EFSP Auxiliary ESL Curriculum

Cybersecurity English Jargon Quick Reference

Field-specific terms, contrast pairs, and high-pressure sentence frames

Audience: security analysts, SOC staff, incident responders, security engineers, GRC specialists, identity teams, vulnerability managers, and security leaders

Focus: A cybersecurity English curriculum for incident response, vulnerability triage, identity, threat modeling, risk communication, compliance, executive briefings, and security pushback.

Designed for advanced ESL learners who already use professional English and need industry-specific terminology, realistic meetings, role-play pressure, careful pushback, and polished workplace outputs.

Teaching stance: this is language and workplace-communication training, not legal, medical, financial, safety, or regulatory advice. Instructors should connect every scenario to the learner's current company policies, local rules, and approved procedures.

Nomenclature and Jargon

These are classroom working definitions. Learners should adapt wording to their organization's policies, systems, and local regulatory environment.

Security Triage and Alert Investigation

Term	Working meaning
SIEM	Working cybersecurity term used in security triage and alert investigation; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
alert	Working cybersecurity term used in security triage and alert investigation; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
false positive	Working cybersecurity term used in security triage and alert investigation; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
privileged account	Working cybersecurity term used in security triage and alert investigation; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Incident Response and Containment

Term	Working meaning
incident	Unplanned event that disrupts service, safety, quality, security, operations, or expected performance.
containment	Working cybersecurity term used in incident response and containment; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
ransomware	Working cybersecurity term used in incident response and containment; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
forensics	Working cybersecurity term used in incident response and containment; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Vulnerability Management

Term	Working meaning
CVE	Working cybersecurity term used in vulnerability management; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
CVSS	Working cybersecurity term used in vulnerability management; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
exploitability	Working cybersecurity term used in vulnerability management; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
compensating control	Working cybersecurity term used in vulnerability management; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Identity, Access, and Least Privilege

Term	Working meaning
IAM	Working cybersecurity term used in identity, access, and least privilege; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
least privilege	Working cybersecurity term used in identity, access, and least privilege; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Term	Working meaning
MFA	Working cybersecurity term used in identity, access, and least privilege; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
RBAC	Working cybersecurity term used in identity, access, and least privilege; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Threat Modeling and Secure Design

Term	Working meaning
threat model	Working cybersecurity term used in threat modeling and secure design; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
attack surface	Working cybersecurity term used in threat modeling and secure design; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
trust boundary	Working cybersecurity term used in threat modeling and secure design; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
abuse case	Working cybersecurity term used in threat modeling and secure design; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Governance, Risk, and Compliance

Term	Working meaning
control	A process, approval, check, or technical safeguard designed to reduce risk.
audit evidence	Working cybersecurity term used in governance, risk, and compliance; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
risk acceptance	Working cybersecurity term used in governance, risk, and compliance; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
remediation	Working cybersecurity term used in governance, risk, and compliance; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Security Awareness and Phishing

Term	Working meaning
phishing	Working cybersecurity term used in security awareness and phishing; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
social engineering	Working cybersecurity term used in security awareness and phishing; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
reporting culture	Working cybersecurity term used in security awareness and phishing; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
security awareness	Working cybersecurity term used in security awareness and phishing; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Executive Risk Briefings

Term	Working meaning
residual risk	Working cybersecurity term used in executive risk briefings; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
threat actor	Working cybersecurity term used in executive risk briefings; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Term	Working meaning
maturity	Working cybersecurity term used in executive risk briefings; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
investment ask	Working cybersecurity term used in executive risk briefings; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Industry-Specific Meeting Moves

Situation	Useful language
Security Triage and Alert Investigation	Before we commit, I want to confirm SIEM, alert, the owner, and the evidence behind the decision. If privilege, behavior, context, and evidence need review., I recommend we document the risk and agree on the next step.
Incident Response and Containment	Before we commit, I want to confirm incident, containment, the owner, and the evidence behind the decision. If scope, containment, evidence preservation, communications, and legal review matter., I recommend we document the risk and agree on the next step.
Vulnerability Management	Before we commit, I want to confirm CVE, CVSS, the owner, and the evidence behind the decision. If exploitability, exposure, asset criticality, compensating controls, and downtime must be balanced., I recommend we document the risk and agree on the next step.
Identity, Access, and Least Privilege	Before we commit, I want to confirm IAM, least privilege, the owner, and the evidence behind the decision. If least privilege, approval, logging, and time-bound access are required., I recommend we document the risk and agree on the next step.
Threat Modeling and Secure Design	Before we commit, I want to confirm threat model, attack surface, the owner, and the evidence behind the decision. If abuse cases, data flows, trust boundaries, and mitigations need design-time attention., I recommend we document the risk and agree on the next step.
Governance, Risk, and Compliance	Before we commit, I want to confirm control, audit evidence, the owner, and the evidence behind the decision. If control design, evidence, ownership, remediation, and risk acceptance need clarity., I recommend we document the risk and agree on the next step.
Security Awareness and Phishing	Before we commit, I want to confirm phishing, social engineering, the owner, and the evidence behind the decision. If behavior, training, reporting culture, and technical controls all matter., I recommend we document the risk and agree on the next step.
Executive Risk Briefings	Before we commit, I want to confirm residual risk, threat actor, the owner, and the evidence behind the decision. If residual risk, threat landscape, controls, investment, and response readiness require nuance., I recommend we document the risk and agree on the next step.

High-pressure pushback frames

- I understand the urgency. The risk is that we move faster than the evidence or process supports.
- I am not blocking the goal. I am naming the condition we need before the decision is safe and credible.
- If we accept this risk, we should name the owner, document the assumption, and define the trigger for escalation.
- That may be possible, but not under the current scope, timeline, or approval path.
- Let's separate what we know, what we assume, and what still needs confirmation.

Contrast Pairs

Do not confuse	Useful distinction
SIEM vs privileged account	In security triage and alert investigation, define whether the discussion is about the current fact pattern, the controlling process, the stakeholder pressure, or the final decision.

Do not confuse	Useful distinction
incident vs forensics	In incident response and containment, define whether the discussion is about the current fact pattern, the controlling process, the stakeholder pressure, or the final decision.
CVE vs compensating control	In vulnerability management, define whether the discussion is about the current fact pattern, the controlling process, the stakeholder pressure, or the final decision.
IAM vs RBAC	In identity, access, and least privilege, define whether the discussion is about the current fact pattern, the controlling process, the stakeholder pressure, or the final decision.
threat model vs abuse case	In threat modeling and secure design, define whether the discussion is about the current fact pattern, the controlling process, the stakeholder pressure, or the final decision.
control vs remediation	In governance, risk, and compliance, define whether the discussion is about the current fact pattern, the controlling process, the stakeholder pressure, or the final decision.
phishing vs security awareness	In security awareness and phishing, define whether the discussion is about the current fact pattern, the controlling process, the stakeholder pressure, or the final decision.
residual risk vs investment ask	In executive risk briefings, define whether the discussion is about the current fact pattern, the controlling process, the stakeholder pressure, or the final decision.