TLCTC JSON Architecture

Organizations need a standardized way to share threat intelligence that separates universal framework definitions from specific attack instances. This guide explains the TLCTC JSON architecture that enables worldwide threat intelligence sharing while maintaining consistency and precision.

Feb 5, 2026 • Bernhard Kreinz • 28 min read

🎯 Understanding the Architecture

The TLCTC framework operates on two distinct but interconnected layers:

📚 Framework Layer (Static)

- Universal threat taxonomy
- Cluster definitions & axioms
- Generic vulnerabilities
- Framework rules & notation
- Control examples

Purpose: Common language everyone uses
Changes: Rarely (framework evolution)

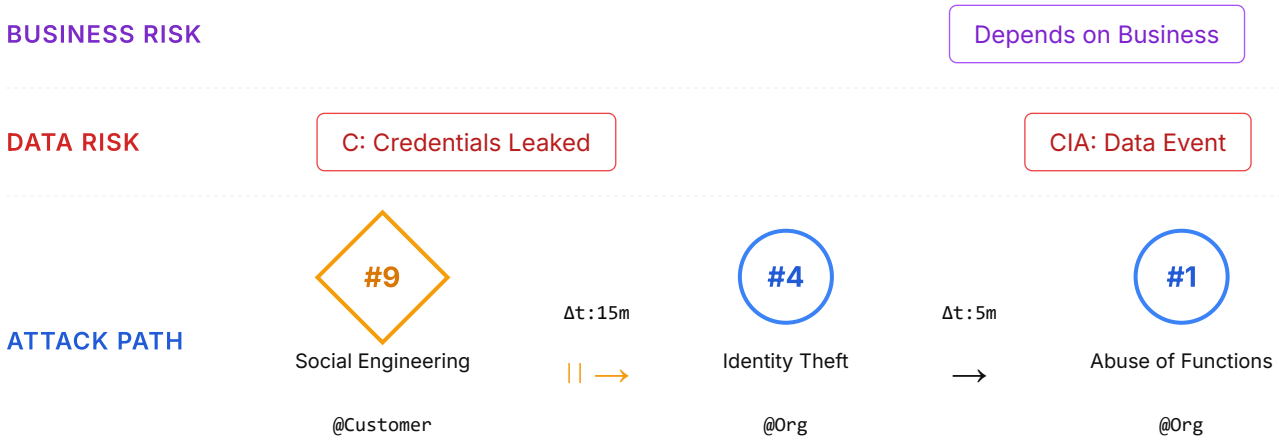
🔍 Intelligence Layer (Dynamic)

- Specific attack instances
- Software versions & CVEs
- Timeline & actor TTPs
- Domain boundaries
- Impact assessment

Purpose: Actual threat intelligence
Changes: Constantly (new incidents)

🎯 The Three-Lane Conceptual Model

TLCTC attack path analysis operates across **three interconnected analytical lanes**. The JSON architecture captures all three lanes and their relationships:



Lane 1: Attack Path
Clusters, velocity (Δt), boundaries, @Spheres
JSON: `attack_sequence[]`

Lane 2: Data Risk

DREs (C/I/A) linked to specific steps

JSON: `attack_sequence[].data_risk_events[]`

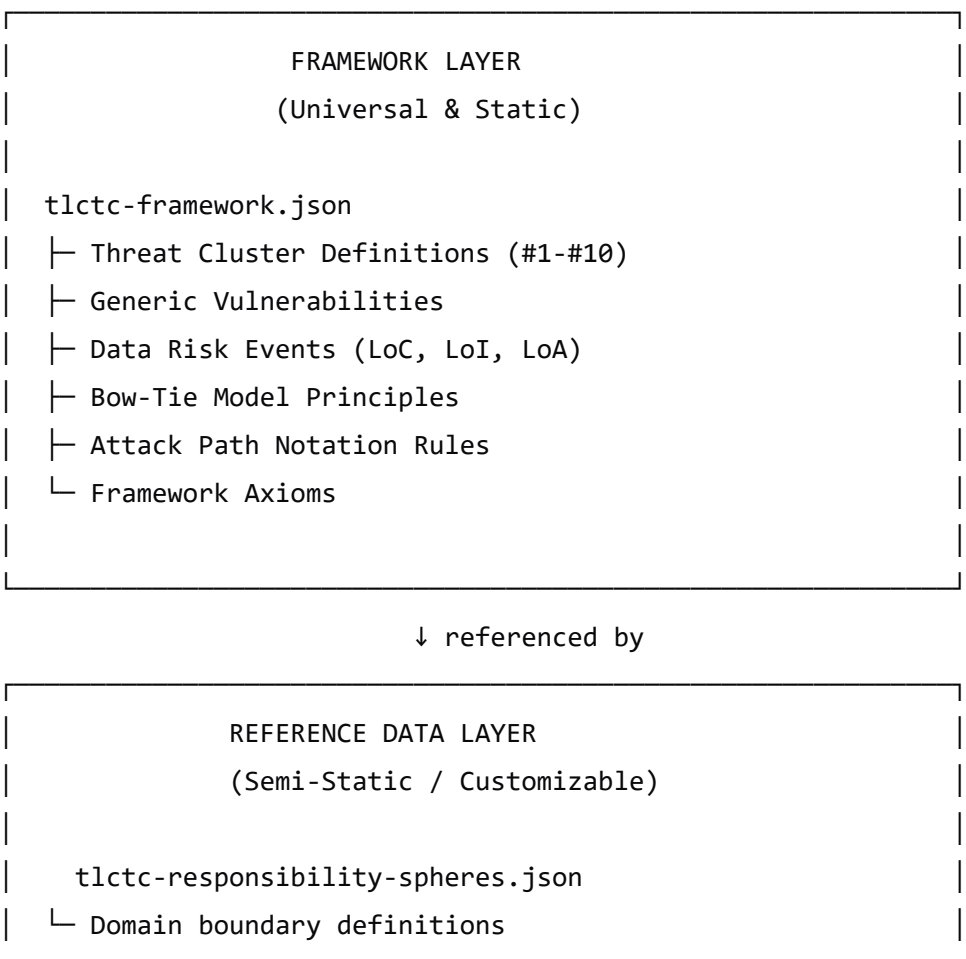
Lane 3: Business Risk

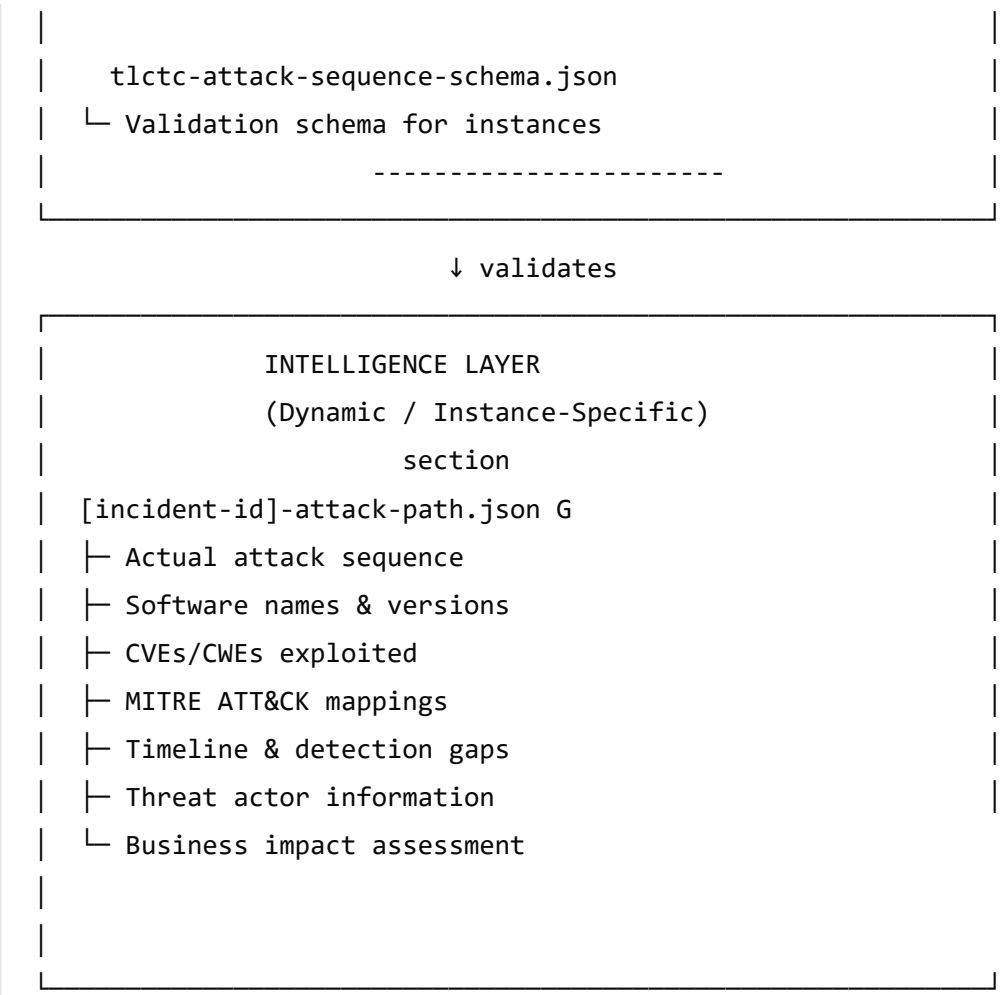
Business impacts linked to steps/DREs

JSON: `business_impacts[]`

Cross-Lane Linkage

- **Attack → Data:** Each step MAY have `data_risk_events[]` recording what data impacts occurred
- **Data → Business:** Each business impact MUST reference either a step (`linked_to_step`) or DRE (`linked_to_dre`)
- **Vertical causality:** The upward arrows represent causal relationships captured through these explicit links





📋 JSON Structure Overview

JSON FILE	PURPOSE	SCOPE	UPDATE FREQUENCY
`tlctc-framework.json`	Core framework definitions	Universal	Rarely (framework updates)
`tlctc-responsibility-spheres.json`	Domain boundary definitions	Customizable	Occasionally (org changes)
`tlctc-attack-sequence-schema.json`	Validation schema	Universal	Rarely (schema evolution)
`[incident]-attack-path.json`	Specific attack instance	Per-incident	Per incident

📦 1. Framework Definition JSON

This is the foundation - the universal taxonomy that everyone references. It contains the threat cluster definitions, generic vulnerabilities, and framework rules.

> **Key Purpose**
>
> Provides the common language for threat classification. Every organization references the same framework, ensuring consistency in threat intelligence sharing.

`tlctc-framework.json`


```
{
  "metadata": {
    "framework": "Top Level Cyber Threat Clusters (TLCTC)",
    "version": "1.9.1",
    "date": "2025-11-09",
    "author": "Bernhard Kreinz",
    "description": "Universal threat taxonomy for cyber risk management",
    "website": "https://www.tlctc.net"
  },

  "notation_systems": {
    "strategic": {
      "format": "#X",
      "description": "Human-readable notation (e.g., #1, #10)",
      "use_case": "Executive communication, risk assessment"
    },
    "operational": {
      "format": "TLCTC-XX.YY",
      "description": "Machine-readable format (e.g., TLCTC-01.00)",
      "use_case": "Tool integration, automation, SIEM"
    },
    "sequence": {
      "format": "#X → #Y → #Z",
      "description": "Attack path progression",
```

```
      "parallel": "#X + #Y indicates simultaneous execution"
    }
  },

  "threat_clusters": [
    {
      "cluster_id": 1,
      "strategic_notation": "#1",
      "operational_notation": "TLCTC-01.00",
      "name": "Abuse of Functions",
      "definition": "An attacker abuses the logic or scope of existing, legitimate sof
tware functions, features, or configurations for malicious purposes. This manipulation
occurs through standard interfaces using expected input types (data, parameters, confi
gurations, sequence of actions), but in a way that subverts the intended purpose or se
curity controls.",
      "generic_vulnerability": "The scope, complexity, or inherent trust placed in leg
itimate software functions, features, and configurations.",
      "asset_type": "Software (logic, functions, configuration)",
      "key_principle": "Data remains data - no foreign code execution",
      "data_to_code": false,
      "attacker_view": "I abuse a functionality, not a coding issue",
      "developer_view": "I must understand and constrain the functional domain"
    },
    {
      "cluster_id": 2,
      "strategic_notation": "#2",
      "operational_notation": "TLCTC-02.00",
      "name": "Exploiting Server",
      "definition": "An attacker targets and leverages flaws originating directly with
in the server-side application's source code implementation using Exploit Code (foreig
n code). This forces a data→code transition by triggering a server-side implementation
flaw.",
      "generic_vulnerability": "The presence of exploitable flaws within the server-si
de source code implementation stemming from insecure coding practices.",
      "asset_type": "Software (server-side source code)",
      "key_principle": "Exploits implementation bugs with foreign code",
      "data_to_code": true,
      "transition_type": "unintended",
      "attacker_view": "I abuse a flaw in the server-side source code",
      "developer_view": "I must apply secure coding principles for server code",
      "refinements": [
        {
```

```
          "id": "TLCTC-02.01",
          "name": "Server Communication Protocol Exploit",
          "examples": ["SSL/TLS vulnerabilities", "HTTP response splitting"]
        },
        {
          "id": "TLCTC-02.02",
          "name": "Server Core Function Exploit",
          "examples": ["SQL injection", "Buffer overflows", "Command injection"]
        },
        {
          "id": "TLCTC-02.03",
          "name": "Server External Handler Exploit",
          "examples": ["SSI injection", "Script engine vulnerabilities"]
        }
      ]
    },
    {
      "cluster_id": 3,
      "strategic_notation": "#3",
      "operational_notation": "TLCTC-03.00",
      "name": "Exploiting Client",
      "definition": "An attacker targets and leverages flaws originating directly with
in the source code implementation of any software acting in a client role. This create
s a data→code transition by abusing a client-side implementation flaw.",
      "generic_vulnerability": "The presence of exploitable flaws within client softwa
re source code implementation.",
      "asset_type": "Software (client-side source code)",
      "key_principle": "Exploits client implementation bugs",
      "data_to_code": true,
      "transition_type": "unintended",
      "attacker_view": "I abuse a flaw in the client source code",
      "developer_view": "I must apply secure coding principles for client code",
      "refinements": [
        {
          "id": "TLCTC-03.01",
          "name": "Client Communication Protocol Exploit",
          "examples": ["TLS vulnerabilities", "HTTP request smuggling"]
        },
        {
          "id": "TLCTC-03.02",
          "name": "Client Core Function Exploit",
          "examples": ["XSS", "Buffer overflows in clients"]
```

```
        },
        {
          "id": "TLCTC-03.03",
          "name": "Client External Handler Exploit",
          "examples": ["PDF exploits", "Office document vulnerabilities"]
        }
      ]
    },
    {
      "cluster_id": 4,
      "strategic_notation": "#4",
      "operational_notation": "TLCTC-04.00",
      "name": "Identity Theft",
      "definition": "An attacker targets weaknesses in identity and access management processes or credential protection mechanisms to illegitimately misuse authentication credentials to impersonate a legitimate identity.",
      "generic_vulnerability": "Weak Identity Management Processes and/or inadequate credential protection mechanisms throughout the identity lifecycle.",
      "asset_type": "Software (IAM systems), Credentials",
      "key_principle": "Credential use always maps to #4, acquisition maps to enabling cluster",
      "credential_dual_nature": {
        "acquisition": {
          "mapping": "Enabling cluster (#1/#2/#3/#5/#7/#8/#9/#10)",
          "consequence": "Loss of Confidentiality"
        },
        "use": {
          "mapping": "Always #4 Identity Theft",
          "consequence": "Loss of Control (system compromise)"
        }
      },
      "attacker_view": "I abuse credentials to operate as a legitimate identity",
      "developer_view": "I must implement secure credential lifecycle management"
    },
    {
      "cluster_id": 5,
      "strategic_notation": "#5",
      "operational_notation": "TLCTC-05.00",
      "name": "Man in the Middle (MitM)",
      "definition": "An attacker intercepts, eavesdrops on, modifies, or relays communication between two parties by exploiting a privileged position on the communication path.",
```

```
      "generic_vulnerability": "The lack of sufficient control, integrity protection, or confidentiality over the communication channel/path.",
      "asset_type": "Network/Communication Channel & Path Infrastructure",
      "key_principle": "Position-based attack on communication path",
      "attacker_view": "I abuse my position between communicating parties",
      "developer_view": "I must ensure confidentiality and integrity of data in transit"
    },
    {
      "cluster_id": 6,
      "strategic_notation": "#6",
      "operational_notation": "TLCTC-06.00",
      "name": "Flooding Attack",
      "definition": "An attacker intentionally overwhelms system resources or exceeds capacity limits through a high volume of requests, data, or operations, leading to denial of service.",
      "generic_vulnerability": "Finite capacity limitations inherent in any system component.",
      "asset_type": "Software, Network, Hardware (finite resources)",
      "key_principle": "Resource exhaustion through volume",
      "primary_outcome": "Loss of Availability",
      "attacker_view": "I abuse the circumstance of always limited capacity",
      "developer_view": "I must implement efficient resource management"
    },
    {
      "cluster_id": 7,
      "strategic_notation": "#7",
      "operational_notation": "TLCTC-07.00",
      "name": "Malware",
      "definition": "An attacker abuses the inherent ability of a software environment to execute foreign executable content, including malicious code or legitimate tools executing attacker-controlled code.",
      "generic_vulnerability": "The software environment's designed capability to execute potentially untrusted 'foreign' code.",
      "asset_type": "Software (execution environment, introduced dual-use tools)",
      "key_principle": "Uses intended execution capabilities",
      "data_to_code": true,
      "transition_type": "intended",
      "sequential_pattern": {
        "pattern": "#1 → #7",
        "description": "Function abuse enabling foreign code execution",
        "examples": ["cmd.exe executing scripts", "Task Scheduler running malware"]
```

```
      },
      "attacker_view": "I abuse the environment's designed capability to execute code, which I introduce.",
      "developer_view": "I must control code execution paths"
    },
    {
      "cluster_id": 8,
      "strategic_notation": "#8",
      "operational_notation": "TLCTC-08.00",
      "name": "Physical Attack",
      "definition": "An attacker gains unauthorized physical interaction with or causes physical interference to hardware, devices, facilities, or data transmission media.",
      "generic_vulnerability": "The physical accessibility of hardware, facilities, and communication media.",
      "asset_type": "Physical (Hardware, Facilities, Media, Signals)",
      "refinements": [
        {
          "id": "TLCTC-08.01",
          "name": "Direct Physical Access",
          "description": "Requires physical touch/interaction",
          "examples": ["Hardware tampering", "Device theft", "USB baiting"]
        },
        {
          "id": "TLCTC-08.02",
          "name": "Indirect Physical Access",
          "description": "Exploits physical properties without direct contact",
          "examples": ["TEMPEST", "Signal jamming", "RFID skimming"]
        }
      ],
      "attacker_view": "I abuse physical accessibility of hardware and devices",
      "developer_view": "I must implement tamper-evident logging and secure failure modes"
    },
    {
      "cluster_id": 9,
      "strategic_notation": "#9",
      "operational_notation": "TLCTC-09.00",
      "name": "Social Engineering",
      "definition": "An attacker psychologically manipulates individuals into performing actions counter to their best interests, such as divulging information, granting access, or executing code.",
```

```
      "generic_vulnerability": "Human psychological factors: gullibility, trust, ignor
ance, fear, urgency, authority bias, curiosity.",
      "asset_type": "Human",
      "key_principle": "Purely human manipulation - technical vulnerabilities never ma
p to #9",
      "common_sequences": [
        {"pattern": "#9 → #4", "description": "Phishing to credential theft"},
        {"pattern": "#9 → #7", "description": "Tricking user to run malware"},
        {"pattern": "#9 → #1", "description": "Tricking user to misconfigure systems"}
      ],
      "attacker_view": "I abuse human trust and psychology",
      "developer_view": "I must design interfaces that promote secure behavior"
    },
    {
      "cluster_id": 10,
      "strategic_notation": "#10",
      "operational_notation": "TLCTC-10.00",
      "name": "Supply Chain Attack",
      "definition": "An attacker compromises systems by targeting vulnerabilities with
in an organization's supply chain, involving third-party components, hardware, service
s, or distribution mechanisms.",
      "generic_vulnerability": "The necessary reliance on and implicit trust placed in
external suppliers and their processes.",
      "asset_type": "Software, Hardware, Services (third-party elements)",
      "key_principle": "Marks trust/domain boundary transitions in attack sequences",
      "boundary_test": "If removing the third-party trust link would stop the step, #1
0 belongs there",
      "refinements": [
        {
          "id": "TLCTC-10.01",
          "name": "Update Vector",
          "description": "Post-deployment compromise via updates",
          "examples": ["SolarWinds", "Compromised auto-updates"]
        },
        {
          "id": "TLCTC-10.02",
          "name": "Development Vector",
          "description": "Pre-deployment compromise during development",
          "examples": ["Compromised build pipelines", "Malicious libraries"]
        },
        {
          "id": "TLCTC-10.03",
```

```
          "name": "Hardware Supply Chain",
          "description": "Hardware component compromise",
          "examples": ["Backdoored hardware", "Compromised manufacturing"]
        }
      ],
      "attack_path_usage": {
        "before": "Actions in attacker/compromised source domain",
        "at": "Trust/domain crossing (supply-chain transition)",
        "after": "Impact on downstream victims"
      },
      "attacker_view": "I abuse trust in third-party components",
      "developer_view": "I must maintain strict dependency hygiene"
    }
  ],

  "data_risk_events": [
    {
      "notation": "LoC",
      "name": "Loss of Confidentiality",
      "definition": "Data stolen - unauthorized access to data",
      "applicable_clusters": ["#1","#2","#3","#4","#5","#7","#8","#9","#10"]
    },
    {
      "notation": "LoI",
      "name": "Loss of Integrity",
      "definition": "Data modified - unauthorized changes to data",
      "applicable_clusters": ["#1","#2","#3","#4","#5","#7","#8","#9","#10"]
    },
    {
      "notation": "LoA",
      "name": "Loss of Availability",
      "definition": "Data inaccessible - data unavailable to legitimate users",
      "applicable_clusters": ["#1","#2","#3","#4","#5","#6","#7","#8","#9","#10"],
      "note": "Deletion and ransomware produce LoA outcomes"
    }
  ],

  "bow_tie_model": {
    "description": "Structured approach connecting threats (causes) with consequences
(effects)",
    "left_side": {
      "name": "Threats (Causes)",
```

```
      "content": "The 10 Top Level Cyber Threat Clusters",
      "controls": "Preventive (IDENTIFY, PROTECT)"
    },
    "center": {
      "name": "System Compromise / Loss of Control",
      "description": "Central risk event - pivot between threat and consequence"
    },
    "right_side": {
      "name": "Consequences (Effects)",
      "content": "Data Risk Events → Business Risk Events",
      "controls": "Detective, Reactive, Corrective (DETECT, RESPOND, RECOVER)"
    },
    "key_principle": "Never mix threats with events or confuse causes with effects"
  },

  "velocity_classes": {
    "description": "Attack velocity determines which defensive modes are structurally
viable",
    "classes": {
      "VC-1": {
        "name": "Strategic",
        "typical_delta_t": "Days to Months",
        "defense_mode": "Log retention, threat hunting, strategic monitoring"
      },
      "VC-2": {
        "name": "Tactical",
        "typical_delta_t": "Hours",
        "defense_mode": "SIEM alerting, analyst triage, guided response"
      },
      "VC-3": {
        "name": "Operational",
        "typical_delta_t": "Minutes",
        "defense_mode": "SOAR/EDR automation, rapid containment"
      },
      "VC-4": {
        "name": "Real-Time",
        "typical_delta_t": "Seconds to Milliseconds",
        "defense_mode": "Architecture, circuit breakers, rate limits"
      }
    },
    "key_insight": "If critical transition is VC-3+, purely human response is structur
ally insufficient"
```

```
  },

  "attack_path_rules": {
    "sequential_notation": "#X → #Y → #Z",
    "parallel_notation": "#X + #Y",
    "velocity_notation": "→[Δt=15m]→ or →[Δt=2h]→",
    "boundary_notation": "|||[context][@Source→@Target]||",
    "dre_notation": "+ [DRE: C] or + [DRE: C,I,A]",
    "principles": [
      "Each cluster in attack path should be counted",
      "Arrows show progression",
      "Plus signs show simultaneous execution",
      "Supply Chain (#10) marks trust boundaries",
      "Credential acquisition ≠ credential use"
    ],
    "common_patterns": {
      "phishing_to_malware": "#9 → #3 → #7",
      "phishing_to_creds": "#9 → #4",
      "exploit_to_malware": "#2 → #7 or #3 → #7",
      "lolbas_execution": "#1 → #7",
      "supply_chain": "#X → #Y → #10 → #7"
    }
  }
}
```

📦 2. Responsibility Spheres JSON

Defines the domain boundaries where responsibility and control shift during an attack. This is semi-static and can be customized per organization.

> ⚠️ **Why This Matters**
>
> Understanding where an attack crosses domain boundaries is critical for incident response, forensics, and legal responsibility. The "sphere" tells you whose assets, whose controls, and whose responsibility is involved at each step.

🌐 `tlctc-responsibility-spheres.json`

```
{
  "metadata": {
    "schema": "TLCTC Responsibility Spheres",
    "version": "1.0",
    "description": "Domain boundary definitions for attack path analysis",
    "customizable": true
  },

  "responsibility_spheres": [
    {
      "id": "@External",
      "name": "External / Attacker Side",
      "description": "Infrastructure and assets controlled by the threat actor or exte
rnal parties",
      "characteristics": [
        "Attacker has full control",
        "No legitimate authority",
        "Source of malicious activity"
      ],
      "typical_assets": [
        "Command & Control (C2) servers",
        "Attacker workstations",
        "Bot networks",
        "Staging infrastructure"
      ],
      "examples": [
        "Attacker's C2 server",
        "Phishing kit hosting server",
        "Attacker's development environment"
      ]
    },
    {
      "id": "@Public",
      "name": "Public Infrastructure",
      "description": "Internet backbone, DNS, public services not controlled by victim
or attacker",
      "characteristics": [
        "Shared public resources",
        "Multiple stakeholders",
        "Generally trusted by default"
      ],
```

```
      "typical_assets": [
        "DNS servers",
        "Public cloud services",
        "Content Delivery Networks (CDNs)",
        "Internet routing infrastructure",
        "Public repositories (npm, PyPI)"
      ],
      "examples": [
        "Compromised npm package",
        "Malicious DNS redirect",
        "BGP hijacking"
      ]
    },
    {
      "id": "@Vendor",
      "name": "Third Party / Vendor",
      "description": "Infrastructure and services provided by trusted third parties",
      "characteristics": [
        "Trust relationship exists",
        "Limited visibility",
        "Contractual relationship"
      ],
      "typical_assets": [
        "Vendor software/services",
        "SaaS platforms",
        "Managed service provider systems",
        "Supply chain components"
      ],
      "examples": [
        "SolarWinds Orion platform",
        "Compromised SaaS provider",
        "Third-party API service"
      ],
      "note": "When this sphere is compromised, #10 Supply Chain often marks the trans
ition"
    },
    {
      "id": "@Org(Perimeter)",
      "name": "Organization Perimeter",
      "description": "The boundary between external and internal organization systems"
,
      "characteristics": [
```

```
      "First line of defense",
      "Network edge",
      "Gateway systems"
    ],
    "typical_assets": [
      "Firewalls",
      "DMZ systems",
      "Public-facing web servers",
      "VPN gateways",
      "Email gateways"
    ],
    "examples": [
      "Web application firewall",
      "VPN endpoint",
      "Public email server"
    ]
  },
  {
    "id": "@Org",
    "name": "Organization Internal",
    "description": "Internal corporate network and systems",
    "characteristics": [
      "Organization has full control",
      "Internal security policies apply",
      "Critical business systems"
    ],
    "typical_assets": [
      "Internal servers",
      "Databases",
      "Active Directory",
      "File shares",
      "Internal applications"
    ],
    "examples": [
      "Domain controller",
      "HR database",
      "Internal file server"
    ]
  },
  {
    "id": "@Customer",
    "name": "Customer / End User Side",
```

```
    "description": "End-user or customer-controlled environment",
    "characteristics": [
      "Limited organizational control",
      "User devices and networks",
      "BYOD scenarios"
    ],
    "typical_assets": [
      "User laptops",
      "Mobile devices",
      "Home networks",
      "Personal cloud storage"
    ],
    "examples": [
      "Employee home laptop",
      "Personal mobile device",
      "Home WiFi network"
    ]
  },
  {
    "id": "@Org(Admin)",
    "name": "Privileged / Admin Level",
    "description": "High-privilege administrative systems and accounts",
    "characteristics": [
      "Elevated access rights",
      "Critical control plane",
      "High-value targets"
    ],
    "typical_assets": [
      "Admin workstations",
      "Privileged access management systems",
      "Domain controllers",
      "Security tools with elevated access"
    ],
    "examples": [
      "Domain admin account",
      "Cloud admin console",
      "Security operations console"
    ]
  }
],

"sphere_transitions": {
```

```
    "description": "Common patterns of how attacks move between spheres",
    "patterns": [
      {
        "name": "External to Internal",
        "path": "attacker-side → organization-perimeter → organization-internal",
        "description": "Classic network breach pattern"
      },
      {
        "name": "Supply Chain Compromise",
        "path": "attacker-side → third-party-vendor → organization-internal",
        "description": "Attack via trusted third party"
      },
      {
        "name": "Phishing Entry",
        "path": "attacker-side → customer-side → organization-internal",
        "description": "Social engineering via end user"
      },
      {
        "name": "Privilege Escalation",
        "path": "organization-internal → privileged-admin",
        "description": "Internal movement to admin access"
      }
    ]
  },

  "usage_guidelines": {
    "purpose": "Document whose infrastructure/assets are involved at each attack step"
,
    "legal_implications": "Sphere information aids in determining liability and respon
sibility",
    "forensics": "Critical for understanding evidence location and jurisdiction",
    "incident_response": "Determines who needs to be involved in response efforts"
  },

  "boundary_contexts": [
    { "id": "dev", "name": "Development/Build", "description": "CI/CD, software supply
chain", "typical_clusters": ["#10"] },
    { "id": "update", "name": "Update Channel", "description": "Software updates, patc
hes", "typical_clusters": ["#10"] },
    { "id": "auth", "name": "Authentication/Federation", "description": "IdP/SP federa
tion, SSO", "typical_clusters": ["#4", "#10"] },
    { "id": "human", "name": "Human Interaction", "description": "Social engineering v
```

```
ector", "typical_clusters": ["#9"] },
    { "id": "physical", "name": "Physical Access", "description": "Physical security c
rossing", "typical_clusters": ["#8"] },
    { "id": "runtime", "name": "Runtime Services", "description": "Managed services, S
aaS control planes", "typical_clusters": ["#10"] },
    { "id": "admin", "name": "Administrative", "description": "Admin/management plane
access", "typical_clusters": ["#1", "#10"] }
  ],

  "business_impact_categories": [
    { "id": "operational", "name": "Operational Impact", "description": "Disruption to
business operations and service delivery" },
    { "id": "financial", "name": "Financial Impact", "description": "Direct monetary l
oss or financial damage" },
    { "id": "reputational", "name": "Reputational Impact", "description": "Damage to b
rand, trust, and stakeholder confidence" },
    { "id": "regulatory", "name": "Regulatory Impact", "description": "Compliance viol
ations, legal exposure, regulatory action" },
    { "id": "strategic", "name": "Strategic Impact", "description": "Long-term competi
tive or market position damage" }
  ]
}
```


📦 3. Attack Sequence Schema JSON

This is the validation schema that defines what fields an attack path instance must/should contain. Think of it as the template.

> **Schema Purpose**
> This schema ensures all attack path instances follow the same structure, making them machine-readable and enabling automated validation, aggregation, and analysis across organizations.

📋 `tlctc-attack-sequence-schema.json`

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "TLCTC Attack Sequence Schema",
  "description": "Validation schema for TLCTC attack path instances",
  "version": "1.0",

  "definitions": {
    "tlctc_cluster": {
      "type": "object",
      "properties": {
        "strategic": {
          "type": "string",
          "pattern": "^#(1|2|3|4|5|6|7|8|9|10)$",
          "description": "Strategic notation (#1-#10)"
        },
        "operational": {
          "type": "string",
          "pattern": "^TLCTC-(0[1-9]|10)\\.(00|01|02|03)$",
          "description": "Operational notation (TLCTC-XX.YY)"
        }
      },
      "required": ["strategic", "operational"]
    },

    "software_component": {
      "type": "object",
      "properties": {
        "name": {
          "type": "string",
          "description": "Software name"
        },
        "version": {
          "type": "string",
          "description": "Version number or range"
        },
        "vendor": {
          "type": "string",
          "description": "Software vendor/publisher"
        },
        "role": {
          "type": "string",
          "enum": [
```

```
          "target",
          "attack-tool",
          "dual-use-tool",
          "legitimate-tool-abused",
          "malware",
          "exploit-delivery",
          "vulnerability-source"
        ]
      },
      "cpe": {
        "type": "string",
        "description": "Common Platform Enumeration identifier"
      }
    },
    "required": ["name", "role"]
  },

  "vulnerability": {
    "type": "object",
    "properties": {
      "cves": {
        "type": "array",
        "items": {
          "type": "string",
          "pattern": "^CVE-[0-9]{4}-[0-9]{4,}$"
        }
      },
      "cwes": {
        "type": "array",
        "items": {
          "type": "string",
          "pattern": "^CWE-[0-9]+$"
        }
      },
      "custom_identifier": {
        "type": "string",
        "description": "Custom or zero-day identifier"
      },
      "description": {
        "type": "string"
      }
    }
```

```
    },

    "attack_step": {
      "type": "object",
      "properties": {
        "step_number": {
          "type": "integer",
          "minimum": 1
        },
        "tlctc_cluster": {
          "$ref": "#/definitions/tlctc_cluster"
        },
        "stage": {
          "type": "string",
          "enum": ["initial", "intermediate", "final"]
        },
        "responsibility_sphere": {
          "type": "string",
          "description": "ID from responsibility-spheres.json (e.g., @Org, @Vendor, @C
ustomer)"
        },
        "delta_t_to_next": {
          "type": "string",
          "description": "Attack velocity - time to next step. Format:  (e.g., 15m, 2h
, ~30s, <5m)",
          "examples": ["15m", "2h", "~30s", "<5m", "instant", "?"]
        },
        "velocity_class": {
          "type": "string",
          "enum": ["VC-1", "VC-2", "VC-3", "VC-4"],
          "description": "VC-1=Strategic(days-months), VC-2=Tactical(hours), VC-3=Oper
ational(minutes), VC-4=Real-Time(seconds)"
        },
        "software": {
          "type": "array",
          "items": {
            "$ref": "#/definitions/software_component"
          }
        },
        "temporal": {
          "type": "object",
          "properties": {
```

```
      "date": {
        "type": "string",
        "format": "date"
      },
      "time": {
        "type": "string",
        "format": "time"
      },
      "duration_minutes": {
        "type": "integer"
      },
      "detection_date": {
        "type": "string",
        "format": "date"
      },
      "detection_gap_days": {
        "type": "integer"
      }
    }
  },
  "mitre_mapping": {
    "type": "object",
    "properties": {
      "tactics": {
        "type": "array",
        "items": {
          "type": "string",
          "pattern": "^TA[0-9]{4}$"
        }
      },
      "techniques": {
        "type": "array",
        "items": {
          "type": "string",
          "pattern": "^T[0-9]{4}(\\.[0-9]{3})?$"
        }
      }
    }
  },
  "vulnerabilities": {
    "$ref": "#/definitions/vulnerability"
  },
```

```
        "impact": {
          "type": "object",
          "properties": {
            "data_risk_events": {
              "type": "array",
              "description": "Data Risk Events at this step (Lane 2)",
              "items": {
                "type": "object",
                "required": ["dre_id", "type"],
                "properties": {
                  "dre_id": {
                    "type": "string",
                    "description": "Unique identifier for this DRE"
                  },
                  "type": {
                    "type": "string",
                    "enum": ["C", "I", "A"],
                    "description": "C=Confidentiality, I=Integrity, A=Availability"
                  },
                  "description": {
                    "type": "string",
                    "description": "What data was affected and how"
                  },
                  "data_type": {
                    "type": "string",
                    "description": "Type of data affected (PII, credentials, IP, et
c.)"
                  },
                  "volume": {
                    "type": "string",
                    "description": "Estimated volume (records, GB, etc.)"
                  },
                  "timestamp": {
                    "type": "string",
                    "format": "date-time"
                  }
                }
              }
            },
            "system_compromise": {
              "type": "boolean"
            },
```

```
    "business_impact": {
      "type": "string"
    },
    "severity": {
      "type": "string",
      "enum": ["low", "medium", "high", "critical"]
    }
  }
},
"evidence": {
  "type": "object",
  "properties": {
    "iocs": {
      "type": "array",
      "description": "Indicators of Compromise",
      "items": {
        "type": "object",
        "properties": {
          "type": {
            "type": "string",
            "enum": ["ip", "domain", "url", "hash", "email", "filename"]
          },
          "value": {
            "type": "string"
          }
        }
      }
    },
    "artifacts": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "log_sources": {
      "type": "array",
      "items": {
        "type": "string"
      }
    }
  }
},
```

```
      "comment": {
        "type": "string",
        "description": "Analyst notes and observations"
      }
    },
    "required": [
      "step_number",
      "tlctc_cluster",
      "stage",
      "responsibility_sphere"
    ]
  }
},

"type": "object",
"properties": {
  "metadata": {
    "type": "object",
    "properties": {
      "sequence_id": {
        "type": "string",
        "description": "Unique identifier for this attack sequence"
      },
      "attack_title": {
        "type": "string"
      },
      "framework_version": {
        "type": "string",
        "description": "TLCTC framework version used"
      },
      "created": {
        "type": "string",
        "format": "date-time"
      },
      "modified": {
        "type": "string",
        "format": "date-time"
      },
      "analyst": {
        "type": "string",
        "description": "Analyst or team who created this"
      },
```

```
    "organization": {
      "type": "string"
    },
    "confidence": {
      "type": "string",
      "enum": ["low", "medium", "high", "confirmed"]
    },
    "classification": {
      "type": "string",
      "enum": ["public", "tlp-white", "tlp-green", "tlp-amber", "tlp-red"]
    },
    "tags": {
      "type": "array",
      "items": {
        "type": "string"
      }
    }
  },
  "required": ["sequence_id", "attack_title", "framework_version", "created"]
},

"threat_actor": {
  "type": "object",
  "properties": {
    "name": {
      "type": "string"
    },
    "aliases": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "type": {
      "type": "string",
      "enum": [
        "nation-state",
        "cybercrime",
        "hacktivist",
        "insider",
        "unknown"
      ]
```

```
    },
    "motivation": {
      "type": "string",
      "enum": [
        "espionage",
        "financial",
        "disruption",
        "ideology",
        "unknown"
      ]
    },
    "sophistication": {
      "type": "string",
      "enum": ["novice", "intermediate", "advanced", "expert"]
    }
  }
},

"attack_sequence": {
  "type": "array",
  "items": {
    "$ref": "#/definitions/attack_step"
  },
  "minItems": 1
},

"attack_path_notation": {
  "type": "string",
  "description": "TLCTC sequence notation (e.g., #9 → #3 → #7)"
},

"business_impacts": {
  "type": "array",
  "description": "Lane 3: Business impacts with linkage to steps or DREs",
  "items": {
    "type": "object",
    "required": ["impact_id", "category"],
    "properties": {
      "impact_id": {
        "type": "string",
        "description": "Unique identifier for this business impact"
      },
```

```
          "category": {
            "type": "string",
            "enum": ["operational", "financial", "reputational", "regulatory", "strate
gic"],
            "description": "Type of business impact"
          },
          "description": {
            "type": "string"
          },
          "severity": {
            "type": "string",
            "enum": ["critical", "high", "medium", "low"]
          },
          "linked_to_step": {
            "type": "integer",
            "description": "step_number that caused this impact (vertical causality)"
          },
          "linked_to_dre": {
            "type": "string",
            "description": "dre_id that led to this impact (vertical causality)"
          },
          "estimated_cost": {
            "type": "object",
            "properties": {
              "amount": { "type": "number" },
              "currency": { "type": "string", "default": "USD" },
              "confidence": { "type": "string", "enum": ["actual", "estimated", "rang
e"] }
            }
          }
        }
      }
    },

    "summary": {
      "type": "object",
      "properties": {
        "total_duration_days": {
          "type": "integer"
        },
        "detection_gap_days": {
          "type": "integer"
```

```
    },
    "affected_systems": {
      "type": "integer"
    },
    "affected_organizations": {
      "type": "integer"
    },
    "sectors_affected": {
      "type": "array",
      "items": {
        "type": "string"
      }
    },
    "estimated_cost": {
      "type": "object",
      "properties": {
        "amount": {
          "type": "number"
        },
        "currency": {
          "type": "string"
        }
      }
    }
  }
},

"references": {
  "type": "array",
  "items": {
    "type": "object",
    "properties": {
      "title": {
        "type": "string"
      },
      "url": {
        "type": "string",
        "format": "uri"
      },
      "source": {
        "type": "string"
      },
```

```
          "date": {
            "type": "string",
            "format": "date"
          }
        }
      }
    }
  },

  "required": [
    "metadata",
    "attack_sequence",
    "attack_path_notation"
  ]
}
```

📦 4. Attack Path Instance JSON (Example)

This is an actual threat intelligence instance - a specific attack that happened. This is what organizations share with each other.

> **Real-World Usage**
> When SolarWinds happened, instead of everyone describing it differently, they would all produce an attack-path.json following this schema. Automated tools could ingest it, compare it to other attacks, and update defenses accordingly.

🎯 `solarwinds-2020-attack-path.json`

```
{
  "metadata": {
    "sequence_id": "APT29-SOLARWINDS-2020",
    "attack_title": "SolarWinds Supply Chain Compromise (SUNBURST)",
    "framework_version": "1.9.1",
    "created": "2020-12-15T00:00:00Z",
```

```
    "modified": "2024-11-09T10:00:00Z",
    "analyst": "Threat Intelligence Team",
    "organization": "FireEye / Mandiant",
    "confidence": "confirmed",
    "classification": "public",
    "tags": [
      "APT29",
      "supply-chain",
      "nation-state",
      "SUNBURST",
      "SolarWinds",
      "critical-infrastructure"
    ]
  },

  "threat_actor": {
    "name": "APT29",
    "aliases": ["Cozy Bear", "The Dukes", "YTTRIUM", "UNC2452"],
    "type": "nation-state",
    "motivation": "espionage",
    "sophistication": "expert",
    "attribution": {
      "suspected_country": "Russia",
      "confidence": "high"
    }
  },

  "attack_sequence": [
    {
      "step_number": 1,
      "tlctc_cluster": { "strategic": "#10", "operational": "TLCTC-10.02" },
      "stage": "initial",
      "responsibility_sphere": "@SolarWinds",
      "delta_t_to_next": "~6mo",
      "velocity_class": "VC-1",
      "software": [
        { "name": "SolarWinds Orion Build Environment", "version": "N/A", "vendor": "S
olarWinds", "role": "vulnerability-source" }
      ],
      "temporal": { "date": "2019-09-01", "duration_minutes": 525600, "detection_date"
: "2020-12-13", "detection_gap_days": 470 },
      "mitre_mapping": { "tactics": ["TA0001"], "techniques": ["T1195.002"] },
```

```
      "vulnerabilities": {
        "cves": [],
        "cwes": ["CWE-506"],
        "custom_identifier": "Supply Chain Compromise",
        "description": "Attackers compromised SolarWinds build environment"
      },
      "impact": {
        "data_risk_events": [],
        "system_compromise": true,
        "business_impact": "Compromise of build pipeline enabling widespread downstrea
m attacks",
        "severity": "critical"
      },
      "evidence": {
        "iocs": [{ "type": "hash", "value": "b91ce2fa41029f6955bff20079468448" }],
        "artifacts": ["Compromised build server logs", "Modified build scripts"],
        "log_sources": ["SolarWinds build system logs", "Version control system"]
      },
      "comment": "#10.02 Development vector: compromise of the pre-deployment build pi
peline at the vendor."
    },

    {
      "step_number": 2,
      "tlctc_cluster": { "strategic": "#7", "operational": "TLCTC-07.00" },
      "stage": "intermediate",
      "responsibility_sphere": "third-party-vendor",
      "domain": "@SolarWinds",
      "software": [
        { "name": "SUNBURST Backdoor", "version": "Embedded in SolarWinds.Orion.Core.B
usinessLayer.dll", "role": "malware" },
        { "name": "SolarWinds Orion Platform", "version": "2019.4 HF 5 through 2020.2.
1 HF 1", "vendor": "SolarWinds", "role": "exploit-delivery" }
      ],
      "temporal": { "date": "2020-03-01", "duration_minutes": 20160 },
      "mitre_mapping": { "tactics": ["TA0002", "TA0003", "TA0011"], "techniques": ["T1
543.003", "T1071.001", "T1132.001"] },
      "vulnerabilities": {
        "cves": [],
        "custom_identifier": "SUNBURST-BACKDOOR",
        "description": "Malicious code injected into legitimate SolarWinds DLL"
      },
```

```
      "impact": {
        "data_risk_events": [],
        "system_compromise": true,
        "business_impact": "Backdoor embedded in trusted software distributed to 18,00
0+ customers",
        "severity": "critical"
      },
      "evidence": {
        "iocs": [
          { "type": "hash", "value": "c15abaf51e78ca56c0376522d699c978" },
          { "type": "domain", "value": "avsvmcloud.com" }
        ],
        "artifacts": ["SolarWinds.Orion.Core.BusinessLayer.dll (trojanized)", "C2 comm
unication logs"],
        "log_sources": ["Network traffic logs", "DNS logs", "EDR telemetry"]
      },
      "comment": "#7 Malware packaged into a signed vendor DLL for later execution in
customer environments."
    },

    {
      "step_number": 3,
      "boundary": {
        "type": "updates",
        "from_domain": "@SolarWinds",
        "to_domain": "@ORG",
        "notation": "|||updates][@SolarWinds→@ORG]||"
      },
      "stage": "intermediate",
      "responsibility_sphere": "trust-boundary",
      "domain": "@ORG",
      "temporal": { "date": "2020-03-01" },
      "impact": {
        "business_impact": "Trojanized update trusted and installed by downstream orga
nizations",
        "severity": "critical"
      },
      "comment": "Explicit trust boundary crossing: vendor → customer via legitimate u
pdate mechanism."
    },

    {
```

```
      "step_number": 4,
      "tlctc_cluster": { "strategic": "#7", "operational": "TLCTC-07.00" },
      "stage": "intermediate",
      "responsibility_sphere": "@Org",
      "delta_t_to_next": "~2w",
      "velocity_class": "VC-1",
      "software": [{ "name": "SUNBURST Backdoor", "role": "malware" }],
      "temporal": { "date": "2020-03-15", "duration_minutes": 43200 },
      "mitre_mapping": { "tactics": ["TA0002", "TA0011"], "techniques": ["T1071.001",
"T1573.001"] },
      "impact": {
        "data_risk_events": [
          {
            "dre_id": "dre-1",
            "type": "C",
            "description": "Initial C2 communication exposes network topology to attac
ker",
            "data_type": "network configuration"
          }
        ],
        "system_compromise": true,
        "business_impact": "Persistent backdoor access to victim networks",
        "severity": "critical"
      },
      "evidence": {
        "iocs": [
          { "type": "domain", "value": "avsvmcloud.com" },
          { "type": "ip", "value": "13.59.205.66" }
        ],
        "artifacts": ["HTTP C2 traffic", "DNS query patterns"],
        "log_sources": ["Firewall logs", "Proxy logs", "DNS logs"]
      },
      "comment": "#7 Malware executes within customer environment and establishes C2."
    },

    {
      "step_number": 5,
      "tlctc_cluster": { "strategic": "#7", "operational": "TLCTC-07.00" },
      "stage": "intermediate",
      "responsibility_sphere": "organization-internal",
      "domain": "@ORG",
      "software": [
```

```
        { "name": "TEARDROP", "role": "malware" },
        { "name": "RAINDROP", "role": "malware" },
        { "name": "Cobalt Strike", "role": "dual-use-tool" }
      ],
      "temporal": { "date": "2020-04-01" },
      "mitre_mapping": { "tactics": ["TA0002", "TA0005"], "techniques": ["T1055", "T11
05", "T1027"] },
      "impact": {
        "data_risk_events": [],
        "system_compromise": true,
        "business_impact": "Additional malware stages deployed for persistence and lat
eral movement",
        "severity": "critical"
      },
      "evidence": {
        "iocs": [{ "type": "hash", "value": "1835b0e8fc19bca99c4b8e0f7d9fa1b3" }],
        "artifacts": ["TEARDROP loader", "Cobalt Strike beacons"]
      },
      "comment": "Further #7 activity: staged loaders and interactive access tooling."
    },

    {
      "step_number": 6,
      "tlctc_cluster": { "strategic": "#4", "operational": "TLCTC-04.00" },
      "stage": "intermediate",
      "responsibility_sphere": "@Org",
      "delta_t_to_next": "~2w",
      "velocity_class": "VC-1",
      "software": [{ "name": "Credential Theft & Reuse", "role": "identity-abuse" }],
      "temporal": { "date": "2020-04-15" },
      "mitre_mapping": { "tactics": ["TA0006"], "techniques": ["T1078.002"] },
      "impact": {
        "data_risk_events": [
          {
            "dre_id": "dre-2",
            "type": "C",
            "description": "Domain admin credentials exfiltrated",
            "data_type": "credentials",
            "volume": "Multiple admin accounts"
          }
        ],
        "system_compromise": true,
```

```
        "business_impact": "Use of stolen domain/admin credentials (impersonation)",
        "severity": "critical"
      },
      "comment": "#4 Identity Theft: the *use* of stolen credentials to impersonate id
entities. (Acquisition occurred via prior #7 activity.)"
    },

    {
      "step_number": 7,
      "tlctc_cluster": { "strategic": "#1", "operational": "TLCTC-01.00" },
      "stage": "intermediate",
      "responsibility_sphere": "privileged-admin",
      "domain": "@ORG",
      "temporal": { "date": "2020-05-01" },
      "mitre_mapping": { "tactics": ["TA0008"], "techniques": ["T1021.001"] },
      "impact": {
        "data_risk_events": [],
        "system_compromise": true,
        "business_impact": "Lateral movement via legitimate remote admin/auth function
s",
        "severity": "high"
      },
      "comment": "#1 Abuse of Functions: moving laterally using built-in authenticatio
n/remote services after #4 impersonation."
    },

    {
      "step_number": 8,
      "boundary": {
        "type": "svc/idp",
        "from_domain": "@ORG",
        "to_domain": "@Microsoft",
        "notation": "|||svc/idp][@ORG→@Microsoft]||"
      },
      "stage": "intermediate",
      "responsibility_sphere": "trust-boundary",
      "domain": "@Microsoft",
      "temporal": { "date": "2020-06-01" },
      "impact": {
        "business_impact": "Federated/service trust crossing to cloud",
        "severity": "critical"
      },
```

```
      "comment": "Explicit crossing to Microsoft service/IdP domain."
    },

    {
      "step_number": 9,
      "tlctc_cluster": { "strategic": "#4", "operational": "TLCTC-04.00" },
      "stage": "final",
      "responsibility_sphere": "organization-internal",
      "domain": "@Microsoft",
      "software": [
        { "name": "Azure AD", "role": "idp" },
        { "name": "Microsoft 365", "role": "target" }
      ],
      "temporal": { "date": "2020-06-01" },
      "mitre_mapping": { "tactics": ["TA0006"], "techniques": ["T1078.004"] },
      "impact": {
        "data_risk_events": ["LoC"],
        "system_compromise": true,
        "business_impact": "Cloud sign-in/token use as impersonated identities",
        "severity": "critical"
      },
      "evidence": { "log_sources": ["Azure AD sign-in logs", "Office 365 audit logs"]
},
      "comment": "#4 Identity Theft in cloud: use of credentials/tokens to assume iden
tities in M365/Azure."
    },

    {
      "step_number": 10,
      "tlctc_cluster": { "strategic": "#1", "operational": "TLCTC-01.00" },
      "stage": "final",
      "responsibility_sphere": "organization-internal",
      "domain": "@Microsoft",
      "software": [
        { "name": "Microsoft 365", "role": "target" },
        { "name": "Azure", "role": "target" }
      ],
      "temporal": { "date": "2020-06-01" },
      "mitre_mapping": { "tactics": ["TA0009"], "techniques": ["T1114.002", "T1213.00
2"] },
      "impact": {
        "data_risk_events": ["LoC"],
```

```
        "system_compromise": true,
        "business_impact": "Mailbox and cloud resource access via legitimate APIs",
        "severity": "critical"
      },
      "evidence": { "log_sources": ["Office 365 audit logs", "Azure activity logs"] },
      "comment": "#1 Abuse of Functions: accessing email and cloud data via normal ser
vice functions."
    },

    {
      "step_number": 11,
      "tlctc_cluster": { "strategic": "#1", "operational": "TLCTC-01.00" },
      "stage": "final",
      "responsibility_sphere": "organization-internal",
      "domain": "@Microsoft",
      "temporal": { "date": "2020-06-15" },
      "mitre_mapping": { "tactics": ["TA0010"], "techniques": ["T1567.002", "T1048.00
3"] },
      "impact": {
        "data_risk_events": ["LoC"],
        "system_compromise": true,
        "business_impact": "Exfiltration of sensitive data using standard HTTPS/cloud
storage APIs",
        "severity": "critical"
      },
      "comment": "#1 Abuse of Functions: data egress through legitimate protocols/serv
ices."
    }
  ],

  "attack_path_notation": "#10.02 → #7 → |||[updates][@SolarWinds→@ORG]|| → #7 → #7 →
(#4 → #1) → |||[svc/idp][@ORG→@Microsoft]|| → (#4 → #1) → #1",

  "business_impacts": [
    {
      "impact_id": "bi-1",
      "category": "regulatory",
      "description": "Mandatory breach notifications to multiple government agencies a
nd affected organizations",
      "severity": "critical",
      "linked_to_step": 4,
      "linked_to_dre": "dre-1"
```

```
    },
    {
      "impact_id": "bi-2",
      "category": "reputational",
      "description": "Significant damage to SolarWinds brand and customer trust",
      "severity": "critical",
      "linked_to_step": 1
    },
    {
      "impact_id": "bi-3",
      "category": "financial",
      "description": "Global incident response, remediation, and legal costs",
      "severity": "critical",
      "linked_to_step": 11,
      "estimated_cost": {
        "amount": 1000000000,
        "currency": "USD",
        "confidence": "estimated"
      }
    },
    {
      "impact_id": "bi-4",
      "category": "strategic",
      "description": "Potential exfiltration of sensitive government and corporate int
ellectual property",
      "severity": "critical",
      "linked_to_dre": "dre-2"
    },
    {
      "impact_id": "bi-5",
      "category": "operational",
      "description": "Mass emergency patching and system rebuilds across 18,000+ organ
izations",
      "severity": "critical",
      "linked_to_step": 4
    }
  ],

  "summary": {
    "total_duration_days": 470,
    "detection_gap_days": 470,
    "affected_systems": 18000,
```

```
    "affected_organizations": 18000,
    "sectors_affected": [
      "government",
      "technology",
      "telecommunications",
      "consulting",
      "energy",
      "healthcare"
    ],
    "estimated_cost": {
      "amount": 1000000000,
      "currency": "USD",
      "note": "Estimated global impact including response and remediation"
    }
  },

  "references": [
    {
      "title": "SUNBURST Backdoor Analysis",
      "url": "https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html",
      "source": "FireEye",
      "date": "2020-12-13"
    },
    {
      "title": "Microsoft Analysis of Solorigate",
      "url": "https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/",
      "source": "Microsoft",
      "date": "2020-12-18"
    },
    {
      "title": "CISA Alert AA20-352A",
      "url": "https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a",
      "source": "CISA",
      "date": "2020-12-17"
    }
  ]
}
```

🔄 How These JSONs Work Together

```
INCIDENT ANALYSIS WORKFLOW
═══════════════════════════════════════════

1. FRAMEWORK FOUNDATION
   └→ Load tlctc-framework.json
      ├─ Threat cluster definitions
      ├─ Data risk event types
      └─ Attack path notation rules

2. REFERENCE DATA
   └→ Load tlctc-responsibility-spheres.json
      └─ Domain boundary definitions

3. CREATE ATTACK INSTANCE
   └→ New JSON following schema
      ├─ Map each step to TLCTC clusters
      ├─ Assign responsibility spheres
      ├─ Document software & versions
      ├─ Add CVEs, MITRE TTPs
      └─ Record timeline & impact

4. VALIDATION
   └→ Validate against tlctc-attack-sequence-schema.json
      └─ Ensures consistency & completeness

5. SHARING & ANALYSIS
   └→ Share attack-path.json with community
      ├─ All orgs understand notation
      ├─ Automated tool ingestion
      ├─ Pattern matching across incidents
      └─ Aggregated threat intelligence
```

✅ Key Benefits of This Architecture

BENEFIT	HOW IT'S ACHIEVED

BENEFIT	HOW IT'S ACHIEVED
Universal Language	Everyone references the same `framework.json` definitions
Machine-Readable	Structured JSON enables automated ingestion and analysis
Consistent Validation	Schema ensures all instances follow same structure
Separation of Concerns	Framework (static) vs Intelligence (dynamic) clearly separated
Evolution-Friendly	Framework can evolve without breaking historical instances
Global Collaboration	Standardized format enables worldwide threat intelligence sharing
Tool Integration	SIEM, SOC, TIP tools can parse and correlate automatically

🎯 Usage Examples

For Security Operations Centers (SOC)

- Load `tlctc-framework.json` into your SIEM/TIP
- Configure detection rules mapped to TLCTC clusters
- When incidents occur, create `[incident-id]-attack-path.json`
- Share with trusted partners / ISACs / threat intelligence communities
- Receive attack paths from others, automatically correlate patterns

For Threat Intelligence Teams

- Document APT campaigns using `attack-path.json` format
- Compare attack sequences across different threat actors
- Identify common patterns (e.g., all APT29 attacks start with #10 → #7)
- Generate Cyber Threat Radars showing cluster distribution

- Feed intelligence into defensive tools using standardized format

For Risk Management

- Reference `tlctc-framework.json` for threat taxonomy in risk register
- Map controls to specific TLCTC clusters using NIST CSF functions
- Analyze historical attack paths to identify control gaps
- Prioritize investments based on cluster frequency in your sector
- Communicate risks to board using strategic notation (#X)

📝 Creating Your Own Attack Path Instance

> **Quick Start**
>
> To document an attack you've observed:
>
> - Copy the `attack-sequence-schema.json` structure
> - For each step in the attack:
>
> Map to appropriate TLCTC cluster (use `framework.json` for reference)
>
> Identify stage (initial/intermediate/final)
>
> Determine responsibility sphere
>
> Document software, CVEs, TTPs observed
>
> Record timeline and impact
> - Generate the attack path notation (e.g., #9 → #3 → #7)
> - Validate against the schema
> - Share with community!

🌐 Tool Integration

These JSON structures are designed to integrate with:

- STIX/TAXII - Enhanced STIX objects with TLCTC mappings
- MITRE ATT&CK Navigator - Techniques mapped to clusters

- SIEM Platforms - Automated rule generation per cluster
- Threat Intelligence Platforms - Standardized ingestion
- Risk Management Tools - Direct mapping to controls
- Incident Response Platforms - Playbook generation per cluster

> ⚠️ **Important Notes**
>
> - Always reference the framework version in your attack instances
> - Respect data classification (use TLP markings)
> - Validate against schema before sharing
> - Include sufficient evidence/references for verification
> - Update modified timestamp when editing instances

🚀 Next Steps

Start Using the Framework:

- Download all four JSON files above
- Load `framework.json` and `spheres.json` into your tools
- Review the schema to understand the structure
- Document your next incident using the attack-path format
- Share with the community to enable global threat intelligence

Contribute to Framework Evolution:

- Provide feedback on the schema structure
- Suggest additional responsibility spheres
- Share real-world attack paths for validation
- Help develop tool integrations
- Join the community at www.tlctc.net

Bernhard Kreinz

BK