLY & TEST DISASTERS RECOVERY

EXAMPLES

- CITY OF AUSTIN mail@austintexas.gov
- COOK COUNTY info@cookcounty.gov
- STATE OF COLORADO contact@state.co.us
- U.S. DEPARTMENT OF HEALTH info@hhs.gov

A .GOV DOMAIN + SECURE EMAIL SHOWS YOU'RE HERE TO SERVE — AND HERE TO STAY.

KEY TAKEAWAYS

- ☆ .GOV BUILDS TRUST & CREDIBILITY
- ☆ ELIGIBILITY ENSURES INTEGRITY
- ☆ SECURE EMAIL PROTECTS DATA
- ☆ THE RIGHT SETUP EMPOWERS YOUR MISSION

SERVING COMMUNITIES STARTS WITH TRUSTED COMMUNICATION.

OPEN-SOURCE INTELLIGENCE (OSINT) & ATTACK SURFACE ANALYSIS

FIND IT. UNDERSTAND IT.
REDUCE RISK. STAY AHEAD.

TRUTH IS OUT THERE.
YOUR ADVANTAGE IS
FINDING IT FIRST.

WHAT IS OSINT & ATTACK SURFACE ANALYSIS?

OSINT IS THE COLLECTION, ANALYSIS, AND DISSEMINATION OF PUBLICLY AVAILABLE INFORMATION.

ATTACK SURFACE ANALYSIS

IDENTIFIES ALL EXTERNAL ASSETS, ENTRY POINTS, AND EXPOSURES THAT COULD BE TARGETED BY AN ATTACKER.

CORE PRINCIPLES

- ☑ PUBLIC ≠ TRIVIAL
- ☑ ETHICAL & LEGAL
- ☑ ACCURACY & VERIFICATION
- ☑ OBJECTIVITY & TRANSPARENCY
- ☑ PROTECT PRIVACY
- ☑ ADD VALUE THROUGH ANALYSIS

SOURCES (EVERYWHERE!)

- **WEB & NEWS MEDIA** — WEBSITES, BLOGS, NEWS OUTLETS
- **SOCIAL MEDIA** — POSTS, PROFILES, COMMENTS
- **GOVERNMENT & PUBLIC DATA** — RECORDS, REPORTS, PORTALS
- **IMAGERY & GEOSPATIAL** — SATELLITE, DRONE, MAPS
- **DOCUMENTS & FILES** — PDFS, PRESENTATIONS, LEAKS
- **PEOPLE & COMMUNITIES** — FORUMS, REVIEWS, NETWORKS
- **TECH & INFRASTRUCTURE** — DNS, IP INFO, CERTIFICATES, CODE

THE OSINT PROCESS

1. **DEFINE OBJECTIVE** — WHAT DO WE NEED TO FIND OUT?
2. **COLLECT** — FIND AS MUCH RELEVANT DATA AS POSSIBLE
3. **PROCESS** — ORGANIZE, CLEAN, AND STRUCTURE THE DATA
4. **ANALYZE** — FIND PATTERNS, CONNECTIONS & MEANING
5. **VERIFY** — CROSS-CHECK, CORROBORATE, AND VALIDATE
6. **REPORT & DISSEMINATE** — DELIVER CLEAR, ACTIONABLE INTELLIGENCE

OSINT FRAMEWORK

- COLLECTION (GATHER WIDELY)
- PROCESSING (ORGANIZE & FILTER)
- ANALYSIS (DERIVE INSIGHT)
- INTELLIGENCE (ACTIONABLE OUTPUT)

FROM NOISE → TO INSIGHT

KEY INSIGHTS

- MOST INFORMATION IS PUBLIC.
- CONTEXT TURNS DATA INTO INTELLIGENCE.
- CORRELATE, DON'T ASSUME.
- BIAS IS THE ENEMY. SKEPTICISM IS A SUPERPOWER.
- TIMELINESS MATTERS.
- ETHICS & LEGALITY KEEP US CREDIBLE.

EXAMPLES OF OSINT + ATTACK SURFACE ANALYSIS

- **SECURITY & DEFENSE** — THREAT MONITORING, SITUATIONAL AWARENESS, ADVERSARY PROFILING
- **BUSINESS INTELLIGENCE** — MARKET RESEARCH, COMPETITOR ANALYSIS, RISK ASSESSMENT
- **ATTACK SURFACE REDUCTION** — DISCOVER EXPOSED ASSETS, SUBDOMAINS, OPEN PORTS, CLOUD RESOURCES, LEAKS
- **HUMANITARIAN & NGO** — CRISIS MAPPING, DISASTER RESPONSE, HUMAN RIGHTS MONITORING
- **LAW ENFORCEMENT** — INVESTIGATIONS, MISSING PERSONS, FRAUD, CRIME ANALYSIS

TOOLS OF THE TRADE (EXAMPLES)

- **SEARCH ENGINES** — GOOGLE, BING, DUCKDUCKGO
- **DOMAIN & DNS** — WHOIS, DNSLOOKUP, AMASS, SECURITYTRAILS
- **MAPS & GEOINT** — GOOGLE EARTH, OPENSTREETMAP
- **IMAGERY** — SENTINEL HUB, PLANET, MAXAR
- **SOCIAL MEDIA** — TWITTER, REDDIT, TELEGRAM
- **DOCUMENTS** — GOOGLE DORKS, ARCHIVE.ORG
- **ANALYSIS** — MALTEGO, EXCEL, GEOPHI, YARA
- **SECURITY** — VIRUSTOTAL, SHODAN, CENSYS, HAVE I BEEN PWNED

★ THE BEST TOOL? YOUR CURIOSITY.

ATTACK SURFACE ANALYSIS

FIND WHAT ATTACKERS CAN SEE.

- DOMAINS & SUBDOMAINS
- IP RANGES & HOSTS
- CLOUD & SAAS EXPOSURES
- EMAIL & USER ENUMERATION
- APPLICATIONS & APIS
- CERTIFICATES & EXPOSED SERVICES

IDENTIFY → PRIORITIZE → MITIGATE
CONTINUOUSLY REDUCE EXPOSURE.

ACTIONABLE TAKEAWAYS

- ☑ START WITH A CLEAR OBJECTIVE.
- ☑ COLLECT BROADLY, FILTER EARLY.
- ☑ CORRELATE EVERY DATA POINT.
- ☑ VERIFY BEFORE YOU TRUST.
- ☑ DOCUMENT EVERYTHING.
- ☑ PROTECT YOUR SOURCES & YOURSELF.
- ☑ TURN INSIGHT INTO ACTION.

OSINT BY THE NUMBERS

- **80%+** OF BUSINESS & INTELLIGENCE DATA IS PUBLIC. – GARTNER
- **5.3B** INTERNET USERS WORLDWIDE (2024)
- **500M+** TWEETS POSTED EVERY DAY
- **90%** OF INVESTIGATIONS START WITH AN ONLINE SEARCH.

★ IN THE INFORMATION AGE, OSINT ISN'T JUST POWERFUL—IT'S ESSENTIAL. ★

3. THE PARTIES

COLLABORATION IS OUR GREATEST STRENGTH.

WHO'S INVOLVED

STATE AGENCIES

LOCAL GOVERNMENTS

TRIBAL GOVERNMENTS

FIRST RESPONDERS

ACADEMIA

PRIVATE SECTOR

COMMUNITY PARTNERS

OUR ROLES

LEAD – SET DIRECTION & PRIORITIES

SUPPORT – PROVIDE RESOURCES & EXPERTISE

COLLABORATE – WORK TOGETHER

ACHIEVE – BUILD A RESILIENT ALABAMA

TOGETHER, WE...

- ✓ SHARE KNOWLEDGE
- ✓ ALIGN EFFORTS
- ✓ LEVERAGE RESOURCES
- ✓ CREATE LASTING IMPACT

WHY IT MATTERS

- ★ STRONG PARTNERSHIPS DRIVE STRONGER PROJECTS.
- ★ STRONGER PROJECTS CREATE SAFER COMMUNITIES.
- ★ SAFER COMMUNITIES BUILD A STRONGER ALABAMA.

ONE STATE. ONE MISSION. STRONGER TOGETHER.

ALABAMA OIT

OFFICE OF INFORMATION TECHNOLOGY

INNOVATE, CONNECT. SECURE. SERVE ALABAMA.

OUR PURPOSE

TO ENABLE A SMARTER, MORE EFFICIENT, AND CONNECTED ALABAMA THROUGH TECHNOLOGY AND INNOVATION.

WHO WE ARE

ALABAMA OIT IS THE STATE'S TECHNOLOGY AGENCY, DELIVERING SECURE, RELIABLE, AND INNOVATIVE TECHNOLOGY SOLUTIONS THAT EMPOWER EXECUTIVE BRANCH STATE GOVERNMENT AGENCIES SERVING CITIZENS.

OUR VALUES

SERVE PEOPLE
WE PUT CITIZENS AND AGENCIES FIRST.

INNOVATE BOLDLY
WE EMBRACE CHANGE AND SEEK BETTER WAYS.

ACT WITH INTEGRITY
WE DO WHAT'S RIGHT.

WORK TOGETHER
ONE TEAM.
ONE ALABAMA.

DELIVER EXCELLENCE
WE TAKE PRIDE IN EVERYTHING WE DO.

OUR SERVICES

CLOUD & INFRASTRUCTURE
SCALABLE, SECURE, AND RELIABLE SOLUTIONS

CYBERSECURITY
PROTECTING DATA, SYSTEMS, AND PEOPLE

APPLICATION SERVICES
BUILDING AND MODERNIZING SYSTEMS THAT DRIVE GOVERNMENT

NETWORK & CONNECTIVITY
KEEPING ALABAMA CONNECTED

DATA & ANALYTICS
TURNING DATA INTO INSIGHTS AND IMPACT

BY THE NUMBERS

1,700+
TEAM MEMBERS

100+
STATE AGENCIES SERVED

1,000+
APPLICATIONS SUPPORTED

24/7/365
SYSTEMS MONITORED AND PROTECTED

OUR IMPACT

EMPOWERING STATE AGENCIES
with secure, reliable technology to better serve Alabamians.

DRIVING EFFICIENCY
through automation, modern systems, and smarter data.

BUILDING A STRONGER ALABAMA
through innovation, collaboration, and trusted technology.

OUR FRAMEWORK

HOW WE DELIVER

LISTEN
UNDERSTAND NEEDS & CHALLENGES

PLAN
DESIGN SOLUTIONS THAT ALIGN TO GOALS

BUILD
DEVELOP & INTEGRATE SECURELY

DELIVER
DEPLOY, SUPPORT, AND OPTIMIZE CONTINUOUSLY

IMPROVE
MEASURE, LEARN, AND DRIVE BETTER OUTCOMES

FOCUS AREAS

- MODERNIZE LEGACY SYSTEMS
- EXPAND CLOUD & DIGITAL SERVICES
- ENHANCE CYBER RESILIENCE
- LEVERAGE DATA FOR DECISIONS
- INVEST IN OUR PEOPLE
- IMPROVE CITIZEN EXPERIENCE

EXAMPLES OF OUR WORK

ONLINE SERVICES
MAKING IT EASIER FOR CITIZENS TO DO BUSINESS WITH THE STATE.

CLOUD FIRST
DELIVERING SCALABLE, COST-EFFECTIVE SOLUTIONS.

CYBERSECURITY
PROTECTING WHAT MATTERS MOST.

DATA-DRIVEN INSIGHTS
TURNING DATA INTO BETTER OUTCOMES.

TAKE ACTION

- PARTNER WITH US
- SHARE YOUR IDEAS
- EMBRACE INNOVATION
- USE TECHNOLOGY TO SERVE

TOGETHER, WE CAN BUILD A BETTER, STRONGER ALABAMA!

"TECHNOLOGY IS OUR TOOL. SERVICE IS OUR MISSION. ALABAMA IS OUR WHY."

LEARN MORE:
oit.alabama.gov

FOLLOW US:

ALABAMA OIT

STRONGER TOGETHER. SAFER ALABAMA.

ALABAMA OIT AND ITS ROLE IN SLCGP

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM

WHO WE ARE

ALABAMA OIT IS THE TECHNOLOGY PARTNER SERVING EXECUTIVE BRANCH STATE GOVERNMENT AGENCIES BY DELIVERING SECURE, RELIABLE, AND INNOVATIVE SOLUTIONS.

- TRUSTED STEWARD OF STATE TECHNOLOGY
- PEOPLE-FOCUSED SERVICE
- INNOVATION WITH PURPOSE
- SECURITY & COMPLIANCE EVERY STEP OF THE WAY

OUR MISSION

EMPOWER ALABAMA'S PUBLIC SAFETY COMMUNITY THROUGH TECHNOLOGY, COLLABORATION, AND EXCEPTIONAL SERVICE.

WHAT IS SLCGP?

THE STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP) IS A FEDERAL PROGRAM MANAGED BY CISA AND FEMA THAT STRENGTHENS THE CYBERSECURITY POSTURE OF STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS.

- BUILDS CAPACITY TO PREVENT, PROTECT AGAINST, AND RESPOND TO CYBER THREATS
- PROVIDES REIMBURSEMENT FOR ELIGIBLE CYBERSECURITY PLANNING AND PROJECTS
- SUPPORTS COLLABORATION AND INFORMATION SHARING
- ENHANCES RESILIENCE OF CRITICAL SERVICES AND INFRASTRUCTURE

THE GOAL: HELP ALABAMA COMMUNITIES STAY SECURE, RESILIENT, AND PREPARED IN AN EVOLVING THREAT LANDSCAPE.

OIT'S ROLE IN SLCGP

- **GRANT SYSTEM ADMINISTRATION**
  MANAGE THE SLCGP SYSTEM, USER ACCOUNTS, AND SECURITY.
- **TECHNOLOGY & PLATFORM MANAGEMENT**
  PROVIDE AND MAINTAIN A SECURE, RELIABLE, AND USER-FRIENDLY GRANT MANAGEMENT SYSTEM.
- **DATA INTEGRITY & REPORTING**
  ENSURE ACCURATE DATA, VALIDATION, AND TIMELY REPORTING TO MEET FEDERAL REQUIREMENTS.
- **TRAINING & SUPPORT**
  OFFER TRAINING, GUIDES, AND ONGOING SUPPORT THROUGHOUT THE GRANT LIFECYCLE.
- **COMPLIANCE & OVERSIGHT**
  UPHOLD FEDERAL AND STATE REQUIREMENTS FOR PRIVACY, SECURITY, AND COMPLIANCE.

HOW IT WORKS

1. ELIGIBLE ENTITIES SUBMIT APPLICATIONS.
2. OIT REVIEWS FOR ELIGIBILITY AND COMPLETENESS.
3. GRANT FUNDS ARE AWARDED AND McCRARY INSTITUTE GUIDES ENTITY PROJECT IMPLEMENTATIONS.
4. PROJECTS ARE MONITORED AND PROGRESS IS TRACKED.
5. OIT OVERSEES REPORTING, REIMBURSEMENT, AND CLOSEOUT.

OUR IMPACT

STRONGER CYBER DEFENSES. PROTECTED DATA.
RESILIENT COMMUNITIES. BETTER OUTCOMES.

TECHNOLOGY + COLLABORATION = STRONGER COMMUNITIES

KEY BENEFITS OF SLCGP

- REDUCES RISK STRENGTHENS CYBERSECURITY POSTURE
- MAXIMIZES RESOURCES USES FEDERAL FUNDS TO STRETCH LOCAL DOLLARS
- BUILDS CAPACITY IMPROVES SKILLS, TOOLS, AND PROCESSES
- SUPPORTS RESILIENCE ENSURES CONTINUITY OF CRITICAL SERVICES

OUR PARTNERS

CISA · FEMA · LOCAL GOVERNMENTS · ALABAMA AGENCIES · PUBLIC SAFETY COMMUNITY

WORKING TOGETHER TO BUILD A MORE SECURE ALABAMA.

BY THE NUMBERS (RECENT TRENDS)

- **60+** LOCAL GOVERNMENTS RECEIVING SLCGP FUNDING
- **HUNDREDS** OF PROJECTS SUPPORTED STATEWIDE
- **ONE MISSION:** BUILD CYBER RESILIENT COMMUNITIES ACROSS ALABAMA

FOLLOW US:

oit.alabama.gov · Alabama OIT · Alabama OIT

ENABLING TODAY. EMPOWERING TOMORROW.

SERVING ALABAMA.

McCRARY INSTITUTE & THE SLCGP

WHO IS McCRARY?

A TRUSTED, NONPARTISAN INSTITUTE WITH DEEP EXPERTISE IN PUBLIC SAFETY, GOVERNANCE, AND TECHNOLOGY.

- ✓ INDEPENDENT & IMPARTIAL
- ✓ NONPROFIT & MISSION DRIVEN
- ✓ DECADES OF EXPERIENCE SERVING PUBLIC SECTOR LEADERS
- ✓ PRACTICAL SOLUTIONS. MEASURABLE IMPACT.

★ OUR MISSION: STRENGTHEN COMMUNITIES THROUGH EXPERTISE, COLLABORATION, AND INNOVATION.

OUR PURPOSE

LEVERAGE CYBERSECURITY EXPERTISE, INTELLIGENCE, AND COLLABORATION TO HELP LOCAL GOVERNMENT ENTITIES REDUCE RISK, IMPROVE RESILIENCE, AND DELIVER BETTER SERVICES TO THEIR COMMUNITIES.

THE SLCGP

McCRARY'S STRENGTH IN CYBERSECURITY

- ✓ CYBERSECURITY EXPERTISE & STRATEGY
- ✓ THREAT INTELLIGENCE & ANALYSIS
- ✓ SECURE TECHNOLOGIES & SOLUTIONS
- ✓ INCIDENT RESPONSE & RESILIENCE
- ✓ RISK REDUCTION THAT WORKS
- ✓ STRONGER, SAFER COMMUNITIES

OUR EXPERTISE

- CYBERSECURITY STRATEGY
- THREAT INTELLIGENCE & ANALYSIS
- RISK ASSESSMENT & MANAGEMENT
- INCIDENT RESPONSE & RESILIENCE
- SECURITY TRAINING & AWARENESS
- COLLABORATION & ADVISORY

HOW WE HELP ALABAMA

ADVISE ALABAMA OIT ON THE CYBERSECURITY LANDSCAPE, TRENDS, AND EMERGING RISKS.

INTELLIGENCE SHARING
FACILITATE TIMELY CYBER THREAT INTELLIGENCE SHARING ACROSS LOCAL GOVERNMENTS.

SUPPORT THE ALABAMA CYBERSECURITY INTELLIGENCE CENTER (ACIC)
STRENGTHEN CAPABILITIES, COORDINATION, AND SITUATIONAL AWARENESS.

CONNECT & COLLABORATE
CONNECT EXPERTS, RESOURCES, AND PARTNERS TO SOLVE REAL-WORLD CHALLENGES.

THE PATH TO STRONGER PROTECTIONS

UNDERSTAND THREATS & RISKS → ASSESS & PRIORITIZE → PLAN & RECOMMEND → IMPLEMENT SOLUTIONS → MEASURE, MONITOR & IMPROVE

PRACTICAL PROJECTS THAT DELIVER MEASURABLE, SUSTAINABLE CYBER PROTECTIONS FOR LOCAL GOVERNMENT ENTITIES.

FOCUS AREAS

- IDENTITY & ACCESS MANAGEMENT
- EMAIL & ENDPOINT PROTECTION
- DATA PROTECTION & BACKUP RESILIENCE
- NETWORK SECURITY
- POLICIES & GOVERNANCE
- VENDOR & THIRD-PARTY RISK MANAGEMENT

WHO WE SERVE

COUNTIES · CITIES & TOWNS · UTILITIES · PUBLIC AUTHORITIES · OTHER LOCAL ENTITIES

HOW WE WORK

LISTEN — UNDERSTAND NEEDS
DESIGN — PRACTICAL SOLUTIONS
DELIVER — EXPERT GUIDANCE & SUPPORT
APPLY — TOOLS THAT REDUCE RISK

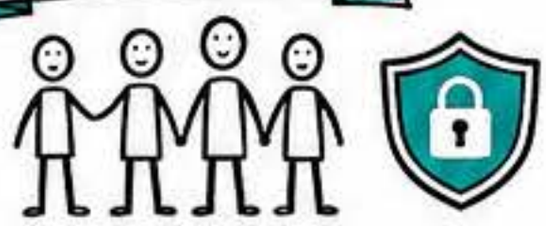
IMPACT

- STRONGER SECURITY POSTURE
- MORE RESILIENT COMMUNITIES
- REDUCED RISK & POTENTIAL COST
- CONFIDENCE TO FOCUS ON CORE SERVICES
- COMPLIANCE & ACCOUNTABILITY

EXPERTISE THAT PROTECTS. INTELLIGENCE THAT CONNECTS.
STRONGER LOCAL GOVERNMENTS. SAFER COMMUNITIES.

ALABAMA CYBERSECURITY INTELLIGENCE CENTER (ACIC)

WHO WE ARE



A PUBLIC-PRIVATE PARTNERSHIP SERVING ALABAMA TO ANTICIPATE, DETECT, AND RESPOND TO CYBER THREATS.

WE BRING TOGETHER

- STATE, LOCAL & FEDERAL GOVERNMENT
- PRIVATE SECTOR BUSINESSES
- ACADEMIA & RESEARCH PARTNERS
- COMMUNITIES & CRITICAL INFRASTRUCTURE STAKEHOLDERS

HOW WE OPERATE

COLLECT
GATHER DATA FROM MULTIPLE SOURCES

ANALYZE
TURN DATA INTO ACTIONABLE INTELLIGENCE

SHARE
DELIVER INTELLIGENCE TO OUR COMMUNITY

PROTECT
ENABLE INFORMED DECISIONS & STRONGER DEFENSES

IMPROVE
CONTINUOUSLY ADAPT AND ENHANCE TO STAY AHEAD OF THREATS

WHAT WE DO

- COLLECT & ANALYZE THREAT INTELLIGENCE
- SHARE TIMELY WARNINGS & INDICATORS
- FACILITATE COLLABORATION & INFORMATION SHARING
- SUPPORT INCIDENT RESPONSE & RECOVERY
- PROVIDE AWARENESS, TRAINING & RESOURCES

INTELLIGENCE. COLLABORATION. PROTECTION.

OUR MISSION

STRENGTHEN ALABAMA'S CYBER RESILIENCE BY SHARING THREAT INTELLIGENCE, FOSTERING COLLABORATION, AND EMPOWERING OUR COMMUNITIES, BUSINESSES, AND GOVERNMENT.

WHY IT MATTERS

CYBER THREATS ARE GROWING IN FREQUENCY, SOPHISTICATION & IMPACT.

60%
OF SMALL BUSINESSES CLOSE WITHIN 6 MONTHS OF A CYBER ATTACK.

SOURCE: NATIONAL CYBER SECURITY ALLIANCE

$10.5T
ESTIMATED GLOBAL COST OF CYBER CRIME ANNUALLY BY 2025.

SOURCE: CYBERSECURITY VENTURES

OUR IMPACT

STRONGER TOGETHER
A COMMUNITY OF TRUST AND SHARED PURPOSE

FASTER RESPONSE
TIMELY INTELLIGENCE REDUCES RISK & IMPACT

BETTER OUTCOMES
INFORMED DECISIONS DRIVE RESILIENCE

A SAFER ALABAMA
PROTECTING WHAT MATTERS MOST

FOCUS AREAS

- CRITICAL INFRASTRUCTURE PROTECTION
- THREAT INTELLIGENCE & ANALYSIS
- WORKFORCE DEVELOPMENT & AWARENESS
- POLICY, RISK & COMPLIANCE SUPPORT
- PUBLIC-PRIVATE PARTNERSHIPS

EXAMPLES OF VALUE

- EARLY WARNING OF EMERGING THREATS
- SHARED INDICATORS TO BLOCK ATTACKS
- COORDINATED INCIDENT RESPONSE
- REDUCED DUPLICATION & COST
- STRONGER SECURITY CULTURE
- MORE RESILIENT ORGANIZATIONS

WHO SHOULD ENGAGE?

- BUSINESS & IT LEADERS
- CISOS & SECURITY TEAMS
- GOVERNMENT AGENCIES
- CRITICAL INFRASTRUCTURE OPS
- ACADEMIA & RESEARCHERS
- ANYONE COMMITTED TO A SAFER ALABAMA

GET INVOLVED

- SHARE INFORMATION
- PARTICIPATE IN EVENTS & WORKING GROUPS
- BUILD YOUR TEAM'S CYBER SKILLS
- STAY INFORMED
- BE A FORCE FOR A SAFER ALABAMA

ACIC
ALABAMA CYBERSECURITY INTELLIGENCE CENTER

TOGETHER, WE CAN
ANTICIPATE. PREPARE. PROTECT.
BE PART OF THE SOLUTION.

LEARN MORE & CONNECT
www.acic.alabama.gov
@ACIC_Alabama

FEMA AND ITS ROLE IN SLCGP

WHO IS FEMA?

FEDERAL EMERGENCY MANAGEMENT AGENCY – A U.S. DEPARTMENT OF HOMELAND SECURITY AGENCY.

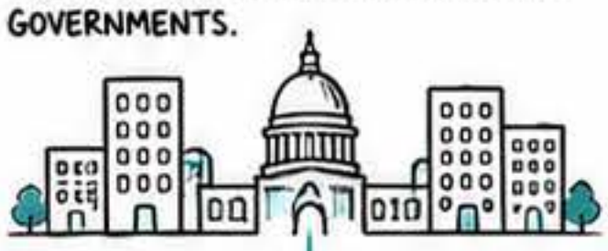
MISSION:
HELP PEOPLE BEFORE, DURING, AND AFTER DISASTERS.

CORE RESPONSIBILITIES

- SUPPORT STATE, LOCAL, TRIBAL & TERRITORIAL PARTNERS
- BUILD CAPACITY & RESILIENCE
- RESPOND TO DISASTERS
- SUPPORT RECOVERY

WHAT IS SLCGP?

THE STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP) STRENGTHENS CYBERSECURITY CAPABILITIES ACROSS STATE, LOCAL, TRIBAL & TERRITORIAL GOVERNMENTS.



FUNDING + RESOURCES
TO REDUCE RISK, IMPROVE DEFENSES, AND ENHANCE CYBER RESILIENCE.

FEMA'S ROLE IN SLCGP

1. **FEDERAL LEADERSHIP**
   FEMA ADMINISTERS SLCGP ON BEHALF OF DHS.
2. **FUNDING & OVERSIGHT**
   MANAGES GRANT FUNDS, ENSURES ACCOUNTABILITY, AND COMPLIANCE.
3. **CAPACITY BUILDING**
   PROVIDES TOOLS, GUIDANCE, TRAINING & TECHNICAL ASSISTANCE.
4. **RISK REDUCTION**
   SUPPORTS INVESTMENTS THAT REDUCE CYBER RISK TO CRITICAL SERVICES & INFRASTRUCTURE.
5. **COLLABORATION**
   CONNECTS PARTNERS WITH FEDERAL RESOURCES AND SHARES THREAT INFORMATION.

SLCGP FUNDING BREAKDOWN

- 80% TO STATES FOR SUBGRANTS TO ELIGIBLE ENTITIES
- 20% SET-ASIDE FOR NATIONAL INITIATIVES

★ FUNDING IS COMPETITIVE AND PERFORMANCE BASED.

HOW FUNDS CAN BE USED

- CYBER RISK ASSESSMENTS
- THREAT DETECTION & RESPONSE
- WORKFORCE DEVELOPMENT
- SECURE CONFIGURATIONS & TECHNOLOGY
- PLANNING & POLICY DEVELOPMENT
- EXERCISES & TABLETOPS
- INFORMATION SHARING

PREPARING TODAY, PROTECTING TOMORROW

STRONGER COMMUNITIES.
SAFER PEOPLE.
RESILIENT NATION.

WHO CAN APPLY?

- STATE GOVERNMENTS
- LOCAL GOVERNMENTS
- TRIBAL GOVERNMENTS
- U.S. TERRITORIES
- PUBLIC K-12 SCHOOL DISTRICTS
- HIGHER EDUCATION INSTITUTIONS
- SPECIAL DISTRICTS
- STATE-RECOGNIZED TRIBAL ORGS

THE SLCGP GRANT PROCESS

1. **PLAN** – ASSESS RISKS & DEVELOP STRATEGY
2. **APPLY** – SUBMIT COMPETITIVE APPLICATION
3. **AWARD** – FEMA REVIEWS & AWARDS FUNDS TO STATES
4. **SUBGRANT** – STATES AWARD FUNDS TO ELIGIBLE ENTITIES
5. **IMPLEMENT** – BUILD CAPABILITIES, REDUCE RISK, IMPROVE RESILIENCE
6. **REPORT** – MEASURE OUTCOMES & DEMONSTRATE IMPACT

CONTINUOUS IMPROVEMENT & RESILIENCE

THE IMPACT

- STRONGER CYBER DEFENSES
- PROTECTED CRITICAL SERVICES
- MORE RESILIENT COMMUNITIES
- A SAFER, MORE SECURE NATION

> "CYBER RESILIENCE IS A TEAM SPORT. FEMA AND OUR PARTNERS BUILD THE TEAM."

KEY TAKEAWAYS

- FEMA LEADS AND ADMINISTERS SLCGP.
- FUNDING BUILDS LOCAL CYBER RESILIENCE.
- COLLABORATION DRIVES STRONGER OUTCOMES.
- PREPARATION TODAY PREVENTS DISRUPTION TOMORROW.

LEARN MORE

FEMA.GOV | CISA.GOV | YOUR STATE HOMELAND SECURITY OFFICE

PARTNER. PLAN. PROTECT. TOGETHER.

CISA AND ITS ROLE IN SLCGP

BRIDGE BETWEEN CYBERSECURITY & PROCUREMENT

ENSURES SECURITY IS BUILT IN, NOT BOLTED ON

WHAT IS CISA?

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

- U.S. FEDERAL AGENCY UNDER DHS
- DEFENDS CRITICAL INFRASTRUCTURE
- REDUCES RISK TO THE NATION'S CYBER AND PHYSICAL SYSTEMS

WHY CISA IN SLCGP?

- BUILDS SECURE, RESILIENT SOLUTIONS FROM THE START
- REDUCES CYBER RISK ACROSS THE ACQUISITION LIFECYCLE
- PREVENTS COSTLY REWORK AND DELAYS
- SUPPORTS MISSION SUCCESS AND PUBLIC TRUST

CISA CORE FOCUS AREAS

- **SECURE BY DESIGN** — Integrate security early in requirements
- **RISK MANAGEMENT** — Identify, assess, and mitigate risks
- **SUPPLY CHAIN RISK** — Ensure trusted, secure suppliers & components
- **ZERO TRUST** — Architecture & principles
- **CONTINUOUS MONITORING & INCIDENT RESPONSE**

VALUE TO SLCGP

- **STRONGER PROPOSALS** — Demonstrate security maturity
- **MEET COMPLIANCE & POLICY REQUIREMENTS** (FAR, NIST, EO 14028, CMMC, etc.)
- **DIFFERENTIATE IN COMPETITIVE ACQUISITIONS**
- **IMPROVE CUSTOMER CONFIDENCE & TRUST**

CISA INTEGRATION THROUGH THE SLCGP LIFECYCLE

1. Solicitation	2. Evaluation	3. Award	4. Performance	5. Closeout
Incorporate security requirements • Clear expectations • Align to frameworks • Supplier capability evaluation	Assess security approaches • Risk & controls • Supply chain risk • Past performance	Include security in contract • Clauses • Deliverables • Reporting	Monitor & manage security • Continuous monitoring • Incident response • Change management	Capture lessons learned • Performance data • Improvements • Knowledge transfer

SECURITY IS CONTINUOUS, NOT A CHECKBOX. CISA HELPS MAKE IT PART OF EVERY STEP.

THE STAKES ARE HIGH

- **85%** of cyber incidents involve the supply chain (Source: Verizon DBIR 2024)
- **60%+** of organizations have experienced a supply chain compromise
- **$4.88M** Average cost of a data breach in 2024 (Source: IBM)

KEY ENABLERS

- **CISA GUIDANCE & TOOLS** — Risk management, Secure by Design, Supply Chain, Zero Trust
- **FRAMEWORKS & STANDARDS** — NIST, CMMC, ISO 27001, FedRAMP, CIS Controls
- **TRAINING & AWARENESS** — Build security skills across teams
- **DATA & THREAT INTELLIGENCE** — Inform decisions, reduce risk

COLLABORATION MAKES IT WORK

GOVERNMENT + INDUSTRY WORKING TOGETHER

- Early Engagement
- Shared Expectations
- Transparent Communication

OUTCOMES / IMPACT

- REDUCED CYBER RISK
- MORE SECURE, RELIABLE SOLUTIONS
- LOWER TOTAL COST OF OWNERSHIP
- STRONGER MISSION OUTCOMES
- INCREASED PUBLIC TRUST & CONFIDENCE

KEY TAKEAWAYS

- **START EARLY** — Integrate security into planning & requirements
- **COLLABORATE OFTEN** — Align with CISA guidance & stakeholders
- **MANAGE CONTINUOUSLY** — Monitor, adapt, and improve
- **DELIVER VALUE** — Secure solutions that meet mission and business goals

CISA + SLCGP = SECURE ACQUISITIONS, STRONGER MISSIONS, A SAFER NATION.